RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

diretta da Sebastiano Faro e Marina Pietrangelo

La Internet governance e le sfide della trasformazione digitale

FASCICOLO MONOGRAFICO

a cura di
L. Abba, A. Lazzaroni, M. Pietrangelo

Anno IV, n. 1/2022 • Periodicità semestrale • ISSN 2704-7318
Periodico telematico: www.rivistaitalianadiinformaticaediritto.it
Direzione e Redazione: Istituto di Informatica Giuridica e Sistemi Giudiziari • Via dei Barucci 20 - 50127 Firenze

1 2022

Consiglio Nazionale delle Ricerche

Rivista italiana di informatica e diritto
Periodico internazionale del CNR-IGSG

Anno IV • n. 1/2022 • Periodicità semestrale
www.rivistaitalianadiinformaticaediritto.it

Direzione
Sebastiano Faro (*IGSG-CNR*) e Marina Pietrangelo (*IGSG-CNR*)

Comitato di direzione
Federigo Bambi (*Univ. Firenze*), Davide Carnevali (*IGSG-CNR*), Gian Luca Conti (*Univ. Pisa*), Enrico Francesconi (*IGSG-CNR*), Erik Longo (*Univ. Firenze*), Elisabetta Marinai (*IGSG-CNR*), Stefano Pietropaoli (*Univ. Firenze*), Francesco Romano (*IGSG-CNR*)

Comitato scientifico nazionale
Laura Abba (*IGSG-CNR*), Agata C. Amato Mangiameli (*Univ. Roma-Tor Vergata*), Andrea Cardone (*Univ. Firenze*), Antonio Carcaterra (*UnitelmaSapienza*), Paolo Caretti (*già Univ. Firenze*), Massimo Carli (*già Univ. Firenze*), Enrico Carloni (*Univ. Perugia*), Elisabetta Catelani (*Univ. Pisa*), Adriana Ciancio (*Univ. Catania*), Renato Clarizia (*Univ. Roma Tre*), Giuseppe Corasaniti (*UnitelmaSapienza*), Pasquale Costanzo (*già Univ. Genova*), Giovanna De Minico (*Univ. Napoli-Federico II*), Rosa Maria Di Giorgi (*IGSG-CNR*), Elio Fameli (*già IGSG-CNR*), Carla Faralli (*Univ. Bologna*), Giusella Finocchiaro (*Univ. Bologna*), Tommaso E. Frosini (*Univ. Napoli-Suor Orsola Benincasa*), Mario Jori (*già Univ. Milano*), Donato A. Limone (*UnitelmaSapienza*), Aldo Loiodice (*Univ. Europea Roma*), Luigi Lombardi Vallauri (*già Univ. Firenze*), Nicola Lupo (*Univ. Roma-LUISS*), Nicoletta Maraschio (*Accademia della Crusca*), Paola Marsocci (*Univ. Roma-Sapienza*), Paolo Moro (*Univ. Padova*), Monica Palmirani (*Univ. Bologna*), Ugo Pagallo (*Univ. Torino*), Giovanni Pascuzzi (*Consiglio di Stato*), Paolo Passaglia (*Univ. Pisa*), Dianora Poletti (*Corte di Cassazione*), Oreste Pollicino (*Univ. Milano-Bocconi*), Giovanni Sartor (*Univ. Bologna*), Andrea Simoncini (*Univ. Firenze*), Carlo Sorrentino (*Univ. Firenze*), Giancarlo Taddei Elmi (*già IGSG-CNR*), Lara Trucco (*Univ. Genova*), Stefano Trumpy (*Internet Society*), Alessandra Valastro (*Univ. Perugia*), Franco Vallocchia (*Univ. Roma-Sapienza*), Giovanni Ziccardi (*Univ. Milano*)

Comitato scientifico dei corrispondenti stranieri
Y. Amoroso (C), T.J.M. Bench Capon (GB), D. Bourcier (F), W.E. Boyd (USA), V. De Mulder (NL), J. Dumortier (NL), F. Galindo (E), A. Gardner (USA), T. Gordon (D), G. Greenleaf (AUS), O.P. Hance (L), W. Kilian (D), F. Lachmayer (A), P. Leith (IRL), E. Mackaay (CAN), A. MacIntosh (GB), P. Maharg (GB), J. Mayor (USA), L.T. McCarty (USA), F. Novak (CZ), A. Paliwala (GB), A.E. Perez-Luño (E), R. Petrauskas (LT), L. Philipps (D), Y. Poullet (B), A. Saarempaa (FIN), E. Schweighofer (A), P. Seipel (S), R. Susskind (GB), W.R. Svoboda (A), H. Yoshino (J), T. Van Engers (NL), M.A. Wimmer (A), R. Winkels (NL), J. Zeleznikow (AUS)

Esperti per la valutazione
Fulvia Abbondante (*Univ. Napoli-Federico II*), Enrico Albanesi (*Univ. Genova*), Maria Romana Allegri (*Univ. Roma-Sapienza*), Marco Bassini (*Univ. Milano-Bocconi*), Raffaella Brighi (*Univ. Bologna*), Elda Brogi (*European University Institute*), Simone Calzolaio (*Univ. Macerata*), Giuseppe Cammarota (*Univ. Cagliari*), Gianluigi Ciacci (*Univ. Roma-LUISS*), Sofia Ciuffoletti (*Univ. Firenze*), Maria Vittoria Dell'Anna (*Univ. Salento*), Fabio Dell'Aversana (*Univ. Cassino e Lazio Meridionale*), Francesco di Ciommo (*Univ. Roma-LUISS*), Rossana Ducato (*Univ. Trento*), Fernanda Faini (*Univ. Pisa*), Elisabetta Frontoni (*Univ. Roma Tre*), Paolo Galdieri (*Univ. Napoli-Federico II*), Riccardo Gualdo (*Univ. Tuscia*), Paolo Guarda (*Univ. Trento*), Antonio Iannuzzi (*Univ. Roma Tre*), Ilaria Kutufà (*Univ. Pisa*), Alessandro Lovari (*Univ. Cagliari*), Gianclaudio Malgieri (*Free University of Brussels – VUB*), Fabio Martinelli (*IIT-CNR*), Daniele Marongiu (*Univ. Cagliari*), Letizia Materassi (*Univ. Firenze*), Matteo Monti (*Univ. Roma-LUISS*), Erica Palmerini (*Scuola Superiore Sant'Anna*), Saulle Panizza (*Univ. Pisa*), Anna Papa (*Univ. Napoli-Parthenope*), Paolo Passaglia (*Univ. Pisa*), Viviana Patti (*Univ. Torino*), Giovanni Piccirilli (*Univ. Roma-LUISS*), Benedetto Ponti (*Univ. Perugia*), Cecilia Robustelli (*Univ. Modena e Reggio Emilia*), Andrea Rossetti (*Univ. Milano-Bicocca*), Simone Scagliarini (*Univ. Modena e Reggio Emilia*), Caterina Sganga (*Scuola Superiore Sant'Anna*), Maurizio Tesconi (*IIT-CNR*), Marco Torre (*Univ. Firenze*), Emilio Tosi (*Univ. Milano-Bicocca*), Giuseppe Vaciago (*Univ. Insubria*), Giulia Venturi (*ILC-CNR*)

Redazione tecnica
Simona Binazzi (segreteria), Giuseppina Sabato (composizione dei testi), Elisabetta Marinai (sito web)

Direzione e Redazione
IGSG/CNR
Via dei Barucci, 20 • 50127 Firenze
tel. 055 43995 • fax 055 4399605 • RivistaRIID@igsg.cnr.it • www.rivistaitalianadiinformaticaediritto.it

Direttore responsabile
Sebastiano Faro

Registrazione presso il Tribunale di Roma al n. 127/2019

Indice

La Internet governance e le sfide della trasformazione digitale

a cura di Laura Abba, Adriana Lazzaroni, Marina Pietrangelo

Parte prima. *Visioni*

7 **Vinton G. Cerf**
On Internet Governance

13 **Guido Scorza**
In principio era Internet e lo immaginavamo diverso

17 **Gianpaolo Maria Ruotolo**
Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet

25 **Wolfgang Kleinwächter**
Wanted: Nobel Peace Price Winners Who Create Peace in Cyberspace

31 **Arturo Di Corinto**
Data commons: privacy e cybersecurity sono diritti umani fondamentali

39 **Vittorio Bertola**
La sovranità digitale e il futuro di Internet

47 **Mauro Santaniello**
Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance

53 **Domenico Alfieri**
Internet: quando la “rete” cattura i minori

63 **Demi Getschko • Carlos Afonso • Alexandre F. Barbosa**
Il ruolo della governance multi-stakeholder di Internet nella diffusione della connettività in Brasile

77 **Gian Luca Conti**
Contratto sociale e *grundnorm* al tempo degli unicorni

93 **Agata C. Amato Mangiameli**
Intelligenza artificiale, big data e nuovi diritti

103 **Veronica Palladini**
Data retention e privacy in rete: verso una regolazione conforme al diritto UE?

113 **Giuseppe De Ruvo**
Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma

125 **Amaury Trujillo**
The surge of non-fungible tokens and its implications for digital ownership from an Internet governance perspective

133 **Pietro Dunn**
Moderazione automatizzata e discriminazione algoritmica: il caso dell'*hate speech*

145 **Alessandro Ortalda • Stefano Leucci**
Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD

157 **Jacopo Ciani Sciolla**
Diritto all'oblio e cooperazione internazionale: problemi e prospettive

175 **Ottavio Grandinetti**
Le piattaforme digitali come "poteri privati" e la censura online

189 **Elena Montagnani**
Le pubbliche amministrazioni nell'era delle tecnologie cloud ed *edge computing* tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali

201 **Giulia Bazzoni**
L'evoluzione normativa dell'intermediazione digitale: nuovi profili di responsabilizzazione

213 **Marco Rhao**
Il paradosso di Nakamoto: utilità attese e pericoli potenziali di un impiego istituzionale della tecnologia *blockchain*

229 **Dimitri Martignago**
Una governance dei dati genetici per lo sviluppo della ricerca scientifica

241 **Igor Marcolongo • Lorenzo Piatti • Alessandra Bossi**
Internet governance: una questione di digital trust

251 **Angelo Alù**
La Governance di Internet oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale

261 **Gloria Mancini Palamoni**
Lo sviluppo sostenibile del patrimonio culturale tra emergenze e tecnologie digitali

273 **Anna Federica Spagnuolo • Elisa Sorrentino**
Open data per l'*e-democracy*

283 **Alessandra Pietroletti • Alessandro Nicotra**
Tutela della salute, sistemi digitali e privacy

295 **Maria Novella Campagnoli**
Relazioni e solitudini nella Rete.
#Social_relation_&_società_confessionale

309 **Antonella Losanno**
Diritti "in rete" e libertà religiosa. L'effettività dei diritti attraverso l'efficacia della Internet governance

323 **Paola Polliani • Andrea Coldesina**
Lo smart working in Italia tra rivoluzione culturale, normativa emergenziale e un futuro ancora da scrivere

333 **Deborah Grbac**
La trasmissione dell'eredità culturale ed intellettuale delle Nazioni Unite online nel contesto internazionale della definizione di un ecosistema della governance di Internet e in particolare della scienza aperta

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0049

On Internet Governance

Vinton G. Cerf

This essay tries to analyze the complex challenge of introducing governance measures to preserve the utility of the Internet, the safety of citizens and to hold accountable those who abuse the privilege of access to the Internet.

Internet based – Applications – Ecosystem – Potential risks – Human behavior

Summary: *1. Introduction – 2. Technical Perspective – 3. Organizational Perspective – 4. Internet Governance – 5. Afterthoughts*

1. Introduction

What do we mean when we speak of "Internet Governance"?

As the third decade of the 21st Century unfolds we find ourselves in the midst of a global pandemic. Among many lessons from this continuing experience, we have found that the global Internet is playing a significant role for many of the nearly 60% of the world's population that has access to it. Of course, the quality, cost and reliability of access vary and in every country there are areas that have little or no useful access. Nonetheless, its benefits have been apparent, especially for those able to work remotely, obtain general access to information and those relying on it for important scientific exchanges. The latter contributed to the speed with which vaccines were developed against the SARS-COV-2 virus that leads to COVID-19 infection.

The power of the Internet and the applications that have developed using the World Wide Web platform that rides on the Internet have alerted governments, the private sector, academia and the general public to the benefits and the hazards that this system affords. The optimism of the early days of the Internet and the World Wide Web have given way to the recognition that this powerful set of technologies can and is being abused by people that do not have the general public's best interests at heart. With the arrival of *social media* such as Facebook, Twitter, Tik-Tok and YouTube, opportunities for group formation on both global and local scales emerged. More generally, the sources of information have dramatically grown without regard to quality, thanks to these new application technologies. Opportunities for abuse of the Internet have mounted and become both more visible and potentially more harmful (think ransomware and destructive mal-

Vinton G. Cerf is an American computer scientist who is recognized as one of the "Fathers of the Internet". He founded the Internet Society (ISOC) and served as its first president. With his work, he completely revolutionized information transmission processes, allowing the unrestricted flow of information all around the world. He serves as vice president and chief Internet evangelist for Google and his primary responsibility is to identify new enabling technologies to support the development of advanced Internet-based products and services for the company.

This essay was prepared by the Author at the invitation of the Editors of this special issue of the journal as an introduction to the foundational concepts related to the Internet governance. The paper provides the reader with a realistic overview of the Internet ecosystem, especially from an organizational perspective, clarifying that the Internet is a much more complex and multilayered structure than the World Wide Web and all the applications that use it.

The paper is part of the Special issue "Internet governance and the challenges of digital transformation" edited by Laura Abba, Adriana Lazzaroni and Marina Pietrangelo.

An Italian translation of this essay edited by Laura Abba is available on CNR-IGSG website.

ware, misinformation and disinformation, phishing and spam email), governments have concluded that some kind of regulatory response is needed, including law enforcement.

It is in this context that this essay tries to analyze the complex challenge of introducing governance measures to preserve the utility of the Internet, the safety of citizens and to hold accountable those who abuse the privilege of access to the Internet.

2. Technical Perspective

It is important for parties interested in the governance of the Internet to know about the basic layering of the Internet (including the World Wide Web) because the various opportunities for governance interventions vary depending on the layer in which issues arise requiring regulation.

The Internet is designed as a layered system. The lower layers of its implementation involve the physical transport of digital information using *packet switching technology*. A useful analogy is to imagine electronic postcards that have *to* and *from* addresses and some content. Internet packets, like postcards, don't know how they are being carried. They could be transmitted on wires, coaxial cables, optical fibers, radio and satellite channels. In addition, like postcards, Internet packets don't know what information they are carrying. This ignorance is actually a major design benefit. When new transmission technologies come along, they can easily carry the digital packets of the Internet. Moreover, if a new application is developed that needs to interpret the payload of the Internet packets (think "things written on the postcard"), the network need not change because it doesn't care what the application is. While this produces a *best efforts network*, rather than one fine-tuned for specific applications, the Internet has been able to adapt to a remarkable number of applications including electronic mail, remote access to time-shared computers, streaming audio and video, video conferencing, real-time gaming, remote device control (think *Internet of Things* – IOT) and a host of others.

It is important to recognize that the basic Internet is not the World Wide Web nor is it all the applications that use it. For purposes of this essay, the Internet is a transport system that moves packets of data from source to destination. There are a number of *protocols* (think: practices, procedures, standard formats of data) that make it possible for the Internet to move packets around. Several core protocols make up the basic Internet. These are the Internet Protocol (IP), the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). One can think of IP as a basic postcard service. IP packets have numerical addresses for all sources and destinations in the Internet and a method for finding routes from source to destination. TCP makes sure all the postcards are delivered completely and in order by introducing a layer above the IP protocol to achieve those objectives. It keeps track of re-ordering packets that might arrive out of order, re-transmitting any that might appear to be lost, filtering of duplicate packets and managing the flow of the traffic to keep the receiver from being overwhelmed. The UDP protocol gives access to low delay transport over IP without introducing any of the discipline of the TCP protocol. The result is lower latency (delay) but with the potential for disorderly arrival and receipt of duplicate traffic. The aggregate suite of protocols that make up the basic Internet are sometimes called the *TCP/IP Protocol Suite*. It includes other protocols that support routing of traffic across the global Internet, encryption of packets for confidentiality, translation of *Domain Names* (think: *cnr.it*) into IP addresses.

Applications that use the basic Internet have yet other protocols for their implementation. Remote access to time-shared computers and data centers, electronic mail transport, file transport and streaming audio and video are examples of applications that use the Internet. The World Wide Web is implemented with its own set of protocols (*Hypertext Transport Protocol* – HTTP and *Hypertext Markup Language* – HTML) running on top of TCP/IP.

The introduction of the Apple *iPhone* in 2007 represented an inflexion point in application space with millions of applications being created for smartphones from multiple suppliers. The writers of these applications need only to know how the smartphone accepts and delivers data through *Application Programming Interfaces* (APIs) without knowing all the details of how mobile phones actually move voice and data over the air and through supporting fiber networks. The smartphone made the Internet more accessible and the Internet made the smartphone more useful. It is increasingly the case that smartphones are essentially endpoints in the Internet Protocol space and are directly reachable via TCP/IP and UDP protocols. The applications found on smartphones are increasingly manifestations of access to Web servers in data centers around the world. Voice communication is rapidly becoming *Voice over IP* (VOIP) as opposed to the earlier circuit-switched, analog voice of the past. This is so even on traditional telephone networks that have abandoned cir-

cuit switches for packet switches that cost less and are more flexible.

It is also vital to recognize that the Internet was designed to be expandable. It is a *Network of Networks* designed to allow an arbitrarily large number of networks to be interconnected. Each is operated independently of the others but they all follow the same standard protocols so as to achieve interoperability among all of them. Anything, anywhere on the Internet can communicate with anything else on the Internet regardless to which component networks the source and destination devices are connected.

3. Organizational Perspective

Just as it is important to appreciate the layered technical structure of the Internet and the World Wide Web, it is also important to understand the role of organizations in their implementation and operation. For example, some key players in the Internet environment are cable and fiber operators delivering Internet service to homes, businesses, institutions and government agencies. Similarly the wireless carriers do the same thing over the air. Others provide underlying submarine cable service linking pieces of the Internet around the world.

Other players make *routers* that implement the IP system of network interconnection or smartphones. The Internet of Things refers to a growing number of devices that are *internet-enabled* and are made by manufacturers who want to take advantage of the global connectivity of the Internet to provide devices and possibly associated services such as monitoring or software updates to the users of these devices. Still others make Domain Name resolvers and servers to translate domain names into IP addresses. Companies like Apple, Microsoft and Google make operating systems such as OSX, IOS, Windows or Android used in many smartphones, pads, laptops and IOT devices.

In addition to organizations and businesses that make Internet-enabling or Internet-enabled devices, there are *Internet service providers* (ISPs) that provide access to the Internet. These include mobile smartphone services, fiber and cable services, and low, medium and geo Earth orbit satellite services. Other organizations operate *Internet Exchange Points* that allow for efficient interconnection of many networks that make up the Internet. For the most part, these operators are focused only on the delivery of Internet packets and not on the interpretation of their payloads except to the extent that these are part of the Internet operational control system such as the *Border Gateway Protocol* (BGP) routing system.

Platform companies such as Google, Facebook, Microsoft, Amazon, IBM and others operate multiple data centers around the world, often interconnected by private fiber networks which are, in turn, connected to the public Internet.

It is on these platforms that a significant fraction of Internet and Web-based services are supported. In addition, there are companies such as Akamai that operate *Content Distribution Networks* that bring content closer to users by placing it in servers that are placed with telephone central offices and cable company head ends or nearby Internet Exchange Points.

Countless companies make application software that runs in the various data centers or CDNs to serve customers of these applications. Others create content such as Netflix and Amazon and the traditional movie studio companies which is distributed through streaming on the World Wide Web. Banks provide financial services and millions of companies create websites to serve customers. Advertising is a major component of the 21st Century Internet and drives some businesses that provide free services to users in exchange for showing them advertisements paid for by companies wishing to offer products and services to the general public.

There are, however, another class of organizations that are tied more closely to the technology of the Internet. Some of them create and maintain technical standards for the Internet among which are the Internet Engineering Task Force (IETF) sponsored by the Internet Society; the World Wide Web Consortium (W3C) for Web standards; the Organization for International Standardization (ISO), 3GPP (for mobile standards), the International Telecommunication Union (ITU) and its standards bodies ITU-R (radio) and ITU-T (telecommunication) and the Institute of Electrical and Electronics Engineers (IEEE) along with various national bodies such as the British Standards Institution (BSI), the American National Institute of Standards and Technology (NIST), the European Telecommunications Standards Institute (ETSI) and the Italian Organization for Standardization (UNI).

It is important to recognize in the context of governance that there are many organizations with an interest in the "rules of the road" for the Internet and WWW. This includes civil society and the academic community in addition to governments at all levels. It is for this reason that the notion of *Multistakeholder Internet Governance* has been a common thread in the history of the Internet and the Web.

There are simply an enormous number of interested parties, parties with the power to develop and effect various norms and regulations and parties who are affected by these same rules and regulations.

4. Internet Governance

We come now to the crux of this essay: how is governance of the Internet to be effected with the goal of preserving the enormous value that the free flow of information has provided in the decades of operation of the Internet (since 1983) and the World Wide Web (since 1991). Multistakeholder development of policy including governments, civil society, the academic and standards communities and the private sector is highly desirable so as to include their perspectives and to understand the potential impact on various sectors of choices of policies, regulations and methods of enforcement. While enforcement of policy may fall to a smaller cohort, broadly informed policy development has been beneficial for the Internet and World Wide Web over the course of their evolution.

One important principle to urge is *subsidiarity*. That is, to apply regulatory mechanisms at the appropriate layers and to the appropriate players of the Internet ecosystem. For example, fragmenting the basic Internet in the interest of so-called *data sovereignty* threatens the free flow of information on a global scale. The value of that free flow is vital to the sharing and discovery of information that benefits everyone. If protection of information is a high priority, and it is for many things including *personally identifiable information*, one can make use of cryptographic means both to protect information in transit and at rest and to strongly authenticate users to provide only authorized access to the sensitive information. It is not necessary to confine information to specific geographies to achieve that effect. Low level geo-fragmentation of the Internet has negative consequences including the inhibition of replication of data at multiple datacenters to avoid loss even in the face of catastrophic failure.

If content is unacceptable in some contexts, blocking Internet access at the IP address level is an extremely blunt instrument. Similarly so with domain name blocking. By analogy, if someone is selling drugs illegally from an apartment, arresting all occupants of the building penalizes many innocent parties. If content is widely considered unacceptable, such as Child Sexual Abuse Material (CSAM), a potentially less blunt response is to demand its removal from serving sites. Of course, because the Internet and the Web are global, this might require the cooperation of national governments as is contemplated by the UN Secretary-General's Digital Cooperation proposals. In the absence of cooperation, governments may choose to apply much more blunt instruments.

Regulators will benefit from a refined view of the layered structure of the Internet and World Wide Web as well as an appreciation for the diversity of the ecosystem that animates them. Applying policy to the appropriate parties, recognizing their roles in the system can preserve the benefits of the Internet writ large while focusing attention and regulatory constraints more appropriately. It is worth recognizing that many of the organizations that populate the ecosystem perform multiple roles and some have vertical components that should be viewed from the layered perspective when considering regulatory responses to governance concerns.

5. Afterthoughts

In this brief essay, I have not attempted to deal with some really pernicious problems such as malware, denial of service attacks, the spread of misinformation and disinformation, harmful effects of social networking, the role of the general public and users in defending themselves from risk and harm. It seems valuable, however, to draw attention to some of these matters, however lightly. Users need to be literate about the potential hazards of *online life*. They need to have tools for protection such as two-factor authentication in addition to their usernames and passwords. They need to be able to detect likely *phishing* attacks. They need to avoid downloading files and software from questionable sources. They need to avoid clicking on hyperlinks without applying some critical thinking to their origins and intent.

Open Source Software has been a boon for programmers but a major hazard because careful evaluation of the software is neglected on the assumption that "all the bugs have already been found". Sadly, this assumption often means "none of the bugs have been found". The most recent example of this is the *Log4J* bug that allowed exploitation by running arbitrary software on the infected user's computer. This may be the worst bug found in decades as the software is in extremely wide use. Supply chain attacks that go after critical pieces of software supplied by smaller companies not well-prepared to defend against penetration and alteration of their products have led to very serious consequences for companies and consumers. Ransomware attacks have had cascading side-effects such as the near shutdown of commerce on the US East Coast due to lack of fuel

when the Colonial Pipeline operation was hit with an attack.

In our zeal to strongly identify and authenticate users, it is possible to create massive bio-data collections (faces, fingerprints, eye iris scans) that are extremely attractive to hackers interested in using or reselling this kind of information. As we recognize the potentially harmful aspects of social networking applications, companies and governments will benefit from the advice and insights from sociologists, psychologists, neuro-scientists and even anthropologists. Human behavior is complex and it is partly determined by evolutionary physiology in which emotional triggers spur reaction without much thought (e.g. fight or flight, thinking fast and thinking slow).

I have given little or no space to the whole matter of digital inclusion: making the Internet accessible (in both senses), available, affordable, reliable, safe, secure, privacy-protecting for everyone on the planet. There are many barriers to achieving global access and these, too, deserve governance attention and have not been given adequate treatment in this short essay.

There is no question in my mind that we need to attend to the potential risks we face with computer-based, networked services, but I believe strongly that we must be mindful of losing much of the already demonstrated benefits if we are not cognizant of the complexity of the ecosystem we have created, its structure and players in it.

* * *

Sulla governance di Internet

Riassunto: Questo saggio si propone di analizzare la complessa sfida di introdurre misure di governance volte a preservare l'efficienza del sistema Internet e garantire la sicurezza dei cittadini, sanzionando coloro che approfittano delle possibilità offerte dall'accesso a Internet per commettere abusi.

Parole chiave: Applicazioni basate su Internet – Ecosistema di Internet – Attività umane e potenziali rischi in Internet

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0052

In principio era Internet e lo immaginavamo diverso

Guido Scorza

Nel ripercorrere l'evoluzione di Internet si esamina il rapporto tra diritto e tecnologia, tra Stato e nuovi poteri privati. All'entusiasmo iniziale di un'Internet aperta e libera si è sostituita l'amara constatazione che la dimensione digitale è composta da giardini privati, ciascuno presidiato da pochi grandi soggetti privati. Nel prendere atto che i problemi di domani saranno quelli di ieri, non resta che mettere in pratica gli insegnamenti, spesso rimasti inascoltati, del Maestro Stefano Rodotà.

Rodotà – Internet – Diritto – Metaverso – Piattaforme digitali

In principio era Internet e lo immaginavamo aperto, libero, accessibile a tutti, inarrestabile strumento di informazione, partecipazione, concorrenza e democrazia.

Ed è stato, probabilmente, per questo che, per interi lustri, ad ogni bivio, tra regolamentare o non regolamentare in maniera stringente l'ecosistema digitale che cresceva e si sviluppava attorno a quella rete che chiamavamo Internet, i più di noi suggerivano, senza esitazione, la strada della deregulation.

"La tecnologia è neutra", continuavamo a scrivere e ripetere, tocca agli uomini decidere come utilizzarla e riuscire a orientarla alla massimizzazione del bene comune nell'interesse dei più.

In pochi – e, tra questi, quel gigante visionario del diritto e della democrazia che era Stefano Rodotà – non si stancavano di ripetere che le regole, se sono quelle giuste, servono a garantire le libertà e che, quindi, non c'era ragione per aver paura di regolare le tecnologie e, anzi, bisognava trovare il coraggio di farlo, naturalmente, in maniera moderna, illuminata, partecipata e democratica.

Niente regole di dettaglio, una regolamentazione per principi costruita attorno ai diritti fondamentali da affermare, riconoscere, garantire e far rispettare anche e soprattutto nella dimensione digitale.

Per governare l'ecosistema digitale sarebbe stato necessario un *Internet bill of rights*.

E, forse, avremmo dovuto seguire più convintamente quei suggerimenti, forse avremmo dovuto avere più fiducia nelle regole e meno paura, forse avremmo dovuto credere meno al sogno di tecnologie capaci di liberarci dal gioco di un sistema mediatico oligopolistico che, per decenni, aveva attentato alla democrazia – in Italia più che altrove – e ridotto interi Paesi in una condizione di drammatica semi-libertà e tele-dipendenza.

Ma vedevamo nel Web la prima – e forse l'ultima – speranza di rivincita per chi di quel sistema mediatico era stato spettatore passivo e, invece, con il Web, avrebbe potuto diventare produttore di contenuti, creatore di informazioni, partecipante attivo alle discussioni globali.

Troppo facile, probabilmente, oggi, dire che ci sbagliavamo.

Troppo facile perché Internet, che ieri ci appariva una serie di sconfinate praterie accessibili a chiunque si è, ormai, rivelata come una successione ininterrotta di giardini privati, ciascuno presidiato da porte scorrevoli che si aprono istantaneamente in entrata ma restano poi chiuse in uscita, giardini che sanno attrarci, conquistarci, catturarci e che, poi, quasi fos-

G. Scorza è componente del Garante per la protezione dei dati personali.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

sero popolati dalle Sirene figlie del dio Acheloo e di Melpomene, nelle quali si imbatté Ulisse sulla strada di Itaca ci seducono e tengono prigionieri.

Qualcosa è andato storto, qualcosa non ha funzionato come i più avevano immaginato avrebbe funzionato o, forse, semplicemente, abbiamo sopravvalutato la forza democratica di certe tecnologie e sottovalutato la potenza egemonica dei mercati.

Nel volgere lo sguardo al passato, a cinque anni dalla scomparsa di Stefano Rodotà, il Maestro con il quale in tanti, in Italia e nel resto del mondo, abbiamo un incolmabile debito di riconoscenza per averci indicato – talvolta ascoltato, più spesso inascoltato quasi, per restare alla mitologia greca, le sue fossero le urla di Cassandra nelle notti di Troia – dobbiamo prendere atto che i problemi di oggi e quelli di domani sono e, verosimilmente, resteranno quelli che avremmo, con più energia, coraggio, lungimiranza e saggezza dovuto affrontare e risolvere ieri.

Difficile pensare che il metaverso, erede di Internet nel quale Mark Zuckerberg ci ha, da poco, anticipato stiamo per immergerci, sarà diverso dall'ecosistema digitale nel quale viviamo.

E, se così sarà, allora, è facile, questa volta – salvo non voler ignorare ancora le lezioni di Rodotà e, oggi, anche quelle della storia – identificare il maggiore tra questi problemi nella circostanza che una manciata di piattaforme gestite da una manciata di fornitori di servizi privati sono, ormai, divenute autentiche città-Stato nelle quali oltre la metà della popolazione globale vive la propria quotidianità.

Ma non siamo cittadini di queste città-Stato, non partecipiamo, attraverso dinamiche democratiche al loro governo, ne siamo semplicemente utenti, ci viviamo in una condizione di libertà condizionata, vincolata, circoscritta e perimetrata per contratto.

Possiamo agire o non agire, parlare o non parlare, condividere o non condividere questo o quel contenuto, idea o opinione nei limiti in cui ciò ci è consentito dai termini d'uso che abbiamo accettato – normalmente senza neppure leggerli – il primo giorno in cui siamo entrati in queste piattaforme attratti e sedotti dall'usabilità delle loro interfacce e dalla straordinaria utilità che promettevano di regalarci e che, in effetti – guai a negarlo – ci hanno garantito, anche se non esattamente regalato, sin qui e, probabilmente, continueranno a garantirci negli anni che verranno.

Queste piattaforme-città-Stato sono, ormai, diventate autentiche *essential facilities* della nostra vita in tutte le sue dimensioni, pubbliche e private.

L'ultima, certamente non la più importante conferma – per quanto empirica, superficiale, più simbolica che non sostanziale – di questa situazione è, probabilmente, rappresentata dalla decisione di Facebook, in uno dei moment più difficili della sua esistenza, mentre è sotto attacco da parte dei decisori pubblici e regolatori di mezzo mondo, di annunciare il suo cambio di nome in Meta, anticipando, contestualmente, al mondo che sta per ritrovarsi immerso nel Metaverso.

Zuckerberg, qui, ricorda un po' Alessandro Magno che chiama Alessandria d'Egitto la città che fonda.

Difficile, anche solo a fermarsi al significato delle parole, pensare che Meta giocherà nel metaverso un ruolo marginale.

Nessun dubbio che Facebook ora Meta si stia, invece, candidando – certamente non da sola – a giocare un ruolo determinante, diverso ed ulteriore rispetto a quello di una semplice società commerciale grande quanto si vuole, nel metaverso che verrà.

In questo contesto, probabilmente, i più grandi problemi di tutela dei diritti che abbiamo all'orizzonte sono analoghi a quelli di oggi ma di molti ordini di magnitudine superiore: come si fa e come si farà a garantire la sostenibilità sociale, culturale, economica e democratica della vita delle persone in un mondo che sarà letteralmente creato da una manciata di soggetti privati che lo governeranno – come in buona parte fanno già oggi – imponendo ai cittadini-utenti le loro regole attraverso i termini d'uso dei loro servizi e piattaforme e rendendone *ex ante* impossibile anche la semplice violazione attraverso invincibili algoritmi?

Ma sbaglieremmo se ci abbandonassimo a un *j'accuse* verso questi soggetti privati che, credo, abbiano giocato la loro partita nel migliore dei modi possibile dal punto di vista loro, dei loro azionisti e delle regole del gioco.

I destinatari del *j'accuse*, semmai, dovremmo essere noi, i decisori e regolatori pubblici di mezzo mondo, dapprima, arrivati in ritardo a capire quello che stava accadendo e, quindi, incapaci di trovare soluzioni migliori e più efficaci, per recuperare il ritardo, rispetto a quella di imputare a questi soggetti privati sempre più responsabilità in relazione ai contenuti veicolati dai loro utenti e chiedere loro e, anzi, talvolta imporre loro di fare sempre di più per "tenere pulito" l'ecosistema digitale.

Per questa via, infatti, si è lasciato che le c.d. GAFAM (Google, Apple, Facebook, Amazon e Microsoft) acquisissero sempre più poteri, spesso anche poteri para-statuali che avrebbero dovuto, in una visione sana della democrazia, restare appannaggio esclusivo degli Stati per quanto difficile avrebbe potuto – e potrebbe – risultare esercitarli nel quotidiano.

C'è da rimuovere un contenuto pubblicato da qualcuno in violazione dei diritti d'autore di qualcun altro o, addirittura, di impedirne preventivamente la pubblicazione?

Se ne occupa YouTube.

E pazienza, se, magari, quel contenuto avrebbe potuto, in realtà, essere pubblicato in virtù di una delle tante libere utilizzazioni previste dalla legge sul diritto d'autore e averne impedito la pubblicazione ha fatto sì che il mondo non abbia mai potuto confrontarsi con una storia, un'opinione o un'idea che lo avrebbe invece consentito.

Pazienza se un Giudice o un'Autorità, magari, avrebbero amministrato giustizia in maniera più bilanciata.

Online, a distanza di anni, continuano a "galleggiare" contenuti che parlano del passato di un uomo in toni poco lusinghieri che il protagonista ritiene incompatibili con il suo preteso diritto assoluto a voltar pagina e a che la società si dimentichi di alcuni episodi del suo passato?

Nessun problema, basta compilare un modulo online e sarà direttamente Google a decidere se il c.d. diritto all'oblio del singolo deve prevalere o meno sul diritto della collettività a essere informata, sul diritto di cronaca e, magari, talvolta, sul diritto alla storia.

E pazienza se, magari, per questa strada, per evitare ogni responsabilità, Google nel dubbio dovesse decidere di disindicizzare anche un contenuto che, invece, avrebbe meritato di continuare a essere indicizzato.

E pazienza se, per questa strada, se si interroga Google da Milano si ha una visione della storia diversa da quella che si ha interrogandolo da Lugano appena una manciata di chilometri più a nord, perché Google de-indicizza un contenuto per gli utenti che l'interrogano da un certo Paese ma non per quelli che lo interrogano dall'estero.

Le parole d'odio imperversano sui social – come, peraltro, imperversano da una vita nella società – e questo disturba molti?

Nessun problema basta ritenere Facebook responsabile di quei contenuti per ottenere che quest'ultimo si dia da fare per rimuoverne quanti più possibile.

E pazienza se in quest'ansia da rimozione si finiscano per rimuovere anche contenuti che avrebbero potuto legittimamente rimanere online perché esercizio della libertà di parola di qualcuno.

All'improvviso, nella dimensione digitale, si è ritornati indietro nel tempo.

Niente più diritti fondamentali, niente più diritto a un giusto processo, niente più giustizia terza, imparziale e in contraddittorio.

Il fine giustifica i mezzi e, quindi, meglio la pseudo-giustizia imperfetta ma più o meno veloce dei gestori delle piattaforme private che quella dei Tribunali e delle Autorità.

È la brutta china che abbiamo preso.

Lo testimonia in tutta la sua drammaticità la decisione dei social network di mettere alla porta, nel gennaio del 2021, addirittura Donald the Trump, all'epoca – anche se ancora solo per qualche giorno – Presidente in carica degli Stati Uniti d'America, il rappresentante, democraticamente eletto fino a prova contraria, della maggiore super potenza democratica.

Una manciata di società private, dalla sera alla mattina, hanno deciso che quel signore non aveva più diritto di parola attraverso i loro servizi e lo hanno, semplicemente, silenziato.

Si è trattato di un autentico ostracismo digitale, in tutto e per tutto analogo a quello che, un tempo, colpiva i soggetti più pericolosi per la democrazia greca con la sola vistosa differenza che, all'epoca, l'ostracismo era disposto dal popolo, in maniera democratica mentre, nel caso di Trump, lo hanno deciso i vertici di due o tre società quotate in borsa.

Ma il passato, questo passato, è niente rispetto al futuro che ci aspetta se non si inverte la tendenza.

Domani, infatti, con l'Internet delle cose che avanza e il metaverso nel quale ci immergiamo sarà sempre più ampio il novero delle attività che potremo fare o non fare solo, o, almeno, prevalentemente, grazie all'intermediazione dei grandi fornitori di servizi digitali.

E, a quel punto, che si tratti di farci entrare in una banca se un algoritmo sospetta che noi si sia malintenzionati o di tenere chiuso la porta di casa se siamo in ritardo con il pagamento dell'affitto, ovunque la pseudogiustizia privata delle piattaforme potrà imporre le sue regole e farle rispettare.

Ma davvero vogliamo vivere in una società nella quale i protagonisti dei mercati hanno un ruolo tanto rilevante nelle nostre vite e lo Stato ne ha uno tanto marginalizzato solo perché i primi sono più veloci e efficienti nel raggiungere il risultato?

La risposta corretta, quella che probabilmente Stefano Rodotà ci suggerirebbe di dare è, naturalmente, negativa.

Se si vuole fare in modo che il futuro, nel metaverso, sia migliore del presente e del passato in Internet e se si vuole scongiurare il rischio di tornare a commettere errori che si sono, probabilmente, commessi in passato è necessario far tesoro, almeno ora, delle tante lezioni di Stefano Rodotà: regolamentare per garantire le libertà e i beni comuni anche nella dimensione digitale, farlo fissando principi più che regole di

dettaglio, guardare alla dimensione sovranazionale più che a quella nazionale, non dimenticarsi mai di mettere l'uomo al centro, in tutte le sue dimensioni, e non scordare mai che ciascuno di noi deve avere gli stessi diritti – almeno quelli fondamentali – online, in Internet, nella dimensione digitale, nella realtà virtuale, in quella aumentata o nel metaverso che verrà.

Lo Stato, probabilmente, deve riappropriarsi di ruoli che, in democrazia, non possono essere "delegati" a soggetti privati: primi tra tutti quelli di dettare le regole della civile convivenza anche nella dimensione digitale e di amministrare la giustizia.

E pazienza se, considerata l'entità dei fenomeni che si consumano nell'ecosistema digitale, talvolta la risposta potrebbe arrivare in ritardo o, almeno, in maniera meno celere di quanto accadrebbe lasciando la risposta affidata ai soggetti privati.

Ai fornitori di servizi tecnologici occorre che gli Stati chiedano risorse economiche e tecnologiche per garantire che i più possano approfittare delle straordinarie opportunità offerte dalle loro piattaforme senza pregiudicare la sostenibilità sociale e democratica della nostra esistenza.

Ma come si raggiunge questo risultato? Come si evita, nel metodo prima che nel merito, di tornare a commettere errori che si sono già commessi?

Con soggetti che hanno raggiunto le dimensioni economiche raggiunte dai soggetti dei quali stiamo parlando – Facebook ora Meta da sola ha una capitalizzazione pari, più o meno, al doppio del PIL italiano – e hanno assunto il ruolo che hanno assunto nelle nostre democrazie serve, probabilmente, immaginare sistemi di regolamentazione completamente diversi da quelli utilizzati sin qui, sistemi non convenzionali, più simili a quelli che si usano per disciplinare i rapporti tra Stati che a quelli che si usano per regolamentare i mercati.

Non ci sono ricette miracolose per governare il presente e il futuro, in particolare, nella dimensione digitale ma c'è una stella polare da seguire senza esitazioni: quella dei diritti fondamentali.

La scelta giusta, a ogni bivio, sarà sempre quella che garantisce di più quel novero straordinario di diritti, caro sopra a ogni altro a Stefano Rodotà, che plasma la nostra esistenza umana, la nostra natura e quella delle nostre democrazie.

* * *

In the beginning was the Internet and we thought it was different

Abstract: Once upon a time Internet meant freedom. Then it became a big place of walled gardens where States gave powers to "big tech" platforms. Nowadays we know that the issues of yesterday will be the same of tomorrow and we should learn from our mistakes and starting to listen, more than in the past, Stefano Rodotà's lessons regarding how to regulate Internet.

Keywords: Rodotà – Internet – Law – Metaverse – Digital platforms

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0057

Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet

Gianpaolo Maria Ruotolo

Il lavoro analizza le proposte di riforma della responsabilità dei fornitori di servizi su Internet alla luce di Digital Services e Digital Markets Act dell'Unione europea soffermandosi anche, in particolare, al profilo delle misure preventivamente adottabili in materia antitrust e ai rischi di doppia punizione, con conseguente violazione del *ne bis in idem*.

Servizi – Responsabilità – Fornitori – Diritto UE – *Bis in idem*

Sommario: *1. Il regime europeo della responsabilità dei fornitori di servizi di hosting – 2. La proposta di disciplina contenuta nel Digital Services Act (DSA) – 3. La proposta di disciplina contenuta nel Digital Markets Act (DMA) – 4. . . . e i suoi rischi di* bis in idem *in materia antitrust – 5. Alcune brevi considerazioni conclusive*

1. Il regime europeo della responsabilità dei fornitori di servizi di hosting

Il 15 dicembre 2020 la Commissione europea ha presentato un pacchetto di misure per aggiornare la disciplina UE del settore digitale, distinte in due proposte di adozione di atti di diritto derivato, sontuosamente definiti "Acts".

Il regolamento Digital Services Act (DSA)[1] mira a regolare la sicurezza, la trasparenza e le condizioni di accesso ai servizi online e, di conseguenza, a modificare la direttiva 2000/31/CE[2].

Il regolamento Digital Markets Act (DMA)[3], su cui svilupperemo alcune considerazioni *infra*, nel par. 3, si occupa invece degli aspetti commerciali e di concorrenza.

Entrambi si vanno ad aggiungere alla proposta, già adottata, di un Data Governance Act (DGA), del 25 novembre 2020[4], che ha l'obiettivo di promuovere la disponibilità dei dati e a rafforzare la fiducia nei confronti dei c.d. intermediari, nonché di potenziare strumenti e meccanismi di condivisione dei dati stessi, in particolare con riguardo al riutilizzo dei medesimi da parte del settore pubblico e alla loro condivisione tra imprese[5]. Va pure ricordato che nella regolamentazione del mercato digitale, poi, gioca un ruolo determinante anche quello della tassazione dei proventi delle imprese che in tale mercato operano[6] e che successivamente, nell'aprile 2021, la Commissione, sempre nell'ottica di completare la disciplina delle fattispecie, in particolare se rilevanti per aspetti commerciali, ha anche avviato una procedura di adozione di un regolamento del Parlamento europeo e del Consiglio per stabilire regole armonizzate sull'intelligenza artificiale[7].

Tutte queste proposte sono collegate tra loro e si inseriscono nell'ampio framework predisposto dalla Comunicazione della Commissione del

G.M. Ruotolo è professore ordinario di Diritto internazionale presso il Dipartimento di giurisprudenza dell'Università di Foggia. Il presente scritto costituisce una versione leggermente modificata di una relazione presentata dall'Autore a un Convegno di studi organizzato dall'Università di Macerata e destinata a: G. Caggiano, G. Contaldi, P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2022.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

19 febbraio 2020 "Plasmare il futuro digitale"[8] e, quindi, complessivamente, all'interno delle politiche per la promozione della c.d. "sovranità digitale" dell'Unione[9].

Ricordiamo che con quest'ultima espressione, a volte resa anche con "sovranità tecnologica", si fa riferimento alla capacità dell'Unione (e dei suoi Stati membri) di agire in modo indipendente nel mondo digitale con strumenti sia difensivi sia offensivi, per promuovere l'innovazione e proteggersi, al contempo, dall'influenza economica e sociale di imprese tecnologiche extra-UE che, secondo alcuni, starebbero mettendo in pericolo non solo il controllo dei cittadini europei sui loro dati personali, ma, soprattutto, starebbero ponendo freni alla crescita delle imprese hi-tech europee e addirittura limitando la capacità dei legislatori nazionali e dell'UE di garantire l'*enforcement* delle proprie normative relative a fattispecie digitali, appunto[10].

In questo contesto si inserisce la regolamentazione della responsabilità dei fornitori di servizi di hosting[11] per i contenuti caricati dai loro utenti (il c.d. *user generated content*, appunto), di particolare rilevanza, anche in considerazione della massiva diffusione dei social media e dei rischi connessi[12].

Ricordiamo che la direttiva e-commerce[13], agli articoli 14 e 15, proprio con riferimento al contenuto caricato dagli utenti sulle piattaforme di condivisione online, prevede che il fornitore del servizio non sia responsabile delle informazioni così memorizzate, chiarendo che l'esenzione in parola non si applica solo nel caso in cui il fornitore, non limitandosi al mero trattamento tecnico e automatico dei dati forniti dal cliente, abbia svolto sugli stessi un ruolo attivo e "di merito", prestando all'utente assistenza, volta ad esempio all'ottimizzazione della presentazione dei contenuti o, ancora, se il fornitore, seppur limitandosi alla fornitura neutra del servizio, dovesse essere comunque a conoscenza di fatti e circostanze tali da rendere manifesta l'illegalità dell'attività o dell'informazione condivisa.

Peraltro, il 31 maggio 2016 la Commissione, in applicazione della decisione quadro 2008/913/GAI[14] e dell'art. 16 della stessa direttiva e-commerce, ha finanche promosso un Codice di condotta per il contrasto all'illecito incitamento all'odio online, sottoscritto dai principali operatori privati di servizi online (tra gli altri, Google, Instagram, Snapchat, Dailymotion, Facebook, Twitter, Microsoft, YouTube).

Il Codice contempla l'impegno delle imprese che vi hanno aderito di predisporre procedimenti chiari ed efficaci di esame rapido delle segnalazioni relative a discorsi d'odio che possano condurre alla rimozione tempestiva dei contenuti illegittimi; le stesse imprese, peraltro, si impegnano a dotarsi di linee guida che vietino chiaramente la promozione e l'istigazione alla violenza e alla condotta odiosa, ad esaminare le richieste di rimozione nel rispetto tanto delle linee guida così adottate quanto della pertinente normativa nazionale di recepimento della suddetta decisione quadro, mediante gruppi di lavoro a ciò specificamente deputati, e a far ciò entro ventiquattr'ore dalla conoscenza dell'illecito[15].

Ricordiamo pure che la Direttiva sul diritto d'autore nel mercato unico digitale[16], all'art. 17, par. 3, prevede esplicitamente che quando il prestatore di servizi di condivisione di contenuti online effettui un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico che rientri nell'ambito d'applicazione della direttiva e alle condizioni stabilite dalla stessa, di materiale caricato da utenti, la limitazione di responsabilità di cui all'art. 14, par. 1 della direttiva e-commerce non trova applicazione con riguardo ai profili relativi alla violazione di diritti di proprietà intellettuale[17].

La Corte di giustizia si è pronunciata in più occasioni sulle condizioni di esenzione dalla responsabilità di cui alla direttiva e-commerce chiarendo come la stessa debba essere applicata al fornitore di servizi di hosting che non abbia svolto un ruolo attivo che gli abbia consentito di conoscere il contenuto materiale o assumere il controllo dei dati memorizzati.

Pertanto se il fornitore non ha svolto siffatto ruolo non può essere ritenuto responsabile per i dati che ha memorizzato su richiesta di un utente, salvo che, essendo comunque venuto a conoscenza della natura illecita di tali dati o dell'attività dell'inserzionista, non abbia omesso di rimuoverli prontamente o disabilitare l'accesso agli stessi[18].

Ancora, la Corte, affermando pure l'inesistenza di un obbligo *generalizzato* di controllo sui contenuti, ha poi chiarito che l'esenzione in parola si applica anche ai gestori che non svolgono alcun ruolo attivo che gli permetta di avere conoscenza o controllo circa i dati memorizzati; si ricade invece nel caso di "ruolo attivo", con la conseguente inapplicabilità dell'esenzione, allorché il gestore fornisca ai suoi utenti un'assistenza volta ad ottimizzare la presentazione.

Peraltro, sempre secondo la Corte, anche in assenza di siffatto ruolo attivo, il prestatore di servizi online non potrebbe comunque avvalersi dell'esonero dalla responsabilità qualora sia stato al corrente di fatti o circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità delle inserzioni dei suoi clienti e, nell'ipotesi in cui ne sia stato al corrente, non abbia prontamente agito[19].

I giudici di Lussemburgo hanno anche chiarito che nel caso in cui il fornitore non agisca di propria ini-

ziativa per sospendere l'utente che viola i diritti di proprietà intellettuale in modo da impedirgli di commettere ulteriori violazioni, i tribunali nazionali possono ingiungergli di prendere tutte le misure necessarie non solo a far cessare le violazioni già commesse, ma anche a prevenirne di ulteriori, a condizione che tali misure siano effettive, proporzionate, dissuasive e non creino illegittimi ostacoli al commercio intra-UE[20].

Va, infine, quanto meno accennato che, in merito alla responsabilità del provider per i contenuti illegittimi caricati da terzi si è pronunciata anche la Corte europea dei diritti dell'uomo, la quale, tracciando così una sorta di linea comune di condotta europea, ha ritenuto che il gestore di un sito web con finalità commerciali possa essere legittimamente sanzionato per la diffusione e la mancata rimozione di contenuti lesivi della reputazione altrui qualora non abbia posto in essere un'attività *neutra* e meramente *tecnica*, in quanto unico detentore del controllo sui contenuti pubblicati[21].

2. La proposta di disciplina contenuta nel Digital Services Act (DSA)

Negli ultimi anni, peraltro, i servizi di hosting – anche a causa, come accennavamo prima, dell'avvento e dalla enorme diffusione dei social network, che ormai svolgono funzioni analoghe, consentendo ai loro utenti di caricare contenuti multimediali – hanno mutato radicalmente le loro caratteristiche, e i relativi fornitori hanno aumentato esponenzialmente i servizi che offrono, che, oggi, vanno ben oltre la mera messa a disposizione di spazio per caricare contenuti, i quali vengono invece organizzati dagli stessi fornitori per migliorarne la fruizione (si pensi, ad esempio, alle funzioni di ricerca e indicizzazione o ai "canali" di YouTube).

Al riguardo si è parlato di servizi di *hosting 2.0*.

È pure il caso di ricordare come, con specifico riferimento all'ordinamento italiano, proprio in merito all'applicazione dell'esenzione di responsabilità di cui alla direttiva e-commerce al contesto degli *host 2.0*, si siano radicati, negli anni passati, due orientamenti giurisprudenziali opposti.

Secondo il primo, le caratteristiche evolute di cui abbiamo appena detto sarebbero una conseguenza quasi ontologica dello sviluppo tecnologico in generale e di quello dei servizi di hosting in particolare, i cui fornitori, quindi, continuerebbero a beneficiare dell'esenzione per i contenuti illegittimamente caricati da terzi, almeno finché il titolare di diritti lesi non comunichi loro puntualmente quali contenuti siano caricati in violazione delle sue posizioni giuridiche, o qualora vi sia un ordine di rimozione della pubblica autorità non eseguito[22].

Alla luce del secondo orientamento, più oneroso per i fornitori, invece, le caratteristiche dei nuovi servizi di hosting impedirebbero, per così dire ontologicamente, di poter continuare a considerarli *neutrali*, *passivi* e *meramente tecnici* rispetto ai contenuti che veicolano e, di conseguenza, sebbene gli host, come detto, non siano onerati, per ciò solo, di un obbligo generale di sorveglianza sui contenuti caricati dagli utenti, proprio in conseguenza dell'organizzazione e sistematizzazione dei contenuti (attività che presuppongono la conoscenza del merito dei contenuti) il titolare dei diritti lesi può limitarsi a rivolgere loro una generica richiesta di rimozione, la quale cioè non deve necessariamente contenere l'indicazione puntuale dei contenuti illegittimamente caricati e quindi da rimuovere[23].

È in questo complesso contesto che si inserisce la disciplina contenuta nella proposta di regolamento DSA, che, in particolare, mira a rivedere le regole che disciplinano proprio lo *user generated content* e la relativa responsabilità dei fornitori con riferimento ai profili relativi a violenza, fake news, hate speech, *et similia*, nonché alle violazioni dei diritti di proprietà intellettuale.

A tal fine il DSA crea "categorie" di fornitori di servizi digitali e gradua, di conseguenza, la loro responsabilità, anche (e proprio) in base alle loro capacità di conoscenza dei contenuti caricati dagli utenti.

La proposta pare sviluppare, senza però, va detto, innovare in maniera rivoluzionaria, i concetti già contemplati dal diritto UE che abbiamo illustrato[24].

Ai medesimi, però, vengono conferiti gli effetti tipici delle norme contenute in un regolamento (effetti diretti e prevalenza sul diritto interno incompatibile) con l'intento di eliminare distorsioni applicative nei vari Paesi e, quindi, rafforzarne la certezza: la proposta, infatti, pur abrogando gli articoli da 12 a 15 della direttiva e-commerce, li riproduce, mantenendo così le esenzioni dalla responsabilità per tali prestatori, conformemente all'interpretazione già datane dalla Corte di giustizia, e continua così a distinguere tra i meri provider per così dire tradizionali, i quali cioè forniscono solo servizi di connettività e archiviazione e che quindi hanno scarse o nulle capacità di moderazione dei contenuti diffusi dai loro clienti, dai fornitori *2.0* di cui abbiamo accennato che, invece, hanno capacità di conoscenza – e quindi di moderazione – ben più penetranti, e aggrava la responsabilità di questi ultimi.

Il DSA, quindi, impone esclusivamente ai fornitori di quest'ultimo gruppo una serie di penetranti obblighi di rimozione rapida dei contenuti illegali –

rendendo così vincolante quanto da molti di loro già volontariamente accettato con i Codici di condotta, in particolare quello relativo alla lotta ai discorsi d'odio di cui abbiamo detto, i cui obblighi però vengono resi applicabili anche a fattispecie differenti – e nuove responsabilità, tra cui quella di garantire alle istituzioni pubbliche la possibilità di sottoporre a un esame approfondito i loro dati interni, nonché l'obbligo di produrre annualmente un rapporto sullo stato di rischio dei loro servizi e di nominare un responsabile esterno e indipendente che verifichi il rispetto di tutte queste regole da parte loro.

La graduazione degli oneri in funzione delle capacità dei singoli fornitori, oltre a rappresentare un'incorporazione di orientamenti giurisprudenziali consolidati, peraltro, rappresenta una estrinsecazione del principio di proporzionalità.

Un altro passaggio del draft proposto dalla Commissione impone poi ai fornitori di servizi online l'obbligo di fornire ai loro utenti "informazioni significative" (anche se è poco chiaro cosa ciò voglia significare) sui meccanismi che regolano la pubblicità online e, in particolare, sugli algoritmi di profilazione che decidono in tempo reale quale specifica inserzione mostrare loro.

Da quanto appare, insomma, il regolamento DSA non pare ribaltare *upside-down* la regolamentazione UE della responsabilità dei fornitori di servizi online per i contenuti caricati dai loro utenti, quanto, più semplicemente, razionalizzarla nel rispetto di criteri e principi pregressi, di elaborazione prima giurisprudenziale e poi inseriti in strumenti regolatori già in vigore, come, ad esempio la già citata direttiva sul commercio elettronico o quella sul diritto d'autore nel mercato unico digitale.

3. La proposta di disciplina contenuta nel Digital Markets Act (DMA)

Passando ora, velocemente, al regolamento DMA, esso, avendo come obiettivo quello di rilanciare la competitività delle aziende europee in un settore dominato in larga misura da imprese statunitensi, va ad individuare le imprese c.d. *gatekeeper*.

Con questa espressione il regolamento fa riferimento a quelle imprese che godono di una particolare posizione di rilevanza e che, per questo, possono sollevare barriere all'ingresso di nuove aziende su un determinato mercato (si pensi ai mercati, tra loro distinti e autonomi, del social networking, del cloud computing, della messaggistica, dello streaming, e così via...).

Secondo il progetto della Commissione saranno quindi considerate tali, in base a un criterio quantitativo, le imprese che in un anno fatturano in UE almeno 6,5 miliardi di euro o che hanno almeno 45 milioni di utenti tra i cittadini dell'Unione, nonché, con un criterio invece di tipo qualitativo, quelle, anche se di dimensioni minori, che detengono posizioni di particolare rilevanza su mercati specifici.

Tutte saranno soggette a regole "preventive", volte a impedir loro di adottare comportamenti anticompetitivi: tali regole – e questa pare essere una delle innovazioni del pacchetto proposto, che però potrà essere valutata compiutamente solo dopo la sua approvazione definitiva – sono volte, ancor prima che a sanzionare *ex-post* le violazioni del diritto della concorrenza (le quali sono comunque possibili e sanzionabili autonomamente ai sensi delle relative norme previste dai Trattati), ad impedire preventivamente comportamenti anticoncorrenziali. I *gatekeeper*, infatti, non potranno promuovere esclusivamente i propri servizi o favorirli a discapito di quelli altrui, ciò che, invece, avviene attualmente: le aziende che gestiscono gli *store* di app saranno ad esempio obbligate a garantire la parità di trattamento ai prodotti dei concorrenti, anche consentendo l'utilizzo di sistemi di pagamento e di abbonamento diversi dai loro.

Ora, sotto quest'ultimo profilo, va ricordato come la prassi interna, anche extraeuropea, stia registrando interessanti sviluppi: il 3 maggio 2021, infatti, si è aperto negli Stati Uniti, davanti alla United States District Court for the Northern District of California, un processo antitrust di rilevanza ben più che meramente statunitense, che vede affrontarsi *Epic Games*, lo sviluppatore di videogiochi che ha creato il notissimo gioco online *Fortnite*, e la Apple: a partire dall'agosto 2020 *Epic*, infatti, ha cercato di invogliare, con una politica di forti sconti, i giocatori di *Fortnite* su iPhone ad effettuare i loro acquisti in-game direttamente sul suo sito anziché mediante l'Apple Store, che trattiene a suo beneficio il 30% delle transazioni concluse per il suo tramite.

Per tutta risposta Apple ha radiato *Fortnite* dal suo store, e *Epic*, ritenendo che ciò costituisse un abuso di Apple della sua posizione di dominio sul mercato, oltre ad avviare una campagna pubblicitaria massiva con la quale ha invitato i suoi giocatori a *#FreeFortnite*, ha citato quest'ultima in giudizio[25].

E va pure detto che le cose non vanno meglio per la casa della mela al di qua dell'oceano: il 30 aprile 2021, infatti, la Commissione europea, in un suo *Statement of Objections* ha determinato che, a suo giudizio, Apple starebbe violando anche il diritto UE della concorrenza, stavolta però nei confronti di *Spotify*, il noto servizio di streaming musicale, che, non dissimilmente da *Epic*, si è lamentato della fetta eccessiva di incassi prelevata dalle sue transazioni avvenute

tramite l'Apple Store[26]. Apple, infatti, non applica la medesima politica a tutti i fornitori che ospita sul suo store: Amazon, ad esempio, non paga la stessa, altissima, commissione sugli acquisti in-app per la sua applicazione di streaming Prime Video; Apple, peraltro, applica una commissione del solo 15% per gli sviluppatori minori, quelli che fatturano meno di 1 milione di dollari all'anno, adottando così una politica differenziata rispetto ai concorrenti più forti.

La società di Cupertino si difende da sempre dalle accuse di abuso della sua posizione di dominio sui mercati digitali sostenendo che l'imposizione di una commissione pari a un terzo delle transazioni concluse dai maggiori fornitori grazie al suo negozio digitale rappresenterebbe un corrispettivo equo per le enormi somme di denaro che la stessa ha investito per mettere in piedi e continua a spendere per gestire l'Apple Store e che, comunque, il mercato offre certamente alternative percorribili ed efficaci allo stesso, come, ad esempio, quello di Google.

Va detto che la definizione del ruolo giocato da Apple e dal suo store online sui mercati digitali dipenderà da come chi dovrà decidere, al di qua e al di là dell'Atlantico. riterrà di definire il mercato rilevante dello store stesso, cioè la fetta di mercato sul quale l'azienda detiene e sul quale esercita il suo potere di controllo. E non si tratta affatto di una questione semplice o dalla soluzione scontata: qualche tempo fa la Commissione europea, come noto, aveva ritenuto che il Messenger di Facebook e WhatsApp, due applicazioni di messaggistica, non fossero tra loro in concorrenza dal momento che gli utenti ne fanno un uso differente.

4. . . . e i suoi rischi di *bis in idem* in materia antitrust

Quanto all'impianto punitivo proposto nel contesto DMA per la violazione di questi obblighi, esso appare piuttosto severo, contemplando sanzioni *una tanutm* fino al 10% del fatturato mondiale dell'azienda responsabile e sanzioni periodiche fino al 5% del fatturato globale giornaliero, con il loro aggravamento in caso di recidiva.

La disciplina in questione, tuttavia, rischia di andare a sommarsi alla possibilità che i medesimi comportamenti siano sanzionati anche *ex-post* ai sensi del diritto antitrust: ciò potrebbe porre problemi di compatibilità con il divieto di *bis in idem* che trova, con riguardo alla tutela della concorrenza, una forma di applicazione più morbida rispetto a quanto non avvenga in materia penale.

Il principio del *bis in idem*, infatti, assume caratteri peculiari, nel contesto dell'UE, quando applicato al sistema di diritto antitrust, in cui, in particolare l'elemento dell'"idem" viene interpretato in maniera diversa da quanto avviene nel contesto penale[27].

Nel caso del diritto antitrust la Corte di giustizia ritiene che tale elemento possa dirsi integrato solo in presenza di tre requisiti: identità del fatto, identità del contravventore e unicità dell'interesse giuridico tutelato dalle norme di cui si lamenta la violazione[28]. Sarebbe quest'ultimo elemento, infatti, a consentire di non applicare il principio del *bis in idem* – e di comminare legittimamente, quindi, una doppia sanzione – a tutti i casi in cui un *unico* comportamento del *medesimo* soggetto abbia comportato una riduzione della concorrenza *sia* sul mercato interno *sia* su un mercato nazionale, o su due o più mercati nazionali.

Secondo la Corte, infatti, il diritto antitrust UE e quello interno possono esser fatti oggetto di applicazione concorrente dal momento che le regole dell'Unione e quelle nazionali procedono a valutare le pratiche anticoncorrenziali sotto profili differenti: le autorità nazionali, ai sensi dell'art. 5 del regolamento n. 1/2003, possono quindi legittimamente comminare le sanzioni previste dal diritto nazionale, anche in presenza di sanzioni pregresse provenienti dalla Commissione[29].

La Corte, quindi, pur ricordando che il principio del *ne bis in idem* deve essere rispettato anche in materia antitrust, e che il medesimo «vieta, in materia di concorrenza, che un'impresa venga nuovamente condannata o perseguita per un comportamento anticoncorrenziale per il quale sia stata sanzionata o dichiarata non responsabile in forza di una precedente decisione non più impugnabile», ribadisce che, ai sensi dell'art. 50 della Carta dei diritti fondamentali dell'Unione europea, ciò riguarderebbe solo «la ripetizione di un procedimento conclusosi con una decisione definitiva riguardante il medesimo elemento materiale. Orbene, nella situazione in cui, ai sensi dell'articolo 3, paragrafo 1, seconda frase, del regolamento n. 1/2003, l'autorità nazionale garante della concorrenza procede ad un'applicazione parallela del diritto nazionale della concorrenza e dell'articolo 102 TFUE, è appunto assente siffatta ripetizione».

La dottrina ha criticato questa posizione della Corte, evidenziando come la stessa, portando ad interpretare il medesimo requisito in modo differente a seconda che ci si trovi in materia penale o antitrust, ne neghi la natura di diritto fondamentale e, in particolare nel secondo ambito, ne muti la funzione da strumento di garanzia in meccanismo repressivo[30].

La questione è giunta nuovamente all'attenzione degli operatori giuridici proprio in occasione dell'adozione, da parte della Commissione, della proposta di DMA: come è stato evidenziato[31], la disciplina in questione, infatti rischia di andare a sommarsi alla possibilità che i medesimi comportamenti già sanzionati dal DMA, siano sanzionati anche *ex-post* ai sensi del diritto antitrust: ciò potrebbe porre problemi di compatibilità con il divieto di *bis in idem* proprio per il fatto che il medesimo trova, con riguardo alla tutela della concorrenza, una forma di applicazione più morbida rispetto a quanto non avvenga in materia penale.

5. Alcune brevi considerazioni conclusive

Proviamo ora ad individuare, seppur per sommi capi, alcune linee di tendenza che a nostro parere è possibile evidenziare nelle proposte normative che abbiamo esaminato.

Innanzitutto, in considerazione del fatto che è altamente probabile che i regimi ivi previsti siano applicati (anche) a soggetti che non necessariamente saranno *formalmente* stabiliti sul territorio dell'Unione europea, anche queste proposte si caratterizzano per una almeno potenziale applicazione extraterritoriale del diritto dell'Unione europea.

Si tratta di una linea di tendenza che, a nostro parere, con riguardo al settore digitale, è stata inaugurata dal Regolamento generale sulla protezione dei dati[32] il cui articolo art. 3, par. 2 ne contempla, come noto, l'applicabilità al trattamento dei dati personali di tutti gli individui interessati che si trovino nell'Unione, anche qualora effettuato da soggetti che non sono stabiliti nell'Unione, se tale trattamento riguarda: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Si tratta di una previsione che sta diventando una sorta di *template* normativo, spesso replicato, con i necessari adattamenti, in molti atti di regolamentazione del mercato unico digitale (come, ad esempio, già nel regolamento sui c.d. blocchi geografici[33]).

L'altra linea di tendenza che a nostro giudizio è individuabile in questo complesso normativo è quella che vede l'UE disciplinare le responsabilità degli intermediari, prima ancora che mediante l'imposizione di obblighi *materiali*, cioè di contenuto *sostanziale*, attraverso *norme di rito*, cioè attraverso un procedimento[34] il quale poi, più o meno indirettamente, impatta sulle questioni sostanziali.

Si tratta, anche in questo caso, di una tendenza più generale, che è rintracciabile anche in altri atti di disciplina di fattispecie digitali.

Peraltro, siffatta tecnica regolatoria risulta spesso accoppiata all'uso di strumenti giuridici non vincolanti (come i codici di autoregolamentazione di cui abbiamo detto) o comunque non riconducibili a fonti "formali": si tratta di un modello che è stato rintracciato anche nell'ambito della letteratura relativa al *global administrative law* o al cosiddetto diritto internazionale informale[35].

Ancora, anche con DSA e DMA, a noi pare, l'UE sta cercando di porsi come legislatore "di riferimento" globale, che costruisce *template* normativi che poi, si auspica, possano essere virtuosamente copiati anche da Stati e soggetti extra-UE: e non è un caso che, per cercare di incentivare la diffusione dei suoi modelli regolatori, molte norme adottate all'interno del diritto dell'Unione europea, in particolare per il settore digitale, vengano poi a volte replicate negli accordi commerciali che l'UE conclude con Stati terzi, in una logica quasi frattalica[36].

In conclusione dobbiamo però evidenziare come le brevi considerazioni qui sviluppate dovranno necessariamente essere riponderate alla luce del testo definitivo del DSA, la cui approvazione è prevista entro il 2023.

La proposta, infatti, nel corso della procedura legislativa ordinaria potrebbe subire modifiche anche rilevanti (come è già avvenuto in passato, ad esempio con riguardo alla più volte citata direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale), in conseguenza di un dibattito molto acceso, tanto a livello istituzionale quanto di opinione pubblica: si pensi, ad esempio, agli interessi che potrebbero muovere membri UE come il Lussemburgo o l'Irlanda, in cui risiedono molti degli operatori "Over the Top", o all'impatto che le misure proposte potrebbero avere sulla libertà d'espressione.

Note

[1] Doc. COM (2020) 825 final del 15 dicembre 2020.

[2] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[3] Doc. COM(2020) 842 final del 15 dicembre 2020.

[4] Doc. COM (2020) 767 final del 25 novembre 2020.

[5] Si v. G. Caggiano, *Il cantiere dell'armonizzazione fiscale per il Mercato unico digitale*, in "I Post di AISDUE", 30 luglio 2020.

[6] *Ibidem*.

[7]Doc. COM(2021) 206 final del 21 aprile 2021.

[8]European Commission, *Shaping Europe's digital future*, February 2020.

[9]Si veda al riguardo anche European Parliament, *Digital sovereignty for Europe*, July 2020.

[10]Si veda, al riguardo, tutta la "saga" delle cause promosse dall'attivista Maximilian Schrems dinanzi a corti interne e alla Corte di giustizia, il cui ultimo atto è rappresentato da CGUE, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, 16 luglio 2020, causa C-311/18. In dottrina v. G. Caggiano, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza Schrems II della Corte di giustizia*, in "Studi sull'integrazione europea", 2020, n. 3, pp. 563-585; C. Gentile, *La saga "Schrems" e la tutela dei diritti fondamentali*, in "Federalismi.it", 2021, n. 1, pp. 35-56; M. Nino, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in "Diritti umani e diritto internazionale", 2020, p. 730 ss.; I. Oldani, *The future of data transfer rules in the aftermath of Schrems II*, in "SidiBlog", 23 ottobre 2020.

[11]Ricordiamo che con quest'ultima espressione si fa riferimento a tutti quei servizi Internet in cui una macchina, detta server, offre le sue risorse per conservare e mettere a disposizione per l'accesso online, contenuti caricati dagli utenti; più in dettaglio, si è soliti distinguere il c.d. *web hosting* – il quale permette ad individui e organizzazioni di rendere il proprio sito web accessibile tramite il c.d. world wide web (www), da altre forme di hosting, come possono essere quelle video di *YouTube* o *Vimeo* o quelle audio di *SoundCloud* o quelle di condivisione di testi di *Scribd*, per fare qualche esempio. In questo contesto, come vedremo, è possibile fare ormai rientrare anche i social network.

[12]Su tali rischi, in particolare i pericoli di diffusione di discorsi d'odio e notizie false, anche solo per approfondimenti bibliografici ci permettiamo di rinviare a G.M. Ruotolo, A little hate, worldwide! *Di libertà d'opinione e discorsi politici d'odio on-line nel diritto internazionale ed europeo*, in "Diritti umani e diritto internazionale", 2020, n. 2, p. 592 ss.

[13]Direttiva 2000/31/CE, cit.

[14]Decisione-quadro 2008/913/Gai del Consiglio del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale.

[15]In dottrina si veda K. Podstawa, *Hybrid Governance or... Nothing? The EU Code of Conduct on Combating Illegal Hate Speech Online*, in E. Carpanelli, N. Lazzerini (eds.), "Use and Misuse of New Technologies", Cham, 2019, p. 167 ss.

[16]Direttiva 2019/790/UE del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

[17]Mediante la restrizione della limitazione di responsabilità del provider di cui all'art. 14, par. 1 della direttiva sul commercio elettronico, il legislatore dell'UE ha ristretto il margine d'apprezzamento e discrezionalità che fino ad allora era stato appannaggio della giurisprudenza nella valutazione casistica di tale rapporto. Ciò, di conseguenza, ha in qualche misura de-relativizzato (o, se si vuole, assolutizzato) il rapporto tra diritti di proprietà intellettuale e altri diritti ad essi formalmente pari ordinati. La norma in parola, infatti, impedendo il bilanciamento caso per caso, effettuato invece autoritativamente dal legislatore europeo, evidenzia una precisa scelta valoriale di quest'ultimo in favore della proprietà intellettuale. Per una analisi dettagliata di questo aspetto ci permettiamo di rinviare a G.M. Ruotolo, A Season in the Abyss, *Il nuovo copyright UE tra libertà di informazione, diritti fondamentali e mercato unico digitale*, in "Il diritto dell'Unione europea", 2019, n. 2, p. 367 ss.

[18]CGUE, *Google France*, 23 marzo 2010, cause da C-236/08 a C-238/08; CGUE, *Coöperatieve Vereniging SNB-REACT U.A. contro Deepak Mehta*, 7 agosto 2018, causa C-521/17. In dottrina, tra gli altri, v. J. Cornthwaite, *To Key or Not to Key? The Judgment of the European Court of Justice in the Google France AdWords cases*, in "European Intellectual Property Review", vol. 32, 2010, n. 7, p. 352-359; A. Montanari, *Contratto di AdWords e profili di responsabilità. Osservazioni a margine di Corte di giustizia 23 marzo 2010, cause riunite da C-236/08 a C-238/08*, in "Diritto del commercio internazionale", 2011, n. 2, pp. 524-547; R. Petruso, *La responsabilità dell'Internet service provider nella legislazione e nella giurisprudenza europea*, in P. Cerami, M. Serio (a cura di), "Scritti di comparazione e storia giuridica. Atti dei seminari del Dottorato di Diritto Comparato dell'Università di Palermo", Torino, 2011, p. 180 ss.; R.H. Weber, *Internet Service Provider Liability*, in "Journal of Intellectual Property, Information Technology and Electronic Commerce Law", 2010, p. 145 ss.; G. Spedicato, *La sottile linea di confine tra esclusiva sul segno e usi leciti del marchio altrui: prime riflessioni sulla giurisprudenza comunitaria in materia di keyword advertising*, in "Diritto dell'informazione e dell'informatica", 2010, n. 4-5, pp. 731-754.

[19]CGUE, *L'Oréal c. eBay*, 12 luglio 2011, causa C-324/09, su cui si vedano, tra gli altri, M. Nino, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale ed internazionale*, in "Diritti umani e diritto internazionale", 2016, n. 3, p. 558 e N. Rodean, *Responsabilità del gestore del mercato online per le violazioni ai diritti di marchio altrui*, in "Diritto pubblico comparato ed europeo", 2011, n. 4, pp. 1594-1602.

[20]CGUE, *Eva Glawischnig-Piesczek contro Facebook Ireland Limited*, 3 ottobre 2019, causa C-18/18, su cui v. G.M. Ruotolo, D. Vaira, *Responsabilità dei* social network *per* user generated content *e applicazione extraterritoriale delle misure inibitorie di lesioni dei diritti della personalità alla luce della recente giurisprudenza UE*, in "Ordine internazionale e diritti umani", 2020, n. 1, pp. 187-192.

[21]Corte europea dei diritti dell'uomo, *Delfi c. Estonia*, 16 giugno 2015, n. 64569/09.

[22]Su questo orientamento si veda Corte d'appello Milano, *RTI c. Yahoo!*, sentenza 7 gennaio 2015, in "Corriere giuridico", 2016, n. 6, p. 811-831, con nota di E. Bassoli. Più ampiamente, anche sui rapporti tra gli orientamenti italiani e quelli europei, in letteratura v. M. Bassini, *Internet e libertà di espressione*, Canterano, 2019, p. 145 ss.

[23]Di questo orientamento, invece, si è fatto spesso portatore il Tribunale di Roma. Si veda, al riguardo, G. Cassano, *Sulla responsabilità del provider per la diffusione abusiva in rete di opere audiovisive*, nota a Tribunale di Roma, sez. spec. in materia d'impresa, sez. IX, *R.T.I. Reti Televisive Italiane S.p.a. c. TMFT Enterprises, LLC – Break Media*, sentenza 27 aprile 2016, in "Diritto industriale", 2016, n. 5, pp. 460-468. Più di recente, in questo senso, Tribunale di Roma, n. 693/2019, sentenza 10 gennaio 2019.

[24]La Commissione dichiara esplicitamente che «la proposta conserva le norme relative alla responsabilità dei prestatori di servizi intermediari stabilite dalla direttiva sul commercio elettronico, che rappresentano ormai un fondamento dell'economia digitale e sono essenziali per la tutela dei diritti fondamentali online. Tali norme sono state interpretate dalla Corte di giustizia dell'Unione europea, che ha fornito chiarimenti e orientamenti preziosi».

[25]*Epic Games, Inc. v. Apple Inc. 20-cv-05640-YGR*. Il processo, dopo una fase preliminare, si è aperto il 3 maggio 2021. In considerazione della rilevanza del caso, la cancelleria della Corte ha creato una pagina web specifica, con tutte le informazioni pubblicabili di pertinenza. La Corte, con due separati

atti ("permanent injunction" e "judgment"), entrambi adottati il 10 settembre 2021, ha, per un verso, accolto le richieste della *Epic* relative alla violazione del diritto antitrust da parte di Apple, dichiarando che quest'ultima «and its officers, agents, servants, employees, and any person in active concert or participation with them ("Apple"), are hereby permanently restrained and enjoined from prohibiting developers from (i) including in their apps and their metadata buttons, external links, or other calls to action that direct customers to purchasing mechanisms, in addition to In-App Purchasing and (ii) communicating with customers through points of contact obtained voluntarily from customers through account registration within the app» e, per l'altro, ha accolto la riconvenzionale della stessa Apple per responsabilità contrattuale nei confronti di Epic, condannando quest'ultima a pagare «1) damages in an amount equal to (i) 30% of the $12,167,719 in revenue Epic Games collected from users in the Fortnite app on iOS through Epic Direct Payment between August and October 2020, plus (ii) 30% of any such revenue Epic Games collected from November 1, 2020 through the date of judgment, and interest according to law».

[26]Commissione, doc. AT.40437.

[27]A. Rosanò, E. Salmini Sturli, *L'ultima* legal suasion *dell'AG Wahl in tema di* ne bis in idem *applicato alla concorrenza e un'occasione mancata per la Corte di giustizia*, in "OsservatorioDUE", 2019. Per un'analisi approfondita del principio nel contesto penale si veda A. Procaccino, *I bis in idem tra diritti individuali e discrezionalità dell'apparato. Il doppio processo come pena*, Milano/Padova, 2022, *passim*.

[28]CGUE, *Aalborg Portland*, 7 gennaio 2004, cause riunite C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P e C-219/00 P; CGUE, *Showa Denko*, 29 giugno 2006, causa C-289/04 P; CGUE, *SGL Carbon*, 29 giugno 2006, causa C-308/04; CGUE, *Powszechny Zakład Ubezpieczeń na Życie*, 3 aprile 2019, causa C-617/17.

[29]CGUE, causa C-617/17, cit.

[30]G. Di Federico, *EU Competition Law and the Principle of Ne Bis in Idem*, in "European Public Law", vol. 17, 2011, n. 11, pp. 241-260; R. Nazzini, *Fundamental rights beyond legal positivism: rethinking the ne bis in idem principle in EU competition law*, in "Journal of Antitrust Enforcement", vol. 2, 2014, n. 2, p. 270-304.

[31]Z. Georgieva, *The Digital Markets Act Proposal of the European Commission: Ex-ante Regulation, Infused with Competition Principles*, in "europeanpapers.eu", vol. 6, 2021, n. 1, p. 25-28; G.M. Ruotolo, *Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di bis in idem*, in "SidiBlog.org", 29 marzo 2021.

[32]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[33]Regolamento (UE) 2017/1128 del Parlamento europeo e del Consiglio, del 14 giugno 2017, relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno. Sul regolamento si vedano C. Pesce, *Blocchi geografici ingiustificati*, in "I Post di AISDUE", 5 aprile 2019; G.M. Ruotolo, *La lotta alla frammentazione geografica del mercato unico digitale: tutela della concorrenza, uniformità, diritto internazionale privato*, in "Diritto del commercio internazionale", 2018, n. 2, pp. 501-521, in particolare, per l'aspetto dell'applicazione extraterritoriale, v. p. 518 ss.

[34]In senso, a noi pare, analogo v. O. Pollicino, *Piattaforme digitali e libertà di espressione: l'ora zero*, in "Lavoce.info", parla di "data due process": «se il costituzionalismo analogico è quello dei diritti sostanziali, quello digitale si fonda invece sulla dimensione procedurale».

[35]Per un'analisi complessiva di queste tendenze ci permettiamo di rinviare a G.M. Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Cacucci, 2021, *passim*.

[36]Come noto, i frattali sono oggetti geometrici dotati di omotetia interna, i quali, cioè, ripetono la loro forma allo stesso modo su scale diverse; questa caratteristica, detta autosimilarità o autosomiglianza, comporta che ingrandendo una qualunque parte di un frattale se ne ottiene una figura simile all'originale, in maniera ricorsiva. L'uso di modelli frattali per la spiegazione di fenomeni giuridici non è del tutto nuovo in dottrina, specie anglosassone: v. D.G. Post, M.B. Eisen, *How Long is the Coastline of the Law? Thoughts on the Fractal Nature of Legal Systems*, in "Journal of Legal Studies", vol. 29, 2000, p. 545-584; A.S. Morrison, *The Law is a Fractal: The Attempt to Anticipate Everything*, in "Loyola University Chicago Law Journal", vol. 44, 2013, n. 3, p. 649-681; N.M. Vladoiu, *The Decryption of Law as an Exact Normative Science Using Fractals*, in "Law Review", vol. 4, 2014, n. 2, p. 56-65. Noi abbiamo provato ad analizzare, in base a una logica frattale, appunto, gli accordi commerciali dell'UE, in G.M. Ruotolo, *Gli accordi commerciali di ultima generazione dell'Unione europea e i loro rapporti col sistema multilaterale degli scambi*, in "Studi sull'integrazione europea", 2016, n. 2-3, pp. 329-354.

* * *

The European proposals for the reform of Internet service providers liability

Abstract: The paper analyzes the proposals for the reform of the liability of Internet service providers in the light of the Digital Services and Digital Markets Act of the European Union, also focusing, in particular, on the profile of the preventive measures that can be adopted in the antitrust field and the risks of double punishment, resulting in a violation of the no bis in idem.

Keywords: Services – Liability – Providers – EU law – Bis in idem

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0054

Wanted: Nobel Peace Price Winners Who Create Peace in Cyberspace

Wolfgang Kleinwächter

The paper starts with the statement that for the future of mankind cybersecurity is as important as the management of climate change. Building a global cybersecurity architecture should be a priority for diplomacy in the digital age. The paper covers the three main intergovernmental cybersecurity negotiation platforms: 1. The "Open Ended Working Group" (OEWG), operating under the 1st Committee of the UN General Assembly, deals with norms for state behaviour in cyberspace. 2. The new UN "Ad Hoc Committee" (AHC) has a mandate to draft a convention against cybercrime. 3. The Group of Governmental Experts for Lethal Autonomous Weapon Systems (GGE LAWS) is working on an agreement for drones and killerrobots. The author argues, that due to the complexity of the issues a reasonable involvement of non-state actors is needed to find workable solutions. The paper concludes, that conceptual disagreements about the future of the digital world between cybersuperpowers should not be an obstacle to selective agreement on stability in cyberspace.

Cybersecurity – Cybercrime – Robot Killer – Global Digital Compact

Summary: *1. Introduction – 2. State behaviour in cyberspace – 3. Cybercrime – 4. Autonomous weapons systems – 5. Technical Internet standards – 6. A dual strategy for cyberspace*

1. Introduction

On January 1, 2022, Germany assumed the presidency of the G7. Alongside climate change and the Corona crisis, cybersecurity is to be at the top of the agenda. That makes sense. The pandemic in particular has shown how dependent our world has become on a secure digital infrastructure. Instability in cyberspace is no less threatening to future generations than a destroyed environment.

Hardly anything has changed more in the last two decades than the Internet world. The Internet started as a promise of freedom and growth. Today it is seen more and more as a risk factor. Boundless communication and endless innovation have been overshadowed by the digital arms race, cyber espionage and blackmail software. On the Internet, everything seems to be pregnant with its opposite. Freedom and prosperity for some, Orwellian surveillance and exploitation for others. The Internet gives creative developers, innovative entrepreneurs and responsible citizens the same opportunities as hate preachers, pedophiles and warmongers. And it is still unclear who will gain the upper hand in this newly

W. Kleinwächter is a Professor Emeritus for Internet Policy and Regulation from the University of Aarhus. He was a member of the ICANN Board and a Commissioner in the Global Commission on Stability in Cyberspace. He is involved in Internet Governance issues since the early 1990s and has served in numerous committees in the UN, ITU, Council of Europe and the European Commission.

The paper is part of the Special issue "Internet governance and the challenges of digital transformation" edited by Laura Abba, Adriana Lazzaroni and Marina Pietrangelo.

flared-up struggle between "good" and "evil". If a "real war" were to break out today, U.S. President Joe Biden recently said, it would likely begin with a cyberattack.

In this respect, it is more than justified to make building a global cybersecurity architecture a priority for diplomacy in the digital age. The U.S. and China are heading toward a cold cyberwar. Digital attacks on critical infrastructure are proliferating. Internet-based drones, programmed with facial recognition software, seek out their own targets to kill. What can be done?

The good news is that governments and non-state actors have been talking about the risks and side effects of the information age for years. In 2005, a UN World Summit on the Information Society (WSIS) was held in Tunis. There, an "Agenda" was adopted with guidelines for a people-centered peaceful and open digital future. Since then, there has been the "Internet Governance Forum" (IGF), the UN's annual "digital summit." The next WSIS review conference is due in 2025. And other bodies have been formed under the UN umbrella to address cybersecurity, the digital economy and human rights in virtual space. So the world knows what dangers lurk in cyberspace and what should be done.

But the bad news is that virtually nothing concrete has been agreed so far. There is still a digital divide, regardless of all the progress of information infrastructure development in recent years with nearly five billion Internet users in 2022. There are massive violations of human rights in cyberspace with growing Internet censorship and mass surveillance. There are new oligopolies in the digital economy which hinder fair competition and innovation. Cross border data flow becomes part of a digital tradewar. And cyberattacks by state and non-state actors undermine global peace and international security.

20 years ago, WSIS was the only intergovernmental platform, dealing with Internet related public policy issues. Today there are numerous negotiations platform where governments and non-state actors from business, civil society and the technical community try to find solutions for the issues, which have emerged in the global Internet Governance Ecosystem since 2005, when the "Tunis Agenda" was adopted by 193 heads of state. UNESCO is dealing with artificial intelligence. ITU with the development of a digital infrastructure, WTO with digital trade, ILO with the consequences of digitalization for the labour market. The UN Human Rights Council is discussing how human rights, should be implemented in the online world. Based on the recommendations from a "High Level Panel on Digital Cooperation", chaired by Jack Ma from AliBaba and Melinda Gates from the Microsoft Foundation, UN Secretary General Antonio Guterres has published a "Roadmap on Digital Cooperation" in June 2020 and has now proposed a "Global Digital Compact" which could guide the world towards the 2030s.

However, all the negotiations didn't produce concrete arrangements with clear commitments. There are numerous reports and background papers on the various conference tables, but there is no agreement. There UN bodies – OEWG, AHC, LAWS – are negotiating security in cyberspace. But in all three groups, the controversies are greater than the will to agree on a common blueprint.

2. State behaviour in cyberspace

Lets have a deeper look into the global cybersecurity negotiations. Cybersecurity is now a core problem both of national and international security. And the numbers of attacks in cyberspace is growing.

The first negotiation platform is the Open Ended Working Group (OEWG). The OEWG was established in 2018 under the 1st Committee of the UN General Assembly. It was based on the work of several so-called "Group of Governmental Experts" (GGEs), which since 2004 worked on norms of state behaviour in cyberspace. The GGE could agree on eleven norms – including the norm not to attack critical infrastructures of other countries – and on a number of confidence building measures. It also agreed that international law and the Charter of the United Nations is relevant both offline and online. In 2020 the OEWG mandate was extended to 2025. All 193 UN member states participate in its work. Its task is to clarify what constitutes good behaviour by states in cyberspace in accordance with international law. Based on the agreement that international law applies not only to the analog world, but also to the digital world, this should not be a complicated task. There is no need to reinvent the wheel or to write a new UN Charter. But the controversies begin when things get concrete. When is a "cyber attack" a use of force that is contrary to international law under Article 2, paragraph 4 of the UN Charter and triggers the right to self-defense, laid down in Article 51? Is a "hack back" justified by Article 51 which constitutes the right to self-defence? Or can you asymmetrically answer a cyberattack with a bombing, which is what Israel did in Gaza after a cyberattack by Hamas? The problem is that not only there is disagreement about what exactly constitutes a cyberattack, but also the attacker is in many cases difficult to determine. If a tank rolls across the border, everyone knows where

it comes from. But if malware is installed in a power plant and is activated only after six months, it is not easy for the attacked state to prove one hundred percent where the attack came from.

Therefore, the OEWG is also about the role of non-state actors and confidence – and capacity – building measures. Ideas such as creating a permanent point of contact for crisis situations or organizing closer cooperation between technical experts and diplomats are reasonable steps. The first meeting of the OEWG in New York in early December 2021 took place in a thoroughly constructive atmosphere but it could not agree, how non-state actors will be involved in future negotiations. And it is also unclear what is actually supposed to come out of the negotiations: An action plan? A code of conduct? A cyber non-aggression pact?

3. Cybercrime

The second negotiation platform is about the exploding crime in cyberspace. For organized crime, virtual space has become more profitable than drug or human trafficking. There is already an international treaty against cybercrime: the Budapest Convention, signed in November 2001, just weeks after the terroristic attacks against the World Trade Center in New York on 9/11.

This treaty was drafted under the umbrella of the Council of Europe and it is open to every country for signature. Western countries have long campaigned to universalize the Budapest Convention, but only one-third of the 193 UN countries have signed it. Major Internet countries such as India, Brazil, and China were not involved in the negotiations and supported the Russian proposal to draft a new UN convention.

The concern of Western countries now is that new negotiations will undermine the regulations already in place and lower the quite effective standard of the Budapest Convention. Disputes are expected above all when it comes to the criminalization of information content. How are democracies and autocracies supposed to agree on what expression of opinion is permitted on the Internet?

The plan is that the new UN convention should be ready by the end of 2023. This is a tough timetable, but one that is nevertheless not entirely unrealistic. First, many passages of the Budapest Convention can easily be adopted. And second, the pressure of suffering generated by the global cyber mafia, with its extortion of hospitals and public administrations, and attacks on global supply chains and critical infrastructures, is now evenly distributed across ideological boundaries. If negotiators in the new Ad Hoc Committee (AHC) focus on what is feasible, progress would not be impossible.

4. Autonomous weapons systems

The third negotiation platform is about autonomous weapons systems. There, under the umbrella of the Convention on Conventional Weapons (CCW), a group of experts under the acronym LAWS (Lethal Autonomous Weapon Systems) has been negotiating killer robots and drones since 2014. UN Secretary General Antonio Guterres has been calling for a ban on autonomous weapons for years. But a very mixed group of states – Russia, China, the U.S., Israel, Turkey – have so far rejected even a moratorium. To be sure, there is fundamental agreement not to leave life-or-death decisions to an algorithm. But opinions differ even on the definition of what constitutes an autonomous weapons system. And while the filibustering continues in Geneva, the use of armed drones in local wars is becoming common practice, as in Nagorno-Karabakh, Yemen, Libya, the Middle East, in Ukraine and elsewhere. The problem is complicated. Maximum limits can be agreed upon for nuclear warheads, but what is the limit for an algorithm? Tanks and aircrafts can be counted and controlled, but how do you count and verify bits and bytes?

When it comes to autonomous weapons systems, the traditional rituals of disarmament negotiations are reaching their limits. More than ever, the political will of the actors involved and a minimum of trust are needed. And that depends in no small part on the extent to which it is recognized how a war with digital weapons could play out. NATO Secretary General Jens Stoltenberg recently recalled the time before World War One. Not only had the world "slipped into" a world war in 1914, he said, but the political leaders of the time had completely underestimated the effects of the new technologies of the time – from bombers and tanks to poison gas. Franz Haber, who later won the Nobel Prize for Chemistry and was involved in the development of chlorine gas in the early 1910s, convinced politicians that the use of this weapon would help bring about a quick end to the war. But he was wrong. The opposite was true. Millions of people died and chemical weapons became another source of instability in our fragile world. What would happen if Pandora's can of autonomous weapons systems were opened in a conflict today?

5. Technical Internet standards

And then there is a fourth negotiation platform: protecting the public core of the Internet. The functioning of the Internet infrastructure and the availability of the corresponding resources – root servers, domain names, IP addresses, Internet protocols – is now of the same elementary importance as water and electricity supplies. These resources are managed by various technical organizations – ICANN, IETF, RIRs. In 2016, after the US government – under the Obama administration – transferred its historic oversight of the Internet's A-root server to ICANN, there were repeated doubts, especially from China and Russia, about the ability of this technical community to manage technical resources in the interest of the global community.

But no disaster happened. On the contrary, if there had been a need for a stress test of the resilience of the system, which has been functioning for more than 20 years, the pandemic provided the proof. Since the Corona outbreak, there has been an exorbitant growth in Internet usage. Home office, zoom conferencing, online shopping, distance learning have all caused demand for domain names and IP addresses to explode. As it turned out, the existing system was able to handle these new challenges without any problems. There was no shortage of IP addresses or domain names. The root and name servers worked.

If these technical resources were to be drawn into a geo-strategic power play, there would be significant risks involved. Just as there is no Chinese or American air, only clean or polluted air, the technical Internet resources are politically neutral. If they became the plaything of a political arm-twist, everyone would suffer the damage. It was therefore very sensible that under the British G7 presidency the digital ministers clearly committed themselves to leaving the elaboration of technical digital standards in the hands of the technical community. The German G7 presidency should continue to pursue this path with vigor.

6. A dual strategy for cyberspace

The new German government in its role as chair of the G7 in 2022 is confronted with a broad range of challenges on the digital front. More than ever, the world needs a sustainable and fair multilateralism for cyberspace that is guided by the universal values of the United Nations Charter and the UN Declaration of Human Rights and embedded in close cooperation between governments, business, civil society and the technical community. With the G7 presidency, many eyes are now on Germany, which hosted the UN IGF in 2019. This also affects the negotiations on autonomous weapons systems. In January 2020, Green Party member of the Bundestag Katja Keul had criticized the then German government for not advocating strongly enough for a ban on these weapons under international law. The coalition agreement now states that the new federal government will take early initiatives on arms control in the areas of cyber and artificial intelligence. The German section of the non-governmental organization "Stop Killer Robots" has criticized this as far too soft. The EU has not yet positioned itself either. Katja Keul is now State Secretary in the German Foreign Office. This is an exciting task in which one can also learn from historical experience.

In early December 2021, the Friedrich Ebert Foundation held a conference to mark the 50th anniversary of the award of the Nobel Peace Prize to Willy Brandt. It wisely elaborated that Brandt's Ostpolitik was based on a dual strategy. The concept of "change through rapprochement" consisted both of an outstretched hand toward the system's rival and of strengthening the country's own resources. NATO's 1967 "Harmel Report," in which Brandt had participated as foreign minister of the then Grand Coalition, formed the basis for the creation of a web of "détente treaties" – from bilateral treaties between West Germany and the Soviet Union, Poland and the Czechoslovakia, via the Berlin Agreement (1971), the Soviet-US-SALT Agreements to the Helsinki Final Act (1975) – that ensured peace, at least for Europe, for several decades. The treaties of the 1970s were not based on the fact that the other social system was considered to be good. Here, people agreed to disagree. But there was an overriding interest in renouncing violence and protecting the common heritage of mankind that included the legitimate interests of the other side. Security was understood as collective security with the system rival, not against it.

Joseph Nye, doyen of American political science, reminded us in an essay "The End of Cyber-Anarchy", in the January 2022 issue of "Foreign Affairs", that in the Cold War temporary escalations of crises and stabilizing treaty negotiations were two sides of the same coin. Conceptual disagreements about the future of the digital world should not be an obstacle to selective agreement on stability in cyberspace. Wolfgang Ischinger, ex-head of the Munich Security Conference, also sees a reactivation of the principles of the 1975 CSCE Final Act and of the 1992 Charter of Paris as a sensible strategy to counter the new threats of the 2020s.

UN Secretary-General Antonio Guterres' proposal to use the UN Future Summit, scheduled for

2023, to adopt a "Global Digital Compact" could become an important building block for a new cybersecurity architecture. The idea floated by Finnish President Sauli Niinistö of using the 50th anniversary of the Helsinki Final Act in 2025 to promote security in cyberspace could be a good new beginning. In any case, if somebody will find the code for a lasting cyberpeace, she or he would be a good candidate fort the next Nobel Peace Prize.

* * *

Cercansi vincitori di Premio Nobel per la pace che creino la pace nel cyberspazio

Riassunto: Il saggio inizia con l'affermazione che per il futuro dell'umanità la sicurezza cibernetica è importante quanto la gestione del cambiamento climatico. Costruire un'architettura globale per la cybersecurity dovrebbe rappresentare una priorità per la diplomazia nell'era digitale. Il contributo tratta le tre principali piattaforme negoziali intergovernative sulla sicurezza informatica: 1. L'"Open Ended Working Group" (OEWG), che opera nell'ambito del Primo Comitato dell'Assemblea Generale delle Nazioni Unite, si occupa delle regole per il comportamento degli stati nel cyberspazio. 2. Il nuovo "Ad Hoc Committee" (AHC) delle Nazioni Unite che ha il mandato di redigere una convenzione contro la criminalità informatica. 3. Il "Group of Governmental Experts for Lethal Autonomous Weapon Systems" (GGE LAWS) che sta lavorando alla stesura di un accordo per droni e robot killer. L'autore sostiene che, a causa della complessità delle questioni, è necessario un ragionevole coinvolgimento di attori non statali al fine di trovare soluzioni praticabili. Il contributo si conclude sostenendo che i disaccordi concettuali sul futuro del mondo digitale tra le cyber superpotenze non dovrebbero costituire un ostacolo ad un accordo selettivo sulla stabilità nel cyberspazio.

Parole chiave: Sicurezza informatica – Criminalità informatica – Robot killer – Global Digital Compact

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0053

Data commons: privacy e cybersecurity sono diritti umani fondamentali

Arturo Di Corinto

Google sa di noi più cose di quante ne ricordiamo, conosce abitudini e percorsi quotidiani, sa con chi, quando e per quanto tempo siamo stati; Zoom sa con chi lavoriamo; Facebook mette all'asta le nostre preferenze; bot e troll su Twitter influenzano le nostre opinioni. Anche i meme della disinformazione affollano i social e inquinano il dibattito scientifico. Se non impariamo a proteggere i comportamenti trasformati in dati digitali saremo esposti a un potere incontrollabile, quello della persuasione commerciale, della manipolazione politica e della sorveglianza statuale.

Data commons – Privacy – GDPR – Cybersecurity – Big Tech

Sommario: *1. Introduzione – 2. Il potere delle piattaforme – 3. I termini di servizio della nostra vita* onlife *– 4. Privacy e cybersecurity sono diritti umani fondamentali – 5. Privacy e anonimato – 6. Anonimato, fake news e disinformazione – 7.* Data breach *e banche dati – 8. Le infrastrutture critiche e la privacy – 9. Perimetro nazionale*

1. Introduzione

La privacy è come la libertà: se non gli dai valore, rischi di perderla. Già. Nonostante l'eco mediatica e gli interventi resi possibili dal nuovo Regolamento europeo generale sulla protezione dei dati, il GDPR, sono ancora in tanti, troppi, a non dare valore alla riservatezza dei propri dati personali anche se quei dati identificano comportamenti quotidiani e permettono di profilare gli utenti digitali indirizzandone scelte e azioni. E così, come dice lo storico Noah Yuval Harari «La gente è felice di elargire la propria risorsa più preziosa – i dati personali – in cambio di servizi di posta gratuiti e video di gattini. Un po' come è accaduto agli africani e agli indiani d'America che hanno venduto grandi territori in cambio di perline colorate»[1].

I dati sono l'oro e il petrolio dell'umanità connessa e dalla loro corretta gestione dipendono i gradi di libertà delle scelte quotidiane. E allora perché siamo pronti a darli via solo per partecipare a sonore litigate su Facebook, farci buggerare via email da rapinatori digitali e tracciare da poliziotti zelanti con app pensate per i criminali? La verità è che nella gestione della propria presenza online si rivela quel pericoloso divario digitale che ancora oggi, a 30 anni dal Web, riflette antiche disuguaglianze: tra chi è capace di controllare, difendere e rivendicare la tutela dei suoi dati e chi non è in grado di farlo.

Con gli smartphone *always on* e le app a prova di incapace abbiamo messo armi potentissime in mano ad adulti che si comportano come bambini che bisticciano, tifano, si mostrano crudeli verso gli altri, dimentichi di ogni forma di empatia. Questa ignoran-

A. Di Corinto insegna Identità digitale, Privacy, Cybersecurity nel Corso di laurea in Media, comunicazione digitale e giornalismo di Sapienza - Università di Roma.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

za digitale indirizzata dal mercato è il frutto di vari fattori: la diffusione su scala globale di *personal media* sempre più potenti, maneggevoli ed economici; un sapere comunicativo diffuso promosso da scuole e università; l'iperconnessione religiosa ai social; l'avvento della *me-communication*, la "comunicazione autoriferita", come la chiama il sociologo Manuel Castells[2]. Pilotata dai signori delle piattaforme che oggi sono i signori dei dati, l'ignoranza digitale ha generato un nuovo feudalesimo digitale[3], che divide il mondo in due, tra chi produce gratuitamente questi dati e chi li raccoglie e mette a profitto.

La raccolta, l'organizzazione e l'utilizzo dei dati sono al centro del capitalismo estrattivo delle piattaforme[4] che, conoscendo le più intime inclinazioni, il *sentiment*, dei propri utenti, sono in grado di anticiparne mosse e desideri affinché continuino a produrli. Elaborati da potenti algoritmi con le tecniche proprie delle scienze sociali (la psicometria), diventano il carburante per le intelligenze artificiali che ci sostituiranno (già in parte lo fanno) in compiti complessi per i quali una volta si veniva remunerati per sostenere intere famiglie.

La violazione dei dati realizzata da Cambridge Analytica per cui Facebook è stata multata – facendogli il solletico – rientra in questo schema: se conosco gli orientamenti politici del produttore di dati, e lo so in base ai like che ha messo, sarò in grado di cucirgli addosso un messaggio che non potrà rifiutare. Il messaggio andrà a rinforzare le sue convinzioni pre-esistenti e gli stenderà intorno un "cordone sanitario" affinché non acceda a contenuti che le possano mettere in discussione[5].

2. Il potere delle piattaforme

Google sa tutto di noi. Se facciamo una ricerca in rete Google sa che parola chiave abbiamo usato e se abbiamo cliccato o no sul banner pubblicitario di Adsense. Da quella semplice keyword sa se siamo preoccupati del Covid o se cerchiamo una clinica oncologica. Google sa che siti abbiamo visitato e se abbiamo usato il suo indirizzo Gmail per "loggarci" su un certo sito. Questo vale per i siti erotici come per l'accesso ai siti di giornalismo investigativo. Se la ricerca ci porta su Youtube è in grado di suggerirci i video da vedere favorendo i video simili a quelli che abbiamo già cliccato e presentarci dei contenuti razzisti anziché storie di solidarietà quotidiana.

Mentre navighiamo con il suo browser, Chrome, Google raccoglie le informazioni relative alla nostra permanenza su ciascun sito: sa da dove siamo partiti e dove siamo arrivati durante la nostra sessione di *web surfing*. Se però ce ne andiamo in giro, a piedi o in macchina, e usiamo Google Maps, saprà ancora più cose: da dove partiamo e dove andiamo, se quel percorso è ripetuto e frequente, quanto tempo ci mettiamo per arrivare e se ci siamo fermati a fare shopping presso un negozio identificato sulla mappa.

Queste informazioni che Google raccoglie incessantemente sono scritte con la penna, non con la matita, e sono destinate a rimanere archiviate per successive analisi di mercato. Google lo dichiara apertamente: tutte le informazioni che raccoglie su di noi servono a migliorare i suoi servizi e a produrre annunci e risultati personalizzati in base alle nostre ricerche, anche a favore dei suoi clienti.

In cambio di qualche comodità abbiamo così barattato la nostra privacy, quell'elemento della vita associata che ci permette di nasconderci all'occhio inquisitore degli altri garantendoci il diritto a essere imperfetti. È così che il diritto a non essere valutati e sorvegliati si ferma alle porte di Google. Perché Google sa di noi anche quello che non ci ricordiamo più: dove siamo stati, con chi, per quanto tempo, e quello che abbiamo fatto.

Google è una potenza il cui fatturato è superiore a quello di nazioni intere, ed è più avanti di molti governi nello sviluppo di computer quantistici e delle intelligenze artificiali che ci sostituiranno nel lavoro.

Anche Zoom ci spia. La piattaforma per videoconferenze tanto in voga durante la quarantena passa(va) le nostre informazioni a Facebook. WhatsApp, invece, ha chiesto agli europei di accettare in maniera esplicita la condivisione con la casa madre Facebook (oggi Meta), dei dati che generano usando l'app, se vogliono continuare a usare i suoi servizi generando una vasta levata di scudi. Fuori dell'Europa già lo faceva e continua a farlo. Niente di scandaloso, direte, lo stesso vale per altre app, siti e software che grazie ai dati generati dalle nostre interazioni creano profili statici e dinamici, singoli o aggregati, della nostra persona digitale, quella che ci precede nelle interazioni online e che viene usata da Amazon per decidere il prezzo da proporci quando navighiamo tra i suoi prodotti.

Il capitalismo delle piattaforme in fondo fa proprio questo: estrae valore dalla profilazione degli utenti e dal data mining dei nostri comportamenti online. In questo modo le aziende sanno con precisione che cosa offrirci, quando, dove e a quale prezzo, sapendo già cosa siamo propensi a desiderare. Il loro modello di business è basato sulla conoscenza dei soggetti isolati e iperconnessi che più tempo passano con i loro software gratuiti più facilmente manifesteranno desideri, fragilità e sentimenti da soddisfare con un'azione: postare, condividere, cliccare, comprare. Ogni click diventa l'occasione per arricchire il nostro

profilo psicometrico, venderlo al migliore offerente, anche per le campagne politiche. È così che Trump ha vinto nella campagna elettorale Usa 2016.

La colpa di un uso così disinvolto dei dati è anche nostra. Non abbiamo ancora capito il valore della nostra presenza online. I dati che generiamo quando siamo online indicano dei comportamenti e, in una società digitale, questi comportamenti sono trasformati in dati digitali. Il trattamento dei dati digitali consente di interpretare e spiegare i comportamenti passati ma anche di predire i comportamenti futuri. È così che i nostri dati vengono resi "produttivi". Siccome quei dati possono essere venduti e comprati, le piattaforme ci offrono gratis i loro servizi. Ma quei servizi li paghiamo con i nostri dati. Quando non paghi qualcosa il "prodotto" sei tu.

3. I termini di servizio della nostra vita *onlife*

Quando ci iscriviamo a un sito, app o servizio Internet, in genere ci viene richiesto di accettare i "Termini di servizio", i ToS, che indicano come i nostri dati sono raccolti e usati. La maggior parte delle volte non li leggiamo, semplicemente perché non ne abbiamo il tempo e la voglia, ma soprattutto perché non li capiamo, visto che sono scritti in "legalese".

Eppure è così che perdiamo il controllo dei dati che ci identificano come cittadini, lavoratori e consumatori. Quei dati infatti verranno utilizzati per creare dei profili dettagliati dei nostri comportamenti e verranno commerciati per usi che non sempre conosciamo.

Ad esempio i ToS di Facebook ed Amazon dicono che i nostri dati sono usati per tracciare il nostro comportamento su altri siti, mentre LinkedIn raccoglie, usa e condivide i dati di geolocalizzazione e Instagram ci mette sopra il suo copyright.

I termini di servizio di Reddit, Yahoo e WhatsApp dicono che usandoli accettiamo «di difendere, indennizzare e sollevare il servizio da ogni responsabilità in caso di reclamo». Quasi tutti prevedono che gli stessi termini possono essere modificati in qualsiasi momento a discrezione del fornitore, senza preavviso per l'utente.

Nel suo *Data Manifesto*[6], Kevin Kelly, tecnologo e co-fondatore della rivista *Wired*, dice che i dati «non esistono da soli», che hanno valore solo se messi in relazione ad altri dati e che circolando diventano una risorsa condivisa. Per questo possono risentire della tragedia dei beni comuni, cioè di un'egoistica azione di appropriazione – come quando un privato recinta un pezzo di parco pubblico impedendo ad altri di usarlo – e pertanto vanno protetti dai governi. Noi aggiungiamo che vanno protetti dai Signori dei dati, le aziende che ne fanno costantemente incetta.

Ma i dati sono un bene comune perché, sulla base dei dati raccolti, possiamo costruire una società migliore. I dati che noi produciamo incessantemente attraverso l'interazione con i dispositivi digitali, rappresentano comportamenti quotidiani e possono essere una base di conoscenza importante per sviluppare politiche efficaci, servizi utili alle persone e nuovi prodotti commerciali utili e rispettosi dell'ambiente. I dati, anonimizzati e aggregati, possono servire a migliorare la capacità di uno Stato di rispondere alle esigenze dei propri cittadini.

Due esempi semplici semplici. Se noi abbiamo i dati, anonimi e aggregati, dei pazienti ospedalieri, probabilmente saremo in grado di pianificare meglio le risorse sanitarie necessarie a garantire la salute pubblica. Già viene fatto, pensate agli sforzi di raccolta e analisi dei dati epidemiologici. Se abbiamo i dati di quanti e quali attacchi cibernetici ci sono stati negli ultimi anni, saremo in grado sia di anticipare nuovi attacchi che di imparare a difenderci.

Quindi, il dato inteso come bene comune è questo: è un dato che può essere utilizzato in maniera utile dagli Stati per consentire una migliore qualità della vita delle persone e garantire diritti all'altezza delle democrazie in cui vogliamo vivere.

Il GDPR prevede, in caso di grave violazione dei database, la comunicazione diretta ai singoli interessati entro 72 ore, a pena di multe salatissime, fino a 20 milioni di euro e al 4 per cento del fatturato annuo aziendale. Le sanzioni possono essere un deterrente, ma non lo sono per i grandi player della rete.

Perciò anche noi dobbiamo fare la nostra parte e capire se, quando e come ci conviene cedere i nostri dati.

4. Privacy e cybersecurity sono diritti umani fondamentali

Ma c'è un'altra questione, il rapporto stretto tra la privacy e la cybersecurity. Il motivo è semplice da capire: in un mondo digitale i dati che identificano i nostri comportamenti sono digitalizzati; se non riusciamo a tutelare questi dati digitali, non riusciamo a tutelare i nostri comportamenti. In particolare non riusciamo a tutelare i comportamenti passati dalle tecnologie che li possono spiegare e dalle tecnologie che li possono predire. I dati personali sono uno strumento di intelligence. Pensiamo alle massive violazioni di basi di dati personali usati per orientare il comportamento delle persone. Con i dati ormai ci si fa la "guerra".

Però. Se la privacy è l'altra faccia della cybersecurity è anche vero che la privacy è un diritto fondamentale dell'Unione europea, mentre la cybersecurity non lo è.

Eppure, in un mondo in cui ogni comportamento viene datificato diventando un dato digitale, proteggere quei dati che rimandano ai comportamenti quotidiani è cruciale, lo ripetiamo, proprio per la loro capacità di spiegare i comportamenti passati e di predire quelli futuri.

Se non riusciamo a proteggere i dati che ci definiscono come cittadini, elettori, lavoratori, e vicini di casa, potremmo essere esposti a un potere incontrollabile, quello della sorveglianza di massa, della manipolazione politica e della persuasione commerciale.

Pertanto privacy e cybersecurity sono la precondizione per esercitare il diritto alla libertà d'opinione, d'associazione, di movimento, e altri diritti altrettanto importanti.

Se accettiamo questa premessa possiamo pensare alla sicurezza informatica dei nostri dati come a un diritto umano fondamentale.

5. Privacy e anonimato

Eppure. Mentre la Bbc decide di portare i suoi contenuti nel *dark Web* per tutelare l'anonimato del proprio pubblico all'interno di paesi illiberali, in Italia si discute ancora di identificare gli utenti del Web.

Il dibattito, che pensavamo chiuso dopo le mobilitazioni degli anni scorsi contro la censura in rete, è ricominciato con la proposta di un parlamentare di *Italia Viva* a suo dire preoccupato per il dilagare dell'odio in rete, e che ha suggerito, parole sue, di rendere obbligatorio depositare un documento d'identità prima di aprire un profilo social «per impedire che il Web rimanga la fogna che è diventato».

Purtroppo questa risposta a problemi reali, l'hate speech, le fake news, il cyberbullismo, lo stalking online, il revenge porn, è sbagliata. Per vari motivi. Il primo è che molti odiatori in rete si presentano già con nome e cognome e il riscontro anagrafico non sarebbe un deterrente. Il secondo è che nessuno in rete è veramente anonimo e non c'è bisogno della carta d'identità per risalire ai dati anagrafici dei bulli in rete nonostante abbiano uno pseudonimo.

Per farlo occorrono tempo e risorse, riuscirci non è facile né immediato, ma si fa quando serve. Viceversa l'identificazione in massa degli utenti è un processo tecnicamente complesso e oneroso.

Il punto è qui che gli odiatori che spesso si presentano con nome e cognome in genere sono persone che semplicemente non sanno che un insulto, una minaccia espressa online, può essere perseguita come se fatta a scuola o al bar. I flame, i litigi in rete, inoltre, sono un elemento costitutivo della comunicazione virtuale: i social e i canali di chatting sono strumenti di dialogo veloce, dove si interagisce d'impulso, luoghi dove l'assenza fisica dell'interlocutore fa venire meno il timore della rappresaglia e spesso anche il pudore, la vergogna e la cautela nell'esprimere opinioni estreme.

Eppure la questione è più ampia. Il Web, o i social che ne rappresentano una parte, non è fatto solo di maleducati, odiatori, bulli, stalker, per i quali in realtà ci sono leggi anche severe che ne puniscono i comportamenti.

Il Web usato in maniera anonima è anche il Web dei dissidenti politici, dei profughi senza documenti, dei rifugiati, perseguitati nei loro paesi per essere omosessuali o per avere evaso la leva obbligatoria. E poi ci sono i cooperanti che vivono in zone di guerra, i blogger antimafia che non possono farsi riconoscere, e ci sono i *whistleblower*, i *citizen journalist*, gli impiegati di enti, ministeri e forze armate che devono giocoforza assumere identità fittizie per evitare ritorsioni a fronte delle loro denunce.

In aggiunta ci sono soggetti fragili che per raccontare esperienze di abusi e maltrattamenti mai e poi mai vorrebbero presentarsi con nome e cognome.

Quindi la domanda è: per provare a spaventare gli odiatori in rete è giusto cancellare l'anonimato di chi grazie ad esso può esprimersi liberamente?

Senza anonimato cadrebbero nell'autocensura e nel conformismo preventivo. E saremmo stati noi a togliergli quella tanto faticosamente conquistata libertà di parola. Le catacombe parlamentari sono piene di disegni di legge per limitare la libertà d'opinione in rete.

All'epoca della televisione erano tentativi surrettizi di mantenere la società divisa tra chi ha potere di parola e chi no, come diceva Michel Foucault. Ma oggi? Se queste energie venissero impiegate per educare le persone al rispetto degli altri e al rispetto delle leggi che ci sono, sarebbe già abbastanza.

6. Anonimato, fake news e disinformazione

L'anonimato in rete però permette anche di agire pratiche di disinformazione. E questo è un altro motivo per tutelare i dati personali e collettivi.

Sappiamo che le strategie di disinformazione si basano sulla manipolazione delle percezioni. La disinformazione è un'arma per indurre l'avversario a fare delle scelte sbagliate. Le fake news oggi sono la testa d'ariete di queste strategie di disinformazione

e servono a farci "comprare" quello che altri hanno deciso che "vogliamo" comprare: uno shampoo, una strategia, oppure un candidato politico.

Insieme alla profilazione dei social network le fake news pongono un problema molto serio anche alla sicurezza nazionale soprattutto quando usano deep fake video e deep fake audio o profili di persone che non esistono ma possono essere generate da un'intelligenza artificiale.

Una volta le campagne di disinformazione bersagliavano i decisori – i funzionari pubblici di alto livello, i politici, i giornalisti affermati, i funzionari dello Stato –, oggi queste campagne di disinformazione sono dirette a manipolare quella forma larvale di dibattito pubblico che c'è sui social network.

Come? Agendo attraverso la propaganda computazionale che sfrutta i social media e la credulità di chi li abita, la psicologia umana che non distingue la realtà dalla finzione, le voci e i pettegolezzi tanto cari ai cospiratori e gli algoritmi per manipolare l'opinione pubblica. È così che funzionano i *dark ads*: messaggi promozionali a pagamento diretti solo a specifici indirizzi o territori.

I dati raccolti dalle piattaforme sono usati per creare profili individuali e collettivi. Questa profilazione può essere usata per comunicazioni mirate e geolocalizzate, anche durante le elezioni.

La logica qui è doppia: se so chi sei, so quali contenuti farti vedere. Se conosco le tue scelte passate sono in grado di mostrarti solo le notizie che sei pronto a cliccare. Ogni click dice quali sono le nostre preferenze culturali e politiche, proprio quelle che sono collezionate nei giganteschi database che i padroni dei dati come Google, Amazon e Facebook usano per definire i nostri profili sociali, economici, ed elettorali.

Quindi la manovra è a tenaglia: prima la profilazione e l'esposizione alle fake news per polarizzare l'elettorato, poi il messaggio politico ritagliato *ad hoc* sotto forma di una comunicazione nominativa, diretta a una moltitudine di singoli elettori, ai quali viene recapitata in maniera ripetuta un'informazione specifica e coerente con il proprio profilo psicologico ed elettorale.

Nell'era di Internet la disinformazione fa largo uso delle fake news e la sua viralità approfitta soprattutto di Facebook, Google, Instagram fino a WhatsApp, piattaforme che agiscono da potenti casse di risonanza per i nostri pregiudizi, soprattutto quando sono veicolati da chi ci fidiamo di più: amici e conoscenti. Rappresentano un problema cibernetico.

Se la natura originaria delle bufale è quella di creare traffico web, e quindi macinare soldi dagli annunci pubblicitari, molti "spacciatori" di notizie false agiscono sotto falsa identità e hanno una motivazione ideologica: affermare un punto di vista anziché un altro, distorcere la realtà delle cose e creare "fatti alternativi". Una tecnica propagandistica salita prepotentemente alla ribalta durante la corsa alla Casa Bianca del 2016 e l'assalto a Capitol Hill dopo la sconfitta elettorale del presidente Trump da parte del democratico Joe Biden, ma che ha degli antenati "illustri" nelle *psy-ops*, le operazioni di guerra psicologica condotte da eserciti rivali per demoralizzare le truppe avversarie, influenzare il *sentiment* della popolazione e disorientare i governi.

A produrre disinformazione ci sono oggi i gruppi di *nation-state hackers*, chiamati anche APT (*Advanced Persistent Threat*), "minacce avanzate persistenti" che hanno come obiettivo di interferire con la democrazia. Si tratta di gruppi paramilitari cibernetici che vengono dai ranghi dell'intelligence, della polizia e dell'esercito, e hanno il compito, per conto dello Stato a cui hanno giurato temporanea fedeltà, di raccogliere informazioni su aziende concorrenti, su Stati avversari, su decisori pubblici per orientarne i comportamenti. Possono anche compiere azioni di sabotaggio o di guerra cibernetica. Perché? Per destabilizzarne l'economia o indebolire un avversario, ma anche per realizzare operazioni psicologiche orientate a creare malumore, diffidenza o paura nelle popolazioni, facendo uso di informazioni fasulle su target ben individuati.

Ecco, le campagne di disinformazione orchestrate dagli APT si basano sulla conoscenza del target, sui dati da essi prodotti, e servono a indirizzare le percezioni e le scelte maturate nell'agorà pubblica del Web. Quindi non vanno solo tutelati i dati personali in quanto tali, ma i dati che contribuiscono a definire la nostra persona digitale e che "rappresentano" scelte e desideri.

7. *Data breach* e banche dati

Ovviamente sono i *data breach* il pozzo principale a cui attingono i delinquenti, i cybercriminali e gli APT. Nel dicembre 2019 abbiamo saputo che la banca Unicredit era stata violata o, meglio, che tre milioni di profili dei suoi clienti erano stati violati a seguito di un attacco informatico avvenuto nel 2015. Ma che dire della violazione delle PEC di cinquecentomila indirizzi relativi ai Ministeri che afferiscono al CISR (Comitato interministeriale per la sicurezza della Repubblica) avvenuto nel 2018?

Tra il 2020 e il 2021 una serie di incursioni informatiche operate da gruppi specializzati che le hanno rivendicate nei loro blog del *dark Web* hanno esposto i dati di singoli cittadini, rappresentanti di or-

dini professionali e personaggi istituzionali. In Italia ci sono stati gli attacchi *ransomware* alla campagna vaccinale della Regione Lazio, all'Ordine dei notai e a quello nazionale forense, a livello globale alla società di consulenza Accenture, al Dipartimento del Tesoro Usa e ad altre agenzie nazionali europee.

Sicuramente c'è un tema che riguarda la formazione, la consapevolezza, ma anche la preparazione ad affrontare questi attacchi per tutelare la privacy di tutti: "non chiederti se verrai attaccato ma quando". Un concetto altrettanto importante di quello di resilienza, la capacità di ripartire dopo uno shock, in questo caso informatico.

8. Le infrastrutture critiche e la privacy

Se non è ancora chiaro, possiamo pensare al fatto che un attacco informatico di successo non solo può impossessarsi dei dati dei contribuenti, dei risparmiatori, dei legislatori, ma può determinare l'interruzione di servizi essenziali e bloccare la produzione industriale e mettere a rischio l'incolumità stessa di cittadini. Immaginatevi che cosa potrebbe succedere se ad un certo punto si spegnessero contemporaneamente in una grande città italiana i semafori, si bloccassero le operazioni chirurgiche, le ambulanze non ricevessero più le comunicazioni per andare a prendere i feriti come è successo con il *ransomware* Wannacry lanciato ai danni della Sanità inglese nel 2017. Nel 2021 un attacco cibernetico ha bloccato per giorni il ciclo dei rifiuti dell'area urbana di Firenze in Italia.

Ma cose del genere sono già successe. Nel 2013 ci fu il tentativo di aprire le chiuse della diga di New York utilizzando un telefonino. L'Estonia e l'Ucraina hanno subito il blackout della griglia elettrica a seguito di un attacco informatico. In realtà gli esempi potrebbero continuare all'infinito. Se ricordiamo la minaccia Mirai, la *botnet* che bloccò per quasi un giorno intero le comunicazioni dagli Stati Uniti verso l'Italia, per 18 ore non fu possibile raggiungere i computer che ci permettevano di accedere al New York Times, a Twitter, a Netflix, Amazon e così via. Gli attacchi cibernetici sono sempre più pericolosi: in una società digitalizzata e iperconnessa, sempre più dipendente dalla tecnologia, gli attacchi cibernetici possono fare danni enormi.

9. Perimetro nazionale

Con l'obbiettivo futuro di proteggere dati e informazioni l'Italia ha selezionato una squadra nazionale di hacker. Sono i futuri *cyberdefender*, scelti da scuole e università attraverso la *Cyberchallenge*. L'Italia ha la *Golden Power*, cioè speciali poteri di veto nei confronti di produttori e tecnologie, come il 5G, che possono rappresentare un pericolo per la democrazia e l'economia della penisola. L'Italia ha pure un *Internet kill switch*. Significa che in presenza di un rischio grave ed imminente alla sicurezza nazionale causato dalla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente del Consiglio può disporre la disattivazione, totale o parziale, di Internet. Con le necessarie garanzie di legge. Una possibilità remota, ma prevista dalla legge sul Perimetro nazionale di sicurezza cibernetica.

La legge chiarisce la costante e contemporanea evoluzione dell'assetto cibernetico italiano, la «postura», si dice in gergo, e la mette in relazione con alcuni fattori di crescita e di innovazione che in una società aperta, digitale e iperconnessa, possono trasformarsi nel loro contrario e diventare vere e proprie minacce: cioè gli algoritmi di intelligenza artificiale, la crittografia e l'informatica quantistica. Settori su cui l'Italia dovrebbe investire di più.

E tuttavia ci ricorda che con la legge sul Perimetro nazionale, grazie al raccordo con la normativa sul *Golden Power*, alla nascita del Centro di Valutazione e Certificazione Nazionale, al futuro Csirt per rispondere prontamente alle emergenze, e ai poteri speciali di intervento, l'Italia prova ad «affrontare con la massima efficacia e tempestività situazioni di rischio grave e imminente per la sicurezza nazionale in ambito cyber».

Il grande lavoro svolto dal Dipartimento informazioni per la sicurezza, DIS, ha favorito la realizzazione della legge sul Perimetro nazionale di sicurezza cibernetica. Nelle audizioni precedenti alla conversione della legge è stata detta una cosa molto importante, che il "rischio zero" non esiste e che tutti quanti noi ci dobbiamo impegnare affinché non accada che un ragazzino diciottenne dall'India possa fermare i treni che viaggiano in Italia.

La neonata Agenzia per la cybersicurezza nazionale, ACN, nata nell'agosto del 2021 dovrà mettere a sistema tutte queste innovazioni.

Quindi se la privacy è un diritto fondamentale nell'Unione europea, lo è anche la cybersecurity, la tutela cibernetica di dati, reti e informazioni sono la precondizione per esercitare altri diritti come diceva a proposito della privacy *en general* Stefano Rodotà: il diritto di associazione, di espressione, di opinione, di movimento e così via.

C'è una frase, che viene attribuita anche al presidente americano Thomas Jefferson, che dice «Chi pensa di rinunciare alla propria libertà per avere maggiore sicurezza, non merita né la libertà né la sicurezza». Voleva dire che l'equilibrio nelle scelte che

facciamo per garantire sia la libertà sia la sicurezza dovrebbe essere l'oggetto della nostra attenzione.

Il nostro Paese, a cominciare dal "decreto Monti", successivamente con il "decreto Gentiloni", la legge sul Perimetro nazionale, il recepimento della direttiva NIS, del regolamento GDPR, l'allineamento del lavoro del nostro Parlamento con il *Cybersecurity Act* europeo, ci ha permesso di rimanere saldi in questo equilibrio tra privacy e cybersecurity. Bisogna continuare così.

Negli ultimi anni gli Stati si sono distratti e hanno lasciato che poche multinazionali avessero più dati sugli italiani di quanti ne ha il Governo che protegge gli italiani. Il tema della sovranità digitale diventa il trait d'union fra la questione della privacy e la questione della sicurezza dei dati personali, comuni, aziendali, perciò non ci si può dire sovranisti senza pensare alla sovranità tecnologica e digitale. E non si può essere sovrani senza avere il controllo dei propri dati.

Con un'avvertenza: i dati vanno raccolti nel rispetto dei diritti costituzionali, archiviati in maniera sicura e trattati nel rispetto della legge. E quando si tratta di dati sensibili, come quelli relativi alla salute, vanno distrutti se non servono più.

Note

[1] Y.N. Harari, *21 Lezioni per il XXI secolo*, Bompiani, 2018.

[2] M. Castells, *Comunicazione e Potere*, Università Bocconi Editore, 2017.

[3] P. Mason, *Il Futuro migliore*, Il Saggiatore, 2019.

[4] Cfr. D. Harvey, *La guerra perpetua. Analisi del nuovo imperialismo*, Il Saggiatore, 2006; C. Formenti, *Cybersoviet. Utopie postdemocratiche e nuovi media*, Raffaello Cortina Editore, 2008; S. Zubof, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019.

[5] W. Quattrociocchi, A. Vicini, *Liberi di crederci*, Codice, 2018.

[6] K. Kelly, *Data Manifesto*, 2019.

* * *

Data commons: Privacy and cybersecurity are fundamental human rights

Abstract: Google knows more about us than we remember: it knows our daily habits and paths, it knows with whom, when and for how long we have been there; Zoom knows who we work with, Facebook puts our preferences up for auction; Twitter bots and trolls influence our views. Misinformation memes also crowd social media and pollute the scientific debate. If we do not learn to protect personal behaviors turned into digital data, we will be exposed to an uncontrollable power, that of commercial persuasion, political manipulation and state surveillance.

Keywords: Data commons – Privacy – GDPR – Cybersecurity – Big Tech

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0050

La sovranità digitale e il futuro di Internet

Vittorio Bertola

Da qualche anno si discute di sovranità digitale, ossia di come gli Stati nazionali possano porre regole alle grandi piattaforme globali di Internet a tutela della concorrenza e dei diritti degli utenti. Le politiche originarie di Internet sono infatti state sfruttate da pochi grandi attori geograficamente concentrati per creare "giardini murati". È necessario riaprire queste riserve private e ripristinare l'architettura aperta e decentrata della rete.

Internet governance – Sovranità digitale – Piattaforme internet – Concorrenza – Mercati digitali

Gli ultimi due o tre anni di dibattito sulla governance di Internet, almeno in Europa, sono stati centrati sul concetto di "sovranità digitale": un termine improvvisamente apparso sulla bocca dei leader della rete e dei politici europei, persino quelli non particolarmente specializzati nei temi digitali, e nei documenti dei centri studi e delle società di consulenza strategica. Il termine viene utilizzato per indicare la prerogativa degli Stati nazionali di imporre regole sulle attività e sull'economia della rete, persino se transnazionali e globali, quando esse riguardano i propri cittadini; viene spesso inteso in forma di rivendicazione degli Stati stessi, che ritengono di essere stati progressivamente e indebitamente privati di questa prerogativa dall'approccio globale delle grandi aziende Internet e dal modo in cui esse hanno organizzato le proprie forme giuridiche e la fornitura dei propri servizi.

Trattandosi dunque di una reazione a uno status quo che si è formato nel corso di alcuni decenni, per comprendere appieno il dibattito sulla sovranità digitale è necessario per prima cosa ripercorrere brevemente la storia della governance di Internet e la cultura collettiva che vi sta dietro. Il tema del rapporto tra le regole della rete e i governi nazionali, difatti, non è affatto nuovo; se ne parla sin da quando Internet, a metà degli anni '90, cominciò progressivamente a diventare un sistema di telecomunicazione di massa. È nuovo tuttavia lo scenario in cui esso oggi si sviluppa, che ha costretto molti sostenitori dell'Internet libera e globale ad aggiustare un po' le proprie storiche posizioni.

Internet, infatti, è storicamente un curioso e piuttosto unico caso di rete di telecomunicazione nata da investimenti essenzialmente pubblici e governativi, dell'esercito americano prima e della National Science Foundation poi, che tuttavia – in linea con il liberismo e la tendenza alla globalizzazione economica, in fulgida ascesa negli anni '80 e '90 – fu presto trasformata in un alfiere delle teorie del *laissez-faire*, all'opposto dei precedenti sistemi di telecomunicazione.

Vi è notoriamente una teoria, indubbiamente fondata, sul perché Internet abbia avuto così tanto successo da diventare il sistema protagonista di un cambiamento epocale della società umana, quello dall'era analogica a quella digitale. Alla fine del ventesimo secolo, Internet come tecnologia di telecomunicazione si trovò infatti in concorrenza sia con le

V. Bertola è ingegnere, esperto di policy e governance di Internet, responsabile delle attività di innovazione, standardizzazione e affari pubblici presso Open-Xchange.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

evoluzioni digitali dei precedenti e allora dominanti sistemi di telecomunicazione analogica, *in primis* la telefonia a rete fissa, sia con gli allora nuovi progetti proprietari di interconnessione del pianeta lanciati dalle grandi (ancorché minime rispetto a oggi) aziende digitali dell'epoca (Compuserve, AOL, Microsoft Network...). In pochi anni Internet sbaragliò questa concorrenza e divenne la tecnologia dominante, praticamente l'unica in uso, per la trasmissione dati e la fornitura di servizi digitali su scala globale. Secondo i filosofi e i teorici della rete, a garantire questo successo è stata proprio la mancanza di regolamentazione, e in particolare la libertà di connettersi alla rete e di offrire servizi senza dover pagare royalty o chiedere licenze a nessuno; il cosiddetto principio della "permissionless innovation" (innovazione senza permesso).

Se per creare un operatore telefonico o un fornitore di servizi telefonici – ammesso che la nazione in cui ci si trovava ne ammettesse più d'uno – era necessario pagare costose licenze allo Stato e seguire procedure di anni, e se per fornire servizi sulle reti private era necessario fare un accordo d'affari con le aziende che le possedevano, su Internet bastava attaccare i propri cavi a quelli degli altri, spesso con accordi di scambio dei dati alla pari, e attaccare un server a questi cavi, sul quale utilizzare gli standard aperti della rete, spesso immediatamente disponibili a chiunque sotto forma di software *open source* e gratuito, per fornire contenuti e servizi; e senza dover chiedere niente a nessuno.

Indubbiamente, questo modello deregolato fu alla base della corsa all'oro degli anni '90, della prima ondata di *startup*, del primo boom dei mercati borsistici tecnologici, concentrato su tecnologie aperte e federate che usiamo ancora oggi, in primis il Web e la posta elettronica. Grazie a questo, si crearono in tutto il mondo aziende e posti di lavoro, nacquero siti che misero enormi quantità di informazione a disposizione gratuita di tutta l'umanità, si misero in comunicazione persone e progetti in tutto il pianeta, si creò cultura, educazione, fratellanza.

Fu proprio l'entusiasmo per questa meravigliosa e rapidissima rivoluzione digitale che portò i padri della rete e i loro giovani allievi a codificare e scolpire nella pietra l'antipatia per i governi e per la regolamentazione. D'altra parte, negli anni '90 quasi tutti i governi, anche quelli più moderni e democratici, erano proprietari e monopolisti delle vecchie tecnologie di comunicazione, che erano spesso anche ottime fonti di finanziamento delle casse pubbliche; e nonostante il vento delle privatizzazioni fosse già forte, l'idea di tutelare il vecchio *business* dall'inarrestabile assalto della novità tecnologica pervase l'azione di gran parte della politica, e in molte nazioni i pionieri della rete si trovarono di fronte a regole obsolete volutamente non aggiornate, a prezzi da estorsione per l'accesso alla rete e a pura e semplice incompetenza delle pubbliche amministrazioni nella gestione di un fenomeno nuovo e mai visto prima.

Eppure, la forza del modello di Internet era già tale che i tentativi politici e affaristici di rimettere il genio nella bottiglia fallirono miseramente. L'entusiasmo era così elevato che ci fu chi ritenne che Internet fosse per costruzione e per matematica al di fuori della portata dei governi; la famosissima "Dichiarazione di indipendenza del ciberspazio" ne è l'esempio più noto. Che fosse per via di idee anarco-individualiste americane, o che fosse per via di idee internazionaliste europee, furono molti a teorizzare che Internet avrebbe semplicemente reso superflui i governi, convertito la democrazia rappresentativa in democrazia diretta, e liberato il cittadino illuminato, istruito dalla rete stessa, che avrebbe finalmente goduto della piena libertà di realizzarsi e di decidere del proprio futuro.

Presto Internet cominciò ad espandersi anche fuori dall'Occidente, in nazioni meno aperte o governate direttamente da regimi dittatoriali per cui il controllo diretto delle tecnologie dell'informazione era questione di sopravvivenza politica. Solo qualcuna di queste nazioni ebbe la forza di prendere il controllo della tecnologia, trovando dei modi e dei nodi in cui inserire qualche punto di controllo per limitarne l'uso. Molte altre sollevarono invece il problema in sede politica nell'unica istituzione globale attualmente esistente, le Nazioni Unite. Anche lì, però, il tentativo di riportare lo sviluppo degli standard e delle politiche della rete nell'alveo del ventesimo secolo, dei trattati intergovernativi e dei monopoli di Stato, fallì miseramente; ed ebbe l'unico risultato di rafforzare ancora di più l'attaccamento dei leader politici ed economici della rete al rifiuto delle "intromissioni" dei governi e del tradizionale concetto di sovranità.

Fu anzi proprio in quel periodo tra fine anni '90 e inizio anni 2000, in risposta a queste pressioni, che si concettualizzò il modello di governo della rete nel cosiddetto "multistakeholderismo". I teorici della rete libera furono comunque costretti ad accettare che anche i governi si sedessero al tavolo; del resto, è pur vero che Internet non può esistere senza tubi, antenne e calcolatori, ossia senza una infrastruttura fisica che in quanto tale si trova in un territorio nazionale, è soggetta alle leggi del mondo reale, può essere sequestrata o distrutta.

In cambio, però, i governi riconobbero che molte cose erano ormai fuori dal loro controllo, e che per orientarle serviva un dialogo con questo mondo variegato di aziende, esperti, sviluppatori indipendenti,

accademici, e persino utenti finali, la cui collaborazione o attiva opposizione avrebbe fatto la differenza nella possibilità effettiva di implementare regole nella rete con qualche successo. L'esempio clamoroso dell'industria musicale, completamente stravolta in meno di un lustro da nuove tecnologie online "pirata" che nessuna legge e nessuna agenzia pubblica riuscì a contrastare, sembrò provare l'ineluttabilità del multistakeholderismo.

Il decennio che seguì sembrò segnare il successo inarrestabile di questo modello di governo. Consolidate definitivamente realtà come IETF, ICANN e W3C, molto dello sviluppo della rete rimase libero e in mani private, mentre i governi si concentravano su pochi e urgenti problemi di criminalità in rete, in cui la rete era principalmente uno strumento e non la causa del crimine stesso. Gli standard aperti e il software open source ebbero una affermazione spettacolare, al punto che oggi a livello di infrastruttura di rete e di strumenti di base per la realizzazione di servizi online (purtroppo solo a quel livello, come vedremo presto) quasi la totalità del software utilizzato è libero.

In molti – tra cui il compianto professor Rodotà, con l'idea della Carta dei Diritti della Rete – cercarono di difendere e rafforzare lo spazio di libertà di Internet, attribuendo anzi ai governi la responsabilità di garantire a ogni cittadino la possibilità di accedervi e di usufruirne appieno. Nacquero anche veri e propri esperimenti di esportazione della democrazia online nel mondo reale: i Partiti Pirata nel centro-nord Europa, il primo Movimento 5 Stelle in Italia, altri movimenti nel mondo cominciarono a utilizzare la rete e le sue forme deliberative orizzontali per determinare l'azione politica nel campo delle istituzioni nazionali. Non ci si focalizzava quindi affatto sulla sovranità dello Stato sulla rete, ma al contrario sulla sovranità della rete sullo Stato.

Perché allora, dieci o vent'anni dopo queste esperienze, ci troviamo ora non solo davanti a una forte spinta per il ripristino della sovranità nazionale sulla rete, ma anche di fronte a una ammissione dello stesso mondo della Internet governance, anche se non condivisa da tutti, che almeno un po' di nuova "hard law" sulla rete è necessaria?

Per certi versi, la Internet del 2022 è vittima del proprio successo, e di come un successo di massa su scala planetaria inevitabilmente attiri dinamiche umane ben note: la ricerca senza limiti del potere, della ricchezza, dell'accentramento di tutto nelle mani di pochi. Ciò che è successo, infatti, è che la mancanza di regolamentazione pubblica non ha prodotto il trionfo delle libertà del singolo, della sua auto-realizzazione, delle sue opportunità di crescita; semplicemente, il vuoto lasciato dalla mancanza di regole è stato riempito dall'emersione di mega-conglomerati privati, in gran parte concentrati nella West Coast americana e in certa misura in Cina, che hanno assunto il controllo della rete e dei suoi servizi essenziali, diventandone i regolatori di fatto.

Queste aziende hanno orientato la rete non nella direzione dei diritti degli utenti finali, ma verso la creazione di un sistema economico di "capitalismo di sorveglianza" in cui la privacy viene sacrificata alle esigenze di business degli investitori pubblicitari, e la libertà di espressione viene sottomessa alle scelte private di un operatore mediatico dominante che decide cosa censurare e cosa lasciar circolare sulle proprie piattaforme.

Non è la prima volta che esistono grandi aziende tecnologiche con posizioni dominanti. In fasi diverse della storia, aziende come IBM e AT&T hanno spesso raggiunto dimensioni gigantesche grazie a ruoli centrali in tecnologie di massa; per decenni le società nazionali di telefonia e di telecomunicazione hanno fatto il bello e il cattivo tempo, ognuna nel proprio Paese. Tuttavia, una concentrazione globale a livello di quella attuale non si è mai vista nella storia dell'umanità. Al momento, le cinque aziende a maggior capitalizzazione sul mercato borsistico americano, il più importante del mondo, sono aziende di trasformazione digitale; certo, non tutte sono completamente digitali, perché alcune di esse (come Amazon o Tesla) hanno anche una significativa presenza fisica; ma sono tutte aziende costruite su Internet e sulla digitalizzazione. La capitalizzazione di Apple, al momento in cui scrivo, è vicina ai tre trilioni (tremila miliardi) di dollari; se fosse un PIL, sarebbe superiore a quello di tutte le nazioni dell'Unione Europea ad eccezione della Germania (ma, al ritmo a cui cresce il valore di Apple, la Germania potrebbe essere facilmente raggiunta e superata in un paio d'anni).

Ora, non c'è niente di male nell'iniziativa economica privata, né nel guadagnare denaro, né nell'avere successo, un successo che queste aziende hanno almeno inizialmente ottenuto grazie alla propria abilità e alla propria encomiabile capacità di investire e di disegnare il futuro, inseguendo idee che a molti altri sembravano folli e impossibili. Tuttavia, nessun privato, nessun essere umano, nessuna azienda ha mai avuto in mano un potere economico e sociale del genere su scala globale, almeno nell'era moderna. Non vi sono dunque soltanto gli evidenti rischi a livello economico, derivanti dai comportamenti anticompetitivi che queste aziende mettono spesso in atto, a giudicare dalla diretta esperienza dei mercati digitali dell'ultimo decennio e dai numerosi quanto poco efficaci provvedimenti delle autorità antitrust

di mezzo mondo. Vi sono ormai dei rischi evidenti per la stessa democrazia, per la libertà dei cittadini, per il governo non della rete, ma del pianeta Terra.

Il modello di governance multistakeholder, su questo, non ha avuto e tuttora non ha risposte. I problemi di concentrazione e di posizione dominante non si risolvono col consenso, perché nessuna azienda acconsentirà mai davvero a rinunciare al proprio fatturato, che è il sangue che la tiene viva. Senza offesa per le persone che amministrano queste aziende o che vi lavorano, non si può pensare che una vaga "etica aziendale" o un presunto amore per la natura decentrata della rete possa garantire una soluzione volontaria al problema della concentrazione di potere.

Se mai, spesso vediamo queste aziende difendere Internet dall'intromissione dei governi, invocare un mondo senza più Stati e confini, proclamare l'importanza della libertà e della privacy degli utenti rispetto alle possibili attività di forze dell'ordine e governi nazionali, ripetendo i concetti dell'epoca d'oro del pensiero libertario della rete, e non sappiamo se dicano queste cose perché ci credono, perché fa parte della loro cultura, o se lo facciano semplicemente perché i governi sono ormai l'unico *stakeholder* che ha forse, e sottolineo forse, la possibilità coercitiva per spezzare le loro posizioni dominanti.

Eppure, anche chi come il sottoscritto ha vissuto con entusiasmo l'epoca dell'Internet libera e globale deve riconoscere che l'Internet di oggi è ancora globale, con l'eccezione della Cina, ma è molto meno libera di quella di dieci o vent'anni fa.

Se vent'anni fa chiunque di noi aveva un sito personale e un blog, ed esistevano aggregatori e applicazioni di ogni tipo per raccogliere i contenuti, oggi le notizie e il dibattito pubblico in rete passano quasi per intero tramite una singola interfaccia di un singolo social network, Facebook, che ha potere di vita o di morte sulla persona digitale di ognuno di noi; proprio volendo, si possono trovare delle alternative – Twitter, TikTok – anch'esse però costruite non come strumento orizzontale di collaborazione aperta tra pari, ma come piccoli aspiranti monopolisti che non ce l'hanno ancora fatta.

Se vent'anni fa i primi sistemi di e-commerce permettevano a giovani startup e a piccole aziende locali di fare il salto di dimensione e diventare grandi aziende internazionali, oggi sempre di più tutto il commercio online passa tramite il catalogo e la logistica di un solo operatore globale, Amazon.

Se all'inizio Internet era una opportunità per trovare lavoro più facilmente o per costruirselo dal nulla, oggi le piattaforme di delivery ingaggiano i più derelitti delle nostre società e li spediscono in bicicletta sotto la neve a consegnare hamburger freddi a yuppie distratti, tracciando e cronometrando i loro spostamenti in una nuova forma di schiavitù. Alla base di questi rapporti di forza tra una grande azienda e la popolazione mondiale vi è uno squilibrio di potere, legato all'impossibilità per gli utenti della rete sia di spostarsi con facilità in una piattaforma alternativa, sia di crearsene una da soli secondo il modello dell'innovazione senza permesso, che ormai esiste soltanto come teoria.

Molto è legato al cosiddetto "effetto rete": se tutti già usano la piattaforma dominante, chi prova a creare un servizio concorrente è svantaggiato per la mancanza di economia di scala e per la mancanza di utenti. Questo è particolarmente evidente in servizi puramente immateriali, come la messaggistica: io posso anche inventarmi un'app di messaggistica mille volte migliore di Whatsapp, ma se tutti i miei contatti usano Whatsapp la mia nuova app sarà totalmente inutilizzabile, perché non avrò nessuno a cui scrivere; dovrei convincere in blocco tutti i miei contatti a muoversi sulla nuova piattaforma, ma anch'essi avranno altri contatti rimasti sulla vecchia piattaforma, e così via; dunque la rete di relazioni interpersonali cattura e vincola tutti gli utenti insieme.

Spesso, quindi, per creare più concorrenza e limitare naturalmente queste posizioni dominanti sarebbe sufficiente ritornare al modello originario della rete, non solo nelle parole e negli slogan, ma anche nelle scelte tecniche. Tra i principi architetturali di Internet, così come erano stati riconosciuti negli anni '90, ci sono la *modularità* – spezzare i servizi in blocchi più piccoli ognuno dei quali può essere fornito da un operatore diverso, senza per forza costringere l'utente a usare un "ecosistema" in cui il sistema operativo del cellulare impone di fatto anche il motore di ricerca, il servizio di posta elettronica e persino il metodo di pagamento per gli acquisti online – e la *standardizzazione* – costruire soluzioni concorrenti in modi simili e compatibili, con le stesse interfacce verso l'esterno, in modo che siano tra loro sostituibili senza sforzo. Questi due principi insieme creano l'*interoperabilità*: la possibilità per l'utente di scegliere e cambiare l'applicazione, il dispositivo, il sito che fornisce un determinato servizio e di usarli per interagire con tutti gli altri utenti della rete, compresi quelli che utilizzano fornitori diversi.

Per esempio, se Whatsapp fosse costretta a offrire una interfaccia aperta per scambiare messaggi con gli utenti di altre applicazioni di chat, l'utente potrebbe cambiare app di messaggistica – magari scegliendone una nuova, innovativa, appena prodotta da una *startup* – continuando però a parlare con tutti i propri contatti che ancora utilizzano Whatsapp. La posta elettronica funziona in questo modo: io posso

acquisire una casella di posta elettronica da qualsiasi operatore e usarla per parlare anche con gli utenti di tutti gli altri operatori in tutto il mondo. La stessa cosa accade per la telefonia; col mio numero posso chiamare qualsiasi altro numero di telefono di qualsiasi operatore al mondo. Non c'è alcun motivo tecnico per cui i messaggi istantanei debbano funzionare diversamente; è solo una scelta di business.

Il problema, come dicevamo, è che chi gestisce le piattaforme dominanti è ben cosciente del fatto che permettere l'interoperabilità facilita di molto la nascita di potenziale concorrenza. Per questo motivo, le piattaforme dell'ultimo ventennio sono state costruite come dei "walled garden": una volta entrati, gli utenti insoddisfatti che potrebbero voler uscire si trovano di fronte a tante e tali barriere che cambiare fornitore e servizio diventa quasi impossibile. Abbattere i muri dei giardini è un modo di promuovere nuova concorrenza senza per forza dover intervenire con misure più invasive; ma non succederà se le piattaforme non vengono costrette a farlo.

È questo il punto in cui nella storia di Internet rientra dunque in gioco la sovranità nazionale; il governo, espressione democratica dei cittadini, può essere l'attore che per conto di tutti noi determina e mette in atto le regole necessarie a tutelare la società dal potere eccessivo di una singola azienda e dei privati che la possiedono.

C'è indubbiamente in questo, come lamentano gli oppositori di quest'idea, un elemento di nazionalismo; è però un nazionalismo necessario, reso obbligatorio dalla mancanza di un governo democratico globale del pianeta che possa imporre queste regole su scala internazionale. Non essendoci autorità pubbliche globali dotate di potere coercitivo e dei mezzi per esercitarlo, è necessario ritornare ai governi nazionali, gli unici ad avere qualche possibilità di imporre queste regole (sempre che i governi nazionali non siano già troppo influenzati da queste grandi aziende, spesso altrettanto o più grandi di loro in termini economici; a giudicare dalle posizioni di qualche nazione europea sui tentativi di imporre alle piattaforme Internet globali il pagamento di tasse giuste in tutti i Paesi in cui operano, questo pare un dubbio decisamente motivato).

C'è indubbiamente in questo, almeno in Europa, anche un elemento di protezionismo economico. Molta della ricchezza che queste aziende estraggono dalle economie nazionali non resta nel Paese, ma viene portata alla casa madre e ai soci, negli Stati Uniti o in paradisi fiscali di vario genere. Se il costo della vita in Silicon Valley è andato alle stelle, al punto che bisogna essere miliardari per permettersi un appartamentino a San Francisco, è proprio per questo enorme flusso di ricchezza che da tutto il mondo è "atterrato" in quel lembo di terra. Se è pienamente legittimo che un imprenditore californiano cerchi di conquistare mercati in altre nazioni, è anche ragionevole che quelle nazioni possano pensare a un certo punto di dover favorire la nascita di propri operatori nazionali che paghino tasse e generino indotto sul posto, pena lo svuotamento progressivo delle proprie casse pubbliche e della propria economia. Mentre sarebbe sbagliato chiudere i confini del tutto, perché alla lunga l'isolamento danneggia e lascia indietro le nazioni, è invece ragionevole cercare di ripristinare opportunità di concorrenza che permettano a imprenditori nazionali di offrire ai propri cittadini delle alternative locali, competendo lealmente sul mercato a condizioni eque senza doversi scontrare con posizioni dominanti e con le tecniche messe in atto per renderle perpetue.

C'è indubbiamente in questo anche un elemento culturale. Persino su diritti fondamentali come la libertà di espressione, l'interpretazione varia anche all'interno dell'Occidente. Mentre negli Stati Uniti vi è una interpretazione costituzionale massimalista della libertà di espressione del singolo, in molte nazioni europee esistono contenuti che non devono circolare; è illegittimo incitare al razzismo, promuovere il terrorismo, distribuire materiale abusivo sui bambini, o anche vendere farmaci illegali e trasmettere partite di calcio senza autorizzazione. Anche qui, in attesa di un governo globale e di una uniformità culturale – ammesso che una uniformità culturale sia davvero desiderabile – esiste naturalmente la necessità di garantire a ogni nazione la possibilità di decidere per sé cosa i propri cittadini possano o non possano immettere in rete, secondo i propri processi democratici. Ancorché ben intenzionata, l'idea di utilizzare la rete e la dominanza delle piattaforme americane per imporre a forza anche in Europa e nel resto del mondo una libertà di espressione illimitata, oltre che irrispettosa della storia e della cultura delle varie nazioni, è comunque una forma di imperialismo culturale.

C'è infine indubbiamente in questo un elemento di sicurezza nazionale. È un elemento delicato da trattare, perché ipotizzare tensioni internazionali è spesso il miglior modo per farle nascere. Tuttavia, la dipendenza delle nostre società da Internet è tale che nessun Paese può permettersi il rischio che servizi largamente utilizzati per il funzionamento delle imprese e per la vita quotidiana dei cittadini diventino improvvisamente indisponibili a causa di un embargo o di uno scontro geopolitico.

Persino se le aziende fornitrici non intendessero prestarsi a questo gioco, lo Stato presso cui esse hanno sede può semplicemente imporglielo; i cittadini di Paesi come Iran o Cuba conoscono bene la difficoltà

di accedere a servizi apparentemente globali e tecnicamente neutri, come la registrazione di un dominio *.com* o l'acquisizione di un certificato per un sito Web in HTTPS, perché alla fine tali servizi sono forniti da società americane che per legge della loro nazione non possono accettarli come clienti. Le ordinanze del presidente Trump contro Huawei dimostrano come persino grandi aziende nazionali, portatrici di lavoro e ricchezza nel proprio Paese, possano essere pesantemente danneggiate per scelta di un altro Paese; e il CLOUD Act, la legge che obbliga le aziende americane a fornire alle autorità americane accesso ai dati personali e alle comunicazioni dei cittadini di altri Paesi anche avvenute e conservate all'estero se l'azienda americana ha accesso ai relativi server, mette a rischio la sicurezza e la privacy delle comunicazioni di qualsiasi cittadino o azienda europea.

Per una nazione come l'Italia e per l'Unione europea esistono dunque molti validi motivi per adottare una politica di sovranità digitale, declinata in almeno due diversi aspetti: una ricerca di "autonomia digitale", ovvero di disporre sul proprio territorio e dentro la propria giurisdizione di tutti i servizi Internet che possano permettere all'economia e alla società di funzionare anche in caso di conflitto commerciale e geopolitico (o in caso estremo militare) con Paesi esteri, e una ricerca di sovranità vera e propria, ossia della capacità di porre regole e farle rispettare anche ad attori che non sono basati nella propria giurisdizione, ma che comunque possiedono in essa quote di mercato rilevanti o addirittura dominanti, assumendo un ruolo fondamentale nella vita online del Paese.

Dal punto di vista di chi ha costruito e promosso Internet nel corso degli ultimi decenni, è necessario continuare a sottolineare il suo potere benefico e positivo e l'importanza della sua natura globale, ma è anche necessario rispondere a queste richieste della politica con comprensione e intelligenza. Sarebbe sbagliato contestarle o opporvisi del tutto; in tal modo, si diventerebbe semplicemente strumenti di una dominazione economica e sociale privata, contribuendo alla crescita di una contrapposizione tra industria Internet e Stati nazionali che alla lunga potrebbe solo portare alla distruzione dell'Internet globale e alla sua frammentazione in reti nazionali molto più controllate, seguendo il modello cinese.

Peggio di tutto, è sbagliato rispondere a problemi politici complessi con l'adozione unilaterale di strumenti tecnici che rendano impossibile la loro risoluzione. Il miglior esempio di questa attuale tendenza è il modo in cui diverse aziende Internet stanno introducendo la cifratura generalizzata di tutte le connessioni dei loro dispositivi, spesso associata alla centralizzazione nelle loro mani del traffico e dei servizi. Abbiamo visto browser che improvvisamente vogliono smettere di usare il server DNS locale, sul quale il provider Internet, lo Stato nazionale e l'utente stesso possono configurare forme di controllo o blocco dei contenuti in linea con le loro esigenze e con la legislazione nazionale in materia, e aprono connessioni cifrate verso un server DNS gestito da una grande azienda americana, giurando che questa azienda si è impegnata a non usare i dati per tracciare gli utenti e a non manipolarne le connessioni. Abbiamo visto un produttore dominante di smartphone come Apple introdurre, per ora in maniera opzionale, un servizio per cui tutto il traffico del dispositivo viene cifrato e deviato su un server di Apple stessa e poi su altri server di propri partner commerciali, anche qui in nome della privacy, ma col rischio incancellabile che in futuro queste aziende si organizzino tra di loro per tracciare tutto il traffico dell'utente.

Questi cambiamenti vengono introdotti dalle aziende nel nome degli utenti, con lo scopo dichiarato di impedire qualsiasi possibile tracciamento da parte degli Internet provider e qualsiasi tipo di intercettazione da parte dei governi e delle forze dell'ordine, ma rendono di fatto impossibile ai governi l'esercizio della propria sovranità digitale. Inoltre, esse privano l'utente stesso di qualsiasi possibilità di affidare a strumenti terzi di suo gradimento, come un proprio router o un servizio di sicurezza gestito dal proprio provider Internet, il controllo su ciò che gli applicativi e i dispositivi di queste grandi piattaforme fanno con i suoi dati. Visto che l'industria che persegue queste scelte è una industria che ha collettivamente inventato il "capitalismo di sorveglianza" e che è sempre affamata di dati per alimentare i propri algoritmi di intelligenza artificiale, permettete di esprimere anche qui qualche dubbio sul fatto che le motivazioni ultime siano a vantaggio dell'utente finale.

Di fatto, le nostre case si stanno riempiendo di "assistenti digitali", di app e di dispositivi che passano il tempo a osservare ciò che vi avviene e a inviare dati non meglio precisati a un server centrale, tramite connessioni cifrate che non possono essere monitorate e spesso nemmeno bloccate, neanche da un utente esperto che volesse esplicitamente farlo. Questo sì che è uno scenario di sorveglianza globale, per di più in mano ad aziende private generalmente americane o cinesi, completamente fuori dal raggio d'azione della nostra democrazia. Nessun governo attento e sano di mente può accettare una evoluzione tecnologica di questo genere, che ha come conseguenza, voluta o meno che sia, quella di rendere il governo stesso impotente e inoffensivo per gli interessi economici delle grandi piattaforme.

Chi ha veramente a cuore i principi originari della rete deve dunque cercare di difenderli da possibili attacchi da entrambi i lati, quello dei governi e quello delle aziende, mirando a un equilibrio che mantenga al centro l'utente finale, i suoi diritti e le sue prerogative. In quest'ottica, è possibile immaginare scelte architetturali e scelte legislative tra di loro complementari, che preservino la natura unica e globale della rete, ma che codifichino sin nell'organizzazione tecnica dei servizi e dei protocolli spazi di sovranità digitale per ciascun Paese, in base al luogo e alla cittadinanza dell'utente finale.

I recenti progetti di legge in esame a livello europeo, che al momento in cui scrivo non sono ancora finalizzati e che dunque potremo valutare appieno solo se e quando il loro iter sarà concluso con un testo definitivo, presentano però già nelle attuali bozze richiami importanti ai principi architetturali dell'Internet delle origini, compresi quelli già citati di modularità, standardizzazione e interoperabilità. Leggi che sanciscano questi principi come vincolanti, lasciando poi a una fase di implementazione amministrativa la loro declinazione su specifici prodotti e servizi, e a una fase di standardizzazione tecnica supervisionata dalle autorità pubbliche la definizione degli standard tramite cui implementarli, possono essere molto utili a ripristinare la concorrenza e le possibilità di scelta degli utenti della rete, da cui peraltro dipende spesso anche la difesa dei loro diritti (attualmente molti utenti preferirebbero servizi online non basati sulla pubblicità personalizzata e tracciante, ma questi servizi semplicemente non esistono perché quelli dominanti sono tutti basati su tale modello).

Contemporaneamente, la comunità tecnica della rete deve imparare a comprendere le istanze di sovranità degli Stati democratici e a collaborare con esse, anziché ignorarle o peggio, come nei casi più sopra citati, sviluppare nuove tecnologie e nuovi standard in modo da ostacolare tali istanze il più possibile.

Paradossalmente, in un braccio di ferro tecnico tra aziende e governi sulla possibilità di inserire per esempio un controllo sull'accesso dell'utente a potenziali contenuti illegali o pericolosi (*malware*, *phishing* eccetera), il più danneggiato è l'utente: alla fine i governi non possono rinunciare a implementare le leggi che i loro Parlamenti hanno deliberato, per cui lo faranno comunque con gli strumenti tecnici a disposizione. Più gli strumenti sono grezzi e non standardizzati, più essi avranno effetti collaterali negativi, come il blocco di altri contenuti perfettamente legittimi, e creeranno esperienze utente poco piacevoli, come le connessioni bloccate all'infinito invece di una comprensibile pagina d'errore, col rischio di alienare all'uso di Internet le fasce sociali che già hanno meno dimestichezza con essa e più timore di subire truffe e attacchi cibernetici.

Al contrario, gli standard tecnologici potrebbero codificare i modi in cui inserire controlli sanciti per legge, garantendone così l'efficacia, la correttezza tecnica, l'autenticazione e la semplicità per l'utente; sarebbe poi lasciata alla sovranità di ciascun Paese la decisione sul se e sul come utilizzare questa possibilità, sollecitando o imponendo ai produttori del software e dei dispositivi e ai fornitori dei servizi il rispetto di una policy nazionale quando l'utente si trova sotto la relativa giurisdizione.

In fondo, anche questo sarebbe un modello di governance *multi-stakeholder*, solo non dominato esclusivamente dai grandi attori privati e legato anche alle scelte dei legittimi governi di ciascun Paese, sperabilmente definite tramite processi democratici. Alla fine, ci sono voluti secoli per creare la democrazia rappresentativa come la conosciamo oggi; essa è probabilmente, come si usa dire, "il peggior sistema di governo esclusi tutti gli altri". Le critiche al funzionamento della democrazia rappresentativa sono legittime e spesso fondate, ma una Internet globale in cui la gran parte del potere di definire le regole e determinare il futuro è concentrata nelle mani di poche enormi aziende è senz'altro molto meno democratica del mondo reale.

In fondo, noi possiamo almeno votare per i nostri rappresentanti politici nazionali ed europei, mentre non possiamo eleggere l'amministratore delegato di Google o di Apple. Solo se riusciremo a ripristinare un equilibrio geopolitico ed economico e a riportare il potere di scelta e il controllo sulla rete nelle mani dei suoi utenti sparsi in tutto il mondo, avremo difeso con successo lo spirito di Internet e saremo pronti per scrivere ancora molti nuovi luminosi capitoli della sua storia.

* * *

Digital sovereignty and the future of the Internet

Abstract: The last few years saw the rise of digital sovereignty, the idea that nation States must be able to regulate the big global Internet platforms to uphold competition and user rights. The original Internet policy principles were exploited by a few big and geographically concentrated actors to create "walled

gardens". There is the need to open up these private enclosures and restore the open and decentralized architecture of the Internet.

Keywords: Internet governance – Digital sovereignty – Platform regulation – Competition – Digital markets

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0058

Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance

Mauro Santaniello

Questo saggio descrive e analizza la recente svolta normativa nelle politiche digitali dell'Unione europea, e il tentativo delle istituzioni europee di produrre un nuovo modello globale di Internet governance. L'analisi suggerisce che la peculiarità di tale modello si sostanzia nella combinazione di due distinti framework normativi: il costituzionalismo digitale e la sovranità digitale. In particolare, le nuove proposte legislative dell'UE in materia di digitale mostrano come l'azione regolativa delle istituzioni europee miri, da un lato, alla definizione di un insieme di diritti digitali fondamentali, e, dall'altro, alla costituzione di un complesso di poteri pubblici atti a porre limitazioni effettive all'esercizio del potere digitale.

Internet governance – Sovranità digitale – Costituzionalismo digitale – Diritti digitali

Sommario: *1. Introduzione – 2. Il costituzionalismo digitale e il ruolo delle istituzioni democratiche – 3. La sovranità digitale europea – 4. Conclusioni*

1. Introduzione

Negli ultimi cinque anni le strategie e le politiche europee relative alla governance globale di Internet hanno segnato una repentina inversione di tendenza. L'approccio conservatore che l'Unione europea aveva adottato sin dai tempi del World Summit on the Information Society (WSIS) del 2003 e 2005 ha lasciato il posto a istanze di riforma dell'Internet governance formulate ai più alti livelli istituzionali. Questa svolta riformista si è sostanziata in dichiarazioni e discorsi programmatici di esponenti politici di primo piano, sia dell'Unione che degli Stati membri, nelle iniziative di autorità di regolazione e controllo, in diversi e numerosi documenti di policy, e soprattutto in nuovi processi legislativi che, nell'insieme, testimoniano un cambiamento di paradigma delle politiche digitali UE. Tale trasformazione, come si argomenterà nelle pagine che seguono, si colloca all'incrocio tra due modelli normativi emersi di recente nel dibattito sulla governance di Internet. Il primo è quello del costituzionalismo digitale, che pone al centro dell'azione istituzionale la tutela dei diritti degli utenti delle reti e la salvaguardia dei principi liberal-democratici nello spazio cibernetico. Il secondo modello alla base delle nuove iniziative europee è quello della cosiddetta sovranità digitale, un principio di policy che, in varie forme, tende a riarticolare la distribuzione del potere digitale tra attori statali, privati e della società civile.

Per meglio comprendere i cambiamenti in atto e valutarne la portata politica, questo articolo traccia il perimetro e la direzione di quella che va configurandosi come una terza via nella governance globale di Internet. In particolare, il prossimo paragrafo identifica i tratti principali del modello costituzionalista

M. Santaniello è ricercatore di Scienza politica presso il Dipartimento di studi politici e sociali dell'Università degli Studi di Salerno, dove insegna "Internet governance" e "Politiche digitali".

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

di Internet governance. Successivamente, si analizza il principio della sovranità digitale così come è stato elaborato nell'ambito delle politiche digitali dell'Unione europea, evidenziandone la sostanziale differenza rispetto agli approcci sovranisti all'Internet governance che negli anni hanno caratterizzato l'azione di alcuni potenti governi nazionali. Il paragrafo seguente evidenzia come la sovranità digitale europea, intersecandosi con il modello del costituzionalismo digitale, produca un approccio nuovo alla governance di Internet, distinto tanto dal modello neoliberale promosso dagli USA e dalle *digital corporation*, quanto dalle aspirazioni sovraniste dei regimi autoritari.

2. Il costituzionalismo digitale e il ruolo delle istituzioni democratiche

Il termine "costituzionalismo digitale" è stato reso popolare da un report di ricerca del Berkman Center for Internet and Society dell'Università di Harvard[1]. Gli autori del paper definivano il costituzionalismo digitale come «una costellazione di iniziative che hanno provato ad articolare un insieme di diritti politici, norme di governance, e limitazioni all'esercizio del potere su Internet»[2]. A partire da questa definizione operativa, numerosi studi, prevalentemente di tipo politologico e giuridico, si sono concentrati sull'analisi di dichiarazioni, carte, bill of rights, atti e testi legislativi, cercando di delineare l'insieme dei diritti digitali che le diverse iniziative andavano configurando[3], di chiarire i controversi rapporti che intercorrono tra discorso politico e processi di costituzionalizzazione della rete[4], di definire le specificità del linguaggio utilizzato nei documenti da diversi attori[5], e di investigare le motivazioni dei soggetti coinvolti nella produzione di testi proto-costituzionali[6]. Attualmente, il Digital Constitutionalism Network, ossia la principale rete internazionale di studiosi impegnati nell'analisi del costituzionalismo digitale[7], censisce più di duecento iniziative che rientrano nel perimetro della definizione proposta dai ricercatori del Berkman Center. Da una prospettiva teorica, il costituzionalismo digitale, così definito, si inserisce nel quadro del cosiddetto "costituzionalismo sociale"[8], ossia in quei processi di costituzionalizzazione autopoietica che si attivano nella sfera transnazionale sulla spinta di soggetti che operano al di fuori di un contesto strettamente politico, come le organizzazioni non governative e le comunità epistemiche. In effetti, sin dalla metà degli anni '90, numerose iniziative bottom-up si sono poste l'obiettivo di produrre strumenti normativi efficaci per la protezione dei diritti degli utenti delle reti digitali, mobilitando soggetti della società civile, accademici e membri della comunità tecnica di Internet. Un incremento significativo di tali iniziative si è poi registrato a partire dal 2013, a seguito delle rivelazioni di Edward Snowden sui programmi di sorveglianza elettronica di massa implementati da alcuni governi occidentali con la complicità di alcune grandi corporation del digitale[9]. In anni più recenti, il costituzionalismo digitale è andato configurandosi come una forma di "costituzionalismo ibrido"[10], che alle norme e ai principi elaborati dagli attori sociali ha affiancato un processo di formalizzazione politica e legale che ha coinvolto in misura crescente le istituzioni dei Paesi democratici. Alcuni esempi di codificazione politica dei diritti digitali sono la Dichiarazione italiana dei diritti in Internet[11], fortemente voluta da Stefano Rodotà, e la recente "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale" elaborata dalla Commissione europea e da quest'ultima inviata al Parlamento europeo e al Consiglio il 26 gennaio 2022 per una sottoscrizione congiunta[12]. Sebbene si tratti di testi non vincolanti da un punto di vista giuridico, essi rappresentano un riconoscimento importante delle aspirazioni democratiche e costituzionali delle istituzioni che le hanno prodotte. E fungono da linee guida per i successivi processi di lawmaking e policy-making nei rispettivi contesti. Il testo della Commissione, ad esempio, chiarisce che:

> «La dichiarazione mira a illustrare le intenzioni politiche comuni. Non solo ricorda i diritti più pertinenti nel contesto della trasformazione digitale, ma dovrebbe anche fungere da punto di riferimento per le imprese e altri soggetti interessati allo sviluppo e alla diffusione di nuove tecnologie. La dichiarazione dovrebbe inoltre guidare i responsabili politici nella riflessione sulla loro visione della trasformazione digitale.» (Preambolo, par. 5)

La dichiarazione è solo il punto di approdo di una lunga riflessione su democrazia e diritti nell'ambiente digitale condotta dai principali organismi dell'Unione europea. Ad esempio, la Risoluzione del Parlamento europeo del 20 ottobre 2020 pone al centro delle politiche digitali dell'Unione i diritti fondamentali e le libertà dei suoi cittadini, tra cui le libertà di espressione, informazione e opinione, la libertà di stampa e il pluralismo delle fonti di informazione, la protezione da forme di manipolazione e discriminazione algoritmica, la portabilità dei dati, il diritto alla privacy e alla protezione dei dati, il divieto di archiviazione centralizzata dei dati biometrici, il diritto a un giusto processo e alle garanzie procedurali nei casi di investigazioni informatiche, la criptazione dei dati end-to-end, la trasparenza e l'accountability dei sistemi automatici di decision-making, l'istituzionalizzazione di sistemi di controllo delle intelligen-

ze artificiali, eccetera[13]. Analogamente, il Consiglio dell'Unione europea, nella "Dichiarazione di Berlino sulla società digitale e su un governo digitale fondato sui valori"[14] e nella "Dichiarazione di Lisbona – Democrazia digitale con uno scopo"[15], ha evidenziato la necessità di incanalare la trasformazione digitale nel solco dei valori della *good governance* europea. Queste forme di costituzionalismo digitale condividono con la lunga tradizione degli Internet Bill of Rights il loro carattere di testi non vincolanti, privi di un impianto sanzionatorio e di meccanismi di enforcement. Essi, d'altra parte, hanno prodotto un discorso di policy che di recente si sta istituzionalizzando attraverso una formalizzazione giuridica di diritti e principi, come nel caso delle ultime iniziative legislative dell'Unione in tema di digitale: il Digital Services Act (DSA), il Digital Markets Act (DMA), e l'Artificial Intelligence Act (AIA). In questi atti, il processo di ibridazione del costituzionalismo digitale è evidente. Da un lato, infatti, essi muovono dalla premessa comune della necessità di proteggere i diritti fondamentali dei cittadini dell'UE e i principi di governance delle istituzioni europee. Dall'altro, essi elaborano una complessa architettura di poteri di controllo e sanzione che rende effettive e azionabili le garanzie poste a difesa dei diritti e le limitazioni all'esercizio del potere digitale da parte di organismi statali e di corporation private. È lungo questa direttrice che si realizza un processo di maturazione del costituzionalismo digitale, che non si limita più a una mera elencazione di diritti e principi, ma si spinge fino a costruire, e a organizzare, un nuovo insieme di poteri pubblici, il cui esercizio è posto in capo a vecchie e nuove istituzioni.

3. La sovranità digitale europea

Le rivendicazioni di sovranità da parte degli Stati nazionali nell'ambito della governance globale di Internet non sono una novità. Già ai tempi del WSIS diversi governi avevano manifestato la propria insoddisfazione rispetto al regime di self-regulation costruito dal governo statunitense attorno alla Internet Corporation for Assigned Names and Numbers (ICANN), e avevano avanzato le proprie ambizioni di ricondurre il governo di infrastrutture e protocolli in ambito intergovernativo, e in particolare all'interno della International Telecommunications Union (ITU) delle Nazioni Unite[16]. Negli ultimi anni, però, le rivendicazioni di sovranità sulle reti digitali si sono diffuse anche in numerosi Paesi occidentali. In particolare nell'Unione europea e in alcuni dei suoi Stati membri, la sovranità digitale è diventata una preoccupazione cruciale per i leader politici e i funzionari pubblici[17]. Nelle istituzioni dell'UE, il termine sovranità digitale è stato impiegato per la prima volta in un paio di pareri ufficiali del Comitato europeo delle regioni e del Comitato economico e sociale europeo. Successivamente, il termine è stato utilizzato da leader politici di primo piano, tra cui i ministri dell'Economia di Germania e Francia durante la presentazione ufficiale del progetto Gaia-X nell'ottobre 2019, la cancelliera tedesca Angela Merkel durante il discorso di apertura dell'Internet Governance Forum del 26 novembre 2019, il governo tedesco nel suo programma per la presidenza del Consiglio dell'Unione europea nel luglio 2020, e la presidente della Commissione europea Ursula von der Leyen durante il suo discorso sullo stato dell'Unione del 16 settembre 2020. Da lì, l'espressione sovranità digitale si è diffusa in una lunga serie di recenti documenti ufficiali dell'UE, alcuni di carattere strategico, come la "Nuova strategia industriale per l'Europa" della Commissione (10 marzo 2020), le conclusioni del Consiglio "Plasmare il futuro digitale dell'Europa" (9 giugno 2020), le raccomandazioni della Commissione per un approccio comune al 5G (18 settembre 2020), le conclusioni del Consiglio sulla sicurezza cibernetica dei dispositivi interconnessi (10 dicembre 2020), le "Priorità legislative dell'UE per il 2021" (18 gennaio 2021), la "Bussola per il digitale 2030: il modello europeo per il decennio digitale" (9 marzo 2021), e nei documenti connessi alle nuove regulation come il DSA, il DMA e l'AIA.

In sintesi, questi documenti e i numerosi altri piani, programmi e interventi europei ispirati al principio della sovranità digitale delineano un modello di intervento regolativo che mira a contemperare, da una lato, le esigenze dello sviluppo economico del settore digitale e la capacità di innovazione del tessuto imprenditoriale europeo, e, dall'altro, gli interessi economici e politici dell'Unione. Il DSA, ad esempio, introduce una nuova serie di obblighi di trasparenza e accountability per quelle che definisce "very large online platform", con l'obiettivo dichiarato di sottoporre queste ultime a un "maggiore controllo democratico"[18]. Con tale finalità, il DSA riduce l'ambito di applicazione delle esenzioni di responsabilità previste dalla direttiva eCommerce del 2001, ridefinendo il concetto di piattaforma digitale: non più semplice intermediario di un mercato "multi-sided", ma ecosistema generativo che ha precise responsabilità verso cittadini e autorità pubbliche. Analogamente, il DMA riconosce alle piattaforme digitali una funzione di gatekeeping, che conferisce loro «il potere di agire come rule-makers privati» che si collocano come «colli di bottiglia tra aziende e consumatori»[19]. In virtù di tale riconoscimento, la proposta legislativa prevede un elenco molto dettagliato di obblighi e

proibizioni, corredato da dispositivi sanzionatori e di controllo affidati direttamente alla Commissione. In modo simile, l'Artificial Intelligence Act si propone di affrontare i rischi sociali e individuali dello sviluppo delle intelligenze artificiali attraverso disposizioni legislative che ne assicurino la coerenza con «i valori, i diritti fondamentali e i principi dell'Unione»[20]. È evidente, dunque, che il framework della sovranità digitale si pone in continuità, e a completamento, del framework del costituzionalismo digitale, dotando quest'ultimo di una serie di strumenti – e poteri – che abilitano a un'efficace protezione dei diritti[21]. È qui che si realizza la specificità politicamente più significativa della sovranità digitale europea rispetto agli approcci sovranisti dei Paesi autoritari. Mentre per questi ultimi il principio della sovranità è un fine in sé, che discende da un modello westfaliano dei rapporti interstatali, la sovranità digitale europea viene intesa come un mezzo per giungere a una protezione efficace dei diritti fondamentali dei cittadini dell'Unione e per promuovere i valori e i principi delle democrazie liberali. Da questa prospettiva, la sovranità digitale europea è un progetto politico chiaramente anti-sovranista, che oppone alle istanze nazionaliste e isolazioniste dei singoli Paesi un approccio polifonico e partecipato, aperto alle differenze culturali degli Stati membri e al contributo della società civile. Questo orientamento all'apertura e alla partecipazione è particolarmente evidente quando si analizza l'oggetto delle istanze di sovranità digitale. Mentre le ambizioni dei governi di Russia e Cina dei primi anni 2000 si concentravano principalmente sulla governance dei protocolli e delle risorse critiche di Internet, ossia di quegli elementi della rete che consentono l'interoperatività globale dei diversi network, la sovranità digitale europea è intesa soprattutto come forma di limitazione all'esercizio del potere da parte delle grandi piattaforme digitali. Vi è, nel caso europeo, il tentativo di democratizzare e costituzionalizzare Internet, e questo rappresenta un progetto politico completamente diverso rispetto ai piani di frammentazione e territorializzazione delle reti della comunicazione digitale[22].

4. Conclusioni

L'intersezione tra i principi della sovranità digitale e quelli del costituzionalismo digitale rappresenta la caratteristica principale delle recenti politiche UE sul digitale. Sebbene molti dei processi di policy cui si è fatto riferimento in questo breve contributo siano ancora in divenire, e il loro esito non possa darsi per scontato, essi rimandano inevitabilmente a un progetto politico di più ampio respiro, che mira a realizzare una terza via alla governance di Internet, alternativa tanto al modello di *private self-regulation* promosso dagli USA quanto al modello statocentrico a guida governativa sostenuto dai regimi autoritari. Questa osservazione conclusiva rimanda a un ormai celebre discorso tenuto dal Presidente francese Emmanuel Macron durante la cerimonia inaugurale dell'Internet Governance Forum del 2018. In quell'occasione, infatti, il leader francese invocò un "movimento di riforma" nella Internet governance globale, basato su forme di regolamentazione democratica. Macron parlò apertamente della necessità di istituire «nuove forme di cooperazione multilaterale», e di addivenire a un modello di governance che si opponesse, ad un tempo, al modello californiano "di completa autogestione", descritto come fondamentalmente antidemocratico, e al modello cinese in cui lo Stato è egemonico e i diritti individuali non sono garantiti[23]. In poco più di tre anni, quella visione politica si è rapidamente diffusa in Europa, iniziando a materializzarsi in iniziative e processi tangibili sia sul piano politico che su quello giuridico. D'altra parte, numerose sono le insidie che un simile percorso ha ancora dinanzi a sé. La capacità di lobbying delle grandi *digital corporation* è già stata dispiegata, anche a Bruxelles, per ostacolare gli avanzamenti più radicali del progetto di democratizzazione di Internet, e non sarà facile liberarsene se si considerano la quantità e la qualità delle risorse che questi soggetti hanno a disposizione. Inoltre, l'escalation di tensioni geopolitiche, anche in Europa, rappresenta un altro grande limite a un'azione costituzionalizzante di Internet basata sui diritti, in quanto diventano sempre più concreti i pericoli di una militarizzazione e di una "weaponization" dello spazio cibernetico[24]. Un ulteriore elemento di preoccupazione viene dalle forme che va assumendo il discorso politico sulla governance delle reti. Sebbene, come abbiamo argomentato, la sovranità digitale europea si caratterizzi per un forte orientamento ai diritti fondamentali e ai valori democratici, l'utilizzo stesso del termine "sovranità" da parte delle istituzioni dell'Unione europea comporta il rischio di un allineamento strategico al discorso sovranista promosso dalla coalizione cino-russa. Si tratta di un pericolo che non può essere ignorato, soprattutto in considerazione dell'ascesa del tema della cybersecurity a questione centrale tra le diverse *issues* dell'Internet governance. Rispetto a questi rischi di una deriva securitaria delle strategie e delle politiche europee, l'unico argine immaginabile è quello della partecipazione attiva ai processi della governance delle reti da parte degli attori della società civile: cittadini, associazioni, partiti, sindacati, comunità accademica e comunità tecnica. Torniamo, per questa via, al

grande progetto politico di Stefano Rodotà, che fortemente volle, tra le disposizioni della Dichiarazione dei diritti in Internet, la costituzione di un organismo nazionale multistakeholder «per garantire effettivamente il rispetto dei criteri indicati, anche attraverso una valutazione di conformità delle nuove norme ai principi di questa Dichiarazione» (art. 14, comma 7).

Note

[1]L. Gill, D. Redeker, U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, Berkman Center Research Publication No. 2015-15, 2015.

[2]*Ivi*, p. 2.

[3]D. Redeker, L. Gill, U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, in "International Communication Gazette", vol. 80, 2018, n. 4, p. 302-319; A. Pettrachin, *Towards a Universal Declaration on Internet Rights and Freedoms?*, in "International Communication Gazette", vol. 80, 2018, n. 4, p. 337-353.

[4]C. Padovani, M. Santaniello, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System*, in "International Communication Gazette", vol. 80, 2018, n. 4, p. 295-301; M. Mann, A. Daly, M. Wilson, N. Suzor, *The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia*, in "International Communication Gazette", vol. 80, 2018, n. 4, p. 369-384.

[5]M. Santaniello, N. Palladino, M.C. Catone, P. Diana, *The Language of Digital Constitutionalism and the Role of National Parliaments*, in "International Communication Gazette", vol. 80, 2018, n. 4, p. 320-336.

[6]M. Santaniello, E. De Blasio, N. Palladino, D. Selva, E. De Nictolis, S. Perna, *Mapping the debate on Internet Constitution in the networked public sphere*, in "Comunicazione politica", 2016, n. 3, p. 327-354; D. Redeker, *Exploring the Bottom-Up Constitutionalism of the 'Feminist Principles of the Internet'*, in "Proceedings of the Annual Symposium GigaNet: Global Internet Governance Academic Network", 2018.

[7]V. il portale Digital Constitutionalism Network.

[8]G. Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization*, Oxford University Press, 2012; G. Teubner, *The project of constitutional sociology: Irritating nation state constitutionalism*, in "Transnational Legal Theory", n. 4, 2013, p. 44-58.

[9]M. Zalnieriute, *An international constitutional moment for data privacy in the times of mass-surveillance*, in "International Journal of Law and Information Technology", vol. 23, n. 2, 2015, p. 99-133.

[10]G. Verschraegen, *Hybrid constitutionalism, fundamental rights and the state*, in "Netherlands Journal of Legal Philosophy", vol. 40, 2011, n. 3, p. 216-229.

[11]V. Commissione per i diritti e i doveri relativi ad Internet, *Dichiarazione dei diritti in Internet*, 2015.

[12]V. il comunicato stampa *La Commissione propone una dichiarazione su diritti e principi digitali per tutti nell'UE*, 2022.

[13]Parlamento europeo, *Risoluzione recante raccomandazioni alla Commissione sulla legge sui servizi digitali: migliorare il funzionamento del mercato unico* (2020/2018(INL)), 20 ottobre 2020.

[14]V. nel sito della Commissione europea: *Berlin Declaration on Digital Society and Value-based Digital Government*, 2020.

[15]V. nel sito della Commissione europea: *Lisbon Declaration – Digital Democracy with a Purpose*, 2021.

[16]J. Goldsmith, T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, 2006; M. Mueller, *Networks and States. The Global Politics of Internet Governance*, MIT Press, 2010.

[17]S. Couture, S. Toupin, *What does the notion of "sovereignty" mean when referring to the digital?*, in "New Media & Society", vol. 21, 2019, n. 10, p. 2305-2322; J. Pohle, T. Thiel, *Digital Sovereignty*, in "Internet Policy Review", vol. 9, 2020, n. 4.

[18]V. nel sito della Commissione europea: *The Digital Services Act: ensuring a safe and accountable online environment*.

[19]V. nel sito della Commissione europea: *Digital Markets Act: Ensuring fair and open digital markets*, 2020.

[20]Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, doc. COM(2021) 206 final del 21 aprile 2021.

[21]Si veda anche E. Celeste, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. Fabbrini, E. Celeste, J. Quinn (eds.), "Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty", Hart, 2021.

[22]Su questi concetti si veda M. Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, Polity Press, 2017.

[23]Cfr. M. Santaniello, *From Governance Denial to State Regulation: A Controversy-Based Typology of Internet Governance*, in B. Haggart, N. Tusikov, J.A. Scholte (eds.), "Power and Authority in Internet Governance. Return of the State?", Routledge, 2021, p. 15-36.

[24]J. Zittrain, *"Netwar": The unwelcome militarization of the Internet has arrived*, in "Bulletin of the Atomic Scientists", vol. 73, 2017, n. 5, p. 300-304.

* * *

Digital sovereignty and fundamental rights: A European model of Internet Governance

Abstract: The article describes and analyzes the recent regulatory turn in the European Union's digital policies, and the attempt of the European institutions to advance a new model of global Internet governance. The analysis suggests that the peculiarity of this model comes from the combination of two different normative frameworks: digital constitutionalism and digital sovereignty. More in detail, new EU legislative proposals testify how the regulative endeavor of the European institutions aims, on the one hand, at defining an ensemble of fundamental digital rights, and on the other, at the establishment of a set of public powers able to limit the exercise of digital power.

Keywords: Internet governance – Digital sovereignty – Digital constitutionalism – Digital rights

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0051

Internet: quando la "rete" cattura i minori

Domenico Alfieri

La sicurezza in rete dei minori è un tema complesso che coinvolge in cascata le istituzioni di ogni livello. Numerose sono le iniziative volte alla definizione di policy e best practice per tentare di arginare i fenomeni connessi al rapporto, ormai morboso, che i minori hanno con il mondo digitale con il quale entrano in confidenza prima ancora della scolarizzazione. L'educazione digitale va affrontata in modo capillare a partire dal legislatore fino all'educatore, quest'ultimo spesso troppo lento per stare dietro alla frenesia della rete a cui sono sottoposte le nuove generazioni. Questo lavoro riassume sinteticamente alcune delle principali minacce presenti in rete e le loro ripercussioni sulla salute dei minori, offrendo una panoramica su alcune tra le iniziative strategiche intraprese in ambito europeo e nazionale, al fine di sottolineare l'importanza della formazione e della prevenzione ad ogni livello educativo.

Minori – Cyberbullismo – Strategia – Protezione – Abuso

Sommario: *1. Introduzione – 2. Impatto della rete sui minori – 3. Problema trattato a livello internazionale – 4. Problema trattato a livello nazionale – 5. Conclusioni*

1. Introduzione

Da un progetto finalizzato ad applicazioni militari e strategiche, nacque la prima rete (ARPANET) che consentiva lo scambio di dati tra nodi estremamente distanti dal punto di vista geografico.

Essendo un progetto di ricerca, non ci volle molto che il sistema diventasse un mezzo di scambio di dati e informazioni tra i ricercatori, creando già negli anni Settanta una rete universitaria di ricerca basata su un insieme di regole, chiamate protocolli di rete, che garantissero l'interoperabilità tra le diverse macchine collegate (protocollo TCP/IP).

La semplicità di diffusione, la sua versatilità, l'offerta di contenuti multimediali applicati allo svago, al lavoro e allo studio, favorirono lo sviluppo esponenziale di questo sistema di comunicazione che, negli anni Novanta ebbe un boom vero e proprio trasformandosi in un fenomeno socio culturale senza precedenti che prese il nome di Internet.

Proprio la sua caratteristica di diffusione capillare fece sì che Internet attirasse l'interesse dei privati che attraverso grandi investimenti favorirono l'ampliamento della rete a livello capillare, migliorando qualità e velocità di trasmissione e portandola a diventare quello che oggi è sotto gli occhi di tutti.

Una delle definizioni che viene data a Internet è "La rete delle reti", ma questa rete, che per sua natura tende ad essere sregolata e anarchica, racchiude nella sua definizione due spaccati della realtà diametralmente opposti. Se da un lato infatti si beneficia di uno strumento in cui tutte le maglie sono connesse tra loro consentendo una forma di comunicazione integrata e universale, dall'altro la "rete" è una ve-

D. Alfieri è funzionario informatico del Ministero dello Sviluppo Economico - D.G. per le Tecnologie delle Comunicazioni e la Sicurezza Informatica, Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (DGTCSI-ISCTI). È anche consigliere nel GAC-ICANN per l'Italia.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

ra e propria trappola per chiunque ne sottovaluti la pericolosità facendone un uso inappropriato.

Le minacce presenti nel mondo virtuale sono molteplici e quotidianamente si manifestano con problemi quali:
- il furto d'identità,
- l'esfiltrazione di dati sensibili,
- la violazione della privacy,
- la compromissione di sistemi informatici a volte anche di operatori di servizi essenziali,
- le truffe online,
- i fenomeni di dipendenza,

tutti legati a un suo utilizzo inappropriato o incauto.

Per far fronte a queste minacce nascono degli studi e delle norme sulla sicurezza delle reti e delle informazioni, si formano organismi atti a garantire il rispetto di determinati standard di sicurezza e di determinate regole a tutela delle imprese e del cittadino.

Tutti gli studi e le norme prevedono ovviamente una componente tecnica basata sullo sviluppo e miglioramento a ciclo continuo delle policy di sicurezza e delle tecniche di cybersecurity, e una componente fondamentale che coinvolge il fattore umano. Tale componente può essere definita come una sorta di educazione digitale, ovvero quel processo di formazione imprescindibile alla prevenzione delle minacce informatiche sia a livello d'impresa che a livello domestico/scolastico.

2. Impatto della rete sui minori

I risvolti negativi che caratterizzano la rete si ripercuotono nell'ambiente domestico e scolastico, in particolare nell'utilizzo di Internet da parte dei minori, per cui diventa necessario focalizzare l'attenzione allo sviluppo di un processo educativo orientato alle nuove generazioni.

In termini di apprendimento la rapidità dei "nativi digitali" si contrappone alla lentezza degli adulti che spesso si ritrovano a dover accettare passivamente, e a volte superficialmente, un'evoluzione che non riescono a seguire, spesso a discapito dell'azione protettiva che dovrebbero esercitare.

Con il 69% dei giovani online nel 2019 e un bambino su tre con accesso alla rete da casa, Internet è diventato parte integrante della vita dei minori, offrendo ai bambini e ai giovani molte possibilità di comunicare, imparare, socializzare e giocare, esponendo i bambini a nuove idee e fonti di informazione più diversificate e offrendo loro opportunità di partecipazione politica e civica in modo che crescano, siano creativi e contribuiscano significativamente a una società migliore.

Con i bambini lontani dal loro edificio scolastico e che imparano a distanza, nel 2020 e nel 2021 la pandemia di COVID-19 ha delineato l'importanza di una connettività affidabile come mezzo imprescindibile per l'accesso all'istruzione di base, alle interazioni sociali, e ai servizi di assistenza e supporto.

L'accesso alla connettività è sempre più un fattore determinante delle pari opportunità per i bambini, in particolare per coloro che sono lasciati indietro nei sistemi attuali a causa di povertà, disabilità, etnia, genere, sfollamento o isolamento geografico. L'Information Technology può aiutarli ad esprimere il loro potenziale educativo, facilitare la loro inclusione sociale e amplificare la loro voce nella partecipazione civica, in conformità ai loro diritti sanciti della Convenzione delle Nazioni Unite sui diritti dell'infanzia (UN CRC).

Pur sostenendo e promuovendo i diritti dei bambini, lo stesso ambiente online può esporre i bambini a rischi, alcuni dei quali possono tradursi in potenziali danni.

Infatti l'impalpabilità della rete ha fatto sì che tutto ciò che prima accadeva sotto gli occhi di tutti, per cui facilmente riscontrabile, adesso si sviluppi in modo silente e possa sfuggire al controllo di chi dovrebbe tutelare gli individui più fragili.

Solo nell'aprile 2020, il *National Center for Missing and Exploited Children* - NCMEC ha registrato quattro milioni di segnalazioni di sospetto materiale pedopornografico online, rispetto a un milione registrato nel 2019 nello stesso periodo.

La pandemia di COVID-19 ha dunque aggravato le minacce precedentemente esistenti per i bambini online ed ha sottolineato l'urgente necessità di agire per la prevenzione di rischi quali:
- rischi sui contenuti: esposizione a informazioni imprecise o incomplete, contenuti inappropriati o addirittura criminali come esposizione a contenuti per adulti/estremisti/violenti/crudi, autolesionismo, comportamenti distruttivi e violenti, di radicalizzazione o adesione a contenuti razzisti o discriminatori idee;
- rischi di contatto da parte di adulti o coetanei: molestie, esclusione, discriminazione, diffamazione e danno alla reputazione, abusi e sfruttamento sessuale incluse estorsioni, adescamento (sessuale), materiale pedopornografico, traffico e sfruttamento sessuale dei bambini anche nei viaggi e nel turismo;
- rischi di tipo contrattuale: esposizione a rapporti contrattuali inappropriati, consenso dei minori online, marketing integrato, gioco d'azzardo online nonché violazione e uso improprio di dati per-

sonali come pirateria informatica, frode e furto di identità, truffe, profiling bias;
- rischi comportamentali: come la condivisione di contenuti sessuali autogenerati o rischi caratterizzati da attività dei coetanei: ostilità e violenza come il cyberbullismo, lo stalking, l'esclusione e le molestie.

Dei rischi appena descritti ce ne sono alcuni che si verificano all'ordine del giorno, tra cui:

il cyberbullismo si può definire come la manifestazione in rete di azioni violente e intimidatorie esercitate da un bullo, o un gruppo di bulli, tramite strumenti elettronici nei confronti di un coetaneo incapace di difendersi. Tali azioni che prima riguardavano molestie verbali, aggressioni fisiche e persecuzioni generalmente attuate in ambiente scolastico, adesso si manifestano nelle case delle vittime e in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet.

La pedopornografia (pornografia minorile) è configurabile come ogni rappresentazione, con ogni mezzo, di un minorenne in attività sessuali esplicite, reali o simulate, o qualsivoglia rappresentazione degli organi sessuali per scopi sessuali. Direttamente collegata alla pedopornografia c'è l'adescamento dei minori in rete (*grooming*).

Il *grooming* è una particolare forma di cyberbullismo che sfocia nell'adescamento sessuale. Il predatore si guadagna la fiducia del minore dimostrandosi amico e sviluppando una relazione intima e duratura che può sfociare poi in un incontro sessuale o in uno scambio di materiale pedopornografico.

Tutti fenomeni legati ad un abuso della rete che sfocia nella dipendenza, un fenomeno silente che si verifica con l'abuso degli strumenti informatici da cui scaturisce una mania o una fissazione che a sua volta porta a confondere il piano della vita virtuale con quello della vita reale.

3. Problema trattato a livello internazionale

I problemi da affrontare in ambito di educazione digitale sono molteplici e non potevano non suscitare un interesse a livello globale. Tale interesse ha portato allo sviluppo di leggi, policy, linee guida che hanno stimolato l'interesse della comunità a livello internazionale.

Il tema della protezione online dei minori (*Child Online Protection*) richiede tutt'oggi una risposta globale basata sulla cooperazione internazionale e sul coordinamento nazionale.

Le sfide e le minacce persistono a causa della natura senza confini dell'ambiente online che rende difficili iniziative significative come la formazione di quadri legislativi, piani, strategie, risorse, compresi finanziamenti e istituzioni internazionali e nazionali dedicate a garantire la protezione online dei minori.

Per intraprendere un processo di prevenzione e protezione è necessario adottare a tutti i livelli una strategia inclusiva e multilivello di protezione online dei minori con misure e attività efficaci e mirate, che includono risorse finanziarie e umane. Solo con un approccio multi-stakeholder coordinato e cooperativo i bambini e le generazioni future saranno protetti e autorizzati a prosperare negli ambienti digitali.

In ambito europeo nasce la *European strategy for a better Internet for our children*, che introduce la necessità di contenuti online di qualità nonché l'incremento delle competenze e degli strumenti per utilizzare Internet in modo sicuro e responsabile. Considerata l'età in cui i minori si avvicinano al mondo virtuale, alcuni addirittura prima di saper leggere e scrivere, diventa una necessità lavorare sui contenuti e sulla formazione, stimolando al contempo il potenziale del mercato sui contenuti online interattivi, creativi ed educativi.

La Commissione europea, che segue gli sviluppi della strategia, propone una serie di azioni raggruppate verso i seguenti obiettivi:
- stimolare la produzione di contenuti online creativi ed educativi per i bambini e promuovere esperienze online positive per i più piccoli;
- aumentare la consapevolezza, compresa l'alfabetizzazione digitale e la sicurezza online in tutte le scuole dell'UE;
- creare un ambiente sicuro per i bambini attraverso impostazioni di privacy adeguate all'età, un uso più ampio dei controlli parentali e classificazione in base all'età e ai contenuti;
- lottare contro il materiale pedopornografico online e lo sfruttamento sessuale dei minori.

La strategia coinvolge, oltre la Commissione europea, i paesi dell'UE, gli operatori di telefonia mobile, i produttori di telefoni e i fornitori di servizi di social networking per fornire soluzioni concrete per un Internet migliore per minori.

I compiti svolti dalla Commissione europea in merito alla strategia si sviluppano principalmente attraverso l'attuazione del meccanismo per collegare l'Europa e gli strumenti per il finanziamento dell'infrastruttura dei servizi digitali.

La strategia europea ha influenzato le politiche nazionali nella maggior parte dei paesi dell'UE. Ogni anno, varie azioni e campagne nell'ambito della Stra-

tegia raggiungono migliaia di scuole e giovani, ma anche genitori e insegnanti[1].

Uno degli organismi di rilievo internazionale che si è occupato del tema "tutela dei minori in rete" è l'ITU - *International Telecommunication Union*.

L'ITU ha infatti dedicato alla protezione dei minori in rete una sezione sul proprio sito Internet, all'interno della quale sono presenti linee guida e video lezioni dedicate alla sicurezza in rete dei bambini.

Nella pubblicazione *Keeping children safe in the digital environment: The importance of protection and empowerment*, viene affrontato il problema come *global challenge* (sfida globale) evidenziando come i rapidi progressi della tecnologia, della società e della natura senza confini di Internet richiedano una protezione online dei minori agile e adattiva, pena la sua inefficacia.

La protezione online dei minori necessita di una strategia olistica che favorisca la formazione di ambienti digitali sicuri, rispettosi del genere, adeguati all'età, inclusivi e che sia caratterizzata da:

- un approccio basato sui diritti dell'infanzia, sostenendo i principi sanciti dalla CRC - *Convention on the Rights of the Child* delle Nazioni Unite[2] e dal *General comment No. 25 (2021) on children's rights in relation to the digital environment*[3];
- un equilibrio dinamico tra garanzia di protezione e pari (e sicure) opportunità ai bambini di essere cittadini digitali;
- la prevenzione di eventuali danni;
- una risposta incentrata sul bambino, che sostenga una formazione incentrata sulla responsabilizzazione di fronte alle minacce, con specifico riferimento all'emergenza COVID-19 e agli scenari ad essa connessi.

Questo approccio prevede anche la partecipazione dei minori alla progettazione, implementazione e valutazione delle soluzioni per mantenerli al sicuro nell'ambiente virtuale.

Al fine di rispondere efficacemente ai rischi e ai danni online per i minori diventa necessario adottare una strategia nazionale di protezione inclusiva e multi-stakeholder che integri lo sviluppo di nuove policy con quelle già esistenti fornendo il quadro strategico necessario per affrontare la sfida globale della protezione dei minori in rete.

Tale strategia dovrebbe rafforzare un coordinamento efficace considerando l'importanza, la visione e il ruolo delle seguenti parti interessate:

- governo a livello locale, nazionale e regionale (ad es. affari interni, salute, istruzione, giustizia, assistenza sociale/protezione dell'infanzia, digitale/informazioni, legislatori);
- forze dell'ordine;
- organizzazioni di servizi sociali e sanitari (ad es. consulenza, servizi di supporto, ufficio per il benessere dei giovani, case sicure, riabilitazione, servizi sanitari);
- industria ICT, ad es. piattaforme online, fornitori di contenuti, fornitori di servizi Internet (ISP) e altri fornitori di servizi elettronici (ESP), fornitori di reti di telefonia mobile, fornitori Wi-Fi pubblici;
- organizzazioni internazionali, ONG, OSC e organizzazioni comunitarie (ad esempio, protezione dei minori e altre organizzazioni internazionali e ONG pertinenti, sindacati e organizzazioni di insegnanti/genitori);
- bambini e giovani, nonché i loro genitori/tutori;
- comunità accademica e di ricerca (es. *think tank*, centri di ricerca, biblioteche, scuole e università).

Una strategia nazionale di protezione dei minori online fornisce la tabella di marcia per riunire e coordinare le attività esistenti e le nuove attività rilevanti. Qualsiasi strategia dovrebbe essere di proprietà di un'autorità adeguata ed essere sostenibile con le risorse umane e finanziarie necessarie. Tale quadro dovrebbe avere un mandato chiaro e un'autorità sufficiente attraverso un meccanismo (o consiglio) multi- stakeholder per coordinare tutte le attività relative ai diritti dei bambini, ai media digitali e all'ICT a livello intersettoriale, nazionale, regionale e locale, apprezzando gli sforzi esistenti nella definizione, coordinamento, attuazione e monitoraggio della strategia nazionale di protezione dei minori online.

Il documento dell'ITU propone delle azioni politiche mirate ad affrontare tutti i rischi e i potenziali danni per i bambini online e pensate per essere integrate da quadri più specifici come il modello *WePROTECT National Response (MNR)*[4] sullo sfruttamento e l'abuso sessuale dei bambini, che si concentra su danni specifici.

Le policy proposte sono suddivise per macroaree e vengono di seguito riassunte.

I diritti dei bambini

- Standardizzare la definizione di bambino come chiunque abbia meno di 18 anni in tutti i documenti legali in linea con l'articolo 1 della Convenzione delle Nazioni Unite sui diritti dell'infanzia (UN CRC).
- Costruire e collaborare con istituzioni indipendenti per i diritti umani per i bambini per garantire la protezione dei bambini online attraverso competenze specializzate, indagini e monitoraggio, promozione, sensibilizzazione, formazione e istruzione e con la partecipazione dei bambini.
- Includere la consultazione diretta con i minori, come è loro diritto ai sensi dell'articolo 12 della CRC delle Nazioni Unite, nello sviluppo, attuazione e

monitoraggio di qualsiasi tipo di quadro o piano d'azione per la protezione dei minori online.

Legislazione

- Riesaminare il quadro giuridico esistente per determinare l'esistenza di tutti i poteri giuridici necessari per consentire e assistere le forze dell'ordine e altri attori pertinenti per proteggere le persone di età inferiore ai 18 anni da tutti i tipi di danni online su tutte le piattaforme online.
- Stabilire che qualsiasi atto illegale contro un bambino nel mondo reale sia, "mutatis mutandis", illegale online e che le norme sulla protezione dei dati online e sulla privacy per i bambini siano adeguate.
- Allineare i quadri giuridici con gli standard internazionali esistenti, le leggi e le convenzioni relative ai diritti dei bambini e alla sicurezza informatica, facilitando la cooperazione internazionale attraverso l'armonizzazione delle leggi.
- Incoraggiare l'uso di una terminologia appropriata nello sviluppo della legislazione e delle politiche riguardanti la prevenzione e la protezione dello sfruttamento sessuale e dell'abuso sessuale dei bambini.

Forze dell'ordine

- Garantire che i casi di minori che danneggiano gli altri online siano trattati in linea con i principi dei diritti dei minori, opportunamente iscritti nella legislazione nazionale, favorendo fortemente strumenti diversi dal diritto penale.
- Fornire adeguate risorse finanziarie e umane, nonché formazione e rafforzamento delle capacità per coinvolgere pienamente ed equipaggiare la comunità delle forze dell'ordine.
- Garantire la cooperazione internazionale tra le forze dell'ordine in tutto il mondo, consentendo una risposta più rapida ai reati facilitati online.

Regolamentazione

- Considerare lo sviluppo di una politica di regolamentazione (sviluppo di politiche di coregolamentazione, quadro normativo completo).
- Imporre alle imprese l'obbligo di intraprendere una due diligence sui diritti dell'infanzia e di salvaguardare i propri utenti.
- Istituire meccanismi di monitoraggio per l'indagine e il risarcimento delle violazioni dei diritti dei bambini, al fine di migliorare la responsabilità delle TIC e di altre società pertinenti.
- Rafforzare la responsabilità dell'agenzia di regolamentazione per lo sviluppo di standard rilevanti per i diritti dei bambini e le TIC.

Monitoraggio e valutazione

- Istituire una piattaforma multi-stakeholder per guidare lo sviluppo, l'attuazione e il monitoraggio dell'agenda digitale nazionale per i bambini.
- Sviluppare obiettivi vincolati nel tempo e un processo trasparente per valutare e monitorare i progressi e garantire che le risorse umane, tecniche e finanziarie necessarie siano messe a disposizione per l'efficace funzionamento della strategia nazionale di protezione dei minori online e dei relativi elementi.

Industria delle ICT

- Coinvolgere l'industria nel processo di elaborazione delle leggi sulla protezione dei minori online e di metriche comuni per misurare tutti gli aspetti rilevanti della sicurezza online dei minori.
- Stabilire incentivi e rimuovere le barriere legali per facilitare lo sviluppo di standard e tecnologie comuni per combattere i rischi relativi ai contenuti per i bambini.
- Incoraggiare l'industria ad adottare un approccio di sicurezza e privacy fin dalla progettazione ai propri prodotti, servizi e piattaforme, riconoscendo il rispetto dei diritti dei bambini come obiettivo fondamentale.
- Garantire che l'industria utilizzi meccanismi rigorosi per rilevare, bloccare, rimuovere e segnalare in modo proattivo contenuti illegali e qualsiasi abuso (classificato come attività criminale) contro i bambini.
- Garantire che l'industria fornisca meccanismi di segnalazione adeguati e adatti ai bambini affinché i propri utenti possano segnalare problemi e preoccupazioni e possano ottenere ulteriore supporto.
- Collaborare con le parti interessate del settore per promuovere la consapevolezza al fine di supportare l'identificazione del settore rischi nello sviluppo e correggere prodotti e servizi esistenti. Ciò include la considerazione di altre preoccupazioni delle parti interessate e dei rischi e dei danni a cui sono esposti gli utenti finali.
- Supportare le parti interessate del settore affinché forniscano strumenti adatti all'età per aiutare i loro utenti a gestire meglio la protezione delle loro famiglie online.

Segnalazione

- Istituire e promuovere ampiamente meccanismi per segnalare facilmente i contenuti illegali trovati su Internet.
- Istituire un numero verde nazionale per l'infanzia con la capacità necessaria sui rischi e danni facilitati online o un numero verde per l'infanzia/un numero di assistenza per l'infanzia per facilitare la segnalazione da parte delle vittime di problemi di sicurezza online dei bambini.
- Istituire meccanismi di consulenza, segnalazione e reclamo sicuri e facilmente accessibili a misura di bambino.

Servizi sociali e assistenza alle vittime
- Garantire che siano in atto meccanismi di protezione dell'infanzia universali e sistematici che obblighino tutti coloro che lavorano con i bambini (ad es. assistenti sociali, operatori sanitari, educatori) a identificare, rispondere e segnalare qualsiasi tipo di danno ai bambini che si verifica online.
- Garantire che i professionisti dei servizi sociali siano formati sia per l'azione preventiva che per la risposta ai danni online ai minori, identificando gli abusi sui minori e fornendo un adeguato supporto specializzato e a lungo termine e assistenza ai minori, vittime di abusi.
- Sviluppare strategie e misure di prevenzione degli abusi sui minori basate su prove scientifiche.
- Fornire risorse umane e finanziarie adeguate a garantire il pieno recupero e reinserimento dei bambini e prevenire fenomeni di ricaduta (ri-vittimizzazione).
- Garantire che i bambini abbiano accesso a un'assistenza sanitaria adeguata (compresa la salute mentale e il benessere fisico) anche in caso di vittimizzazione, trauma o abuso online.

Raccolta e ricerca dati
- Effettuare ricerche sullo spettro degli attori nazionali e delle parti interessate per determinare le loro opinioni, esperienze, preoccupazioni e opportunità in merito alla protezione online dei minori.

Formazione scolastica
- Garantire che gli educatori e gli amministratori/professionisti scolastici siano formati per identificare e rispondere adeguatamente nei casi sospetti o confermati di minori vittime di abusi.
- Sviluppare un ampio programma di alfabetizzazione digitale adeguato all'età e incentrato su abilità e competenze per garantire che i bambini possano trarre pieno vantaggio dall'ambiente online, siano attrezzati per identificare le minacce e possano comprendere appieno le implicazioni del loro comportamento online.
- Sviluppare funzionalità di alfabetizzazione digitale come parte del curriculum scolastico nazionale che sia adeguato all'età e applicabile ai bambini fin dalla tenera età.
- Creare risorse educative al di fuori del curriculum scolastico che enfatizzino gli aspetti positivi e responsabilizzanti di Internet per i bambini e promuovano forme responsabili di comportamento online.
- Evitare i messaggi basati sulla paura.
- Consultare i bambini, nonché i genitori e gli accompagnatori sullo sviluppo di programmi, strumenti e risorse educative.

Consapevolezza e capacità nazionale
- Sviluppare campagne nazionali di sensibilizzazione del pubblico, che coprano un'ampia varietà di questioni che possono essere collegate all'ambiente digitale e adattate a tutti i gruppi target.
- Arruolare istituzioni pubbliche e mass media per la promozione di campagne nazionali di sensibilizzazione del pubblico.
- Sfruttare le campagne globali, nonché i quadri e le iniziative multistakeholder per creare campagne nazionali e rafforzare le capacità nazionali in materia di protezione online dei minori[5].

L'aspetto della privacy che coinvolge la tutela dei minori è stato trattato in ambito GDPR (Regolamento Privacy UE/2016/679) in diverse sezioni.

Il considerando 38 recita infatti: «I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore».

Esaminando più nello specifico, si sottolinea che l'articolo 8 dello stesso regolamento, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), contiene nuove e specifiche previsioni relative alle «Condizioni applicabili al consenso dei minorenni in relazione ai servizi della società dell'informazione», cui il nostro ordinamento dovrà adeguarsi con leggi nazionali. L'art. 8.1, in particolare, introduce la regola generale per cui il cd. "consenso digitale", applicato alla fornitura di servizi online per ragazzi under 18, sarà lecito solo laddove il minorenne "abbia almeno 16 anni".

Nel caso in cui, invece, l'interessato abbia un'età inferiore, il trattamento viene considerato lecito «soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale». Tuttavia, lo stesso art. 8.1 prevede una deroga al limite minimo di età per poter considerare valido il consenso rilasciato dal minorenne, precisando che «Gli Stati membri possono stabilire per legge un'età

inferiore a tali fini purché non inferiore ai 13 anni». Al riguardo si delineano diversi orientamenti: se da una parte l'accesso ad Internet offre ai bambini e ai giovani straordinarie opportunità di informazione, comunicazione e conoscenza portabile, immediata e globale, dall'altra li espone, attraverso l'accesso pressoché illimitato a contenuti, persone, luoghi virtuali, a rischi multiformi e complessi dai confini spesso labili e mutevoli.

L'entrata in vigore del GDPR, studiato per arginare i problemi legati alla privacy dell'individuo, ha avuto però un effetto collaterale che si è ripercosso sulla componente di cybersecurity della rete.

Se da un lato ha dettato norme per la protezione della privacy, dall'altro ha indotto gli operatori di registro ad oscurare i dati che confluivano nel WHOIS, dati che venivano utilizzati dalle forze dell'ordine e dagli operatori di cybersecurity come agevolazione nelle indagini sui crimini informatici.

Il tema della protezione dei minori online investe anche il sistema di assegnazione dei nomi a dominio gTLD - *generic Top Level Domain*. Nel momento in cui si discute di policy che riguardano i nomi a dominio, siano essi generici oppure specifici, non si può fare a meno di coinvolgere l'ente di gestione internazionale ICANN - *Internet Corporation for Assigned Names and Numbers*, il cui compito, tra gli altri, è quello di approvare e adottare le policy sull'assegnazione dei nomi a dominio e farle rispettare alle parti contraenti (*registries* e *registrars*) con ovvie ripercussioni sugli utenti finali.

In vista del *new round of gTLDs*, ovvero l'apertura di ICANN alla creazione di nuovi nomi a dominio di tipo generico, sono emerse tante preoccupazioni, una della quali riguarda proprio la tutela dei minori.

L'eNACSO - *European NGOs Alliance for Child Safety Online* ha seguito da vicino lo sviluppo delle policy sugli identificatori univoci di Internet e sul sistema di denominazione dei siti Internet coordinato da ICANN, dialogando con quest'ultimo e proponendo delle policy che regolano i domini generici di primo livello. eNACSO ha sollecitato ICANN al raggiungimento di un consenso sui ruoli e le responsabilità di tutti gli attori coinvolti nella governance di Internet e in particolare allo sviluppo un consenso sui ruoli e le responsabilità di quegli organismi dedicati a mantenere Internet sicuro, stabile e interoperabile.

In particolare, considerando l'impatto che il nuovo round di assegnazione di domini generici di primo livello (gTLD) ha sull'espansione e l'evoluzione di Internet, è stata messa in evidenza l'importanza di anteporre gli interessi dei bambini e dei giovani su quelli economici, specie quando si tratta di domini rivolti a loro o che attirino la loro attenzione (es: *.kid*, *.kids*, *.games*, *.juegos*, *.play*, *.school*, *.toys*...).

È stato richiesto ad ICANN di definire accordi sul funzionamento di tali gTLD, per garantire che i processi e le procedure siano ampiamente condivisi e concordati, tenendo presente che la sicurezza dei bambini dovrebbe avere la priorità.

eNACSO ha proposto lo sviluppo di linee guida e requisiti specifici che siano applicati a tutti i domini che si riferiscono espressamente a bambini e giovani, inclusa la richiesta di competenze specifiche da individui o organizzazioni con un background appropriato.

Il monitoraggio delle procedure di assegnazione dei gTLD con probabile impatto sui minori viene ad oggi seguito anche dal PSWG - *Public Safety Working Group* del GAC - *Governmental Advisory Committee*, che si occupa delle policy e delle procedure di sicurezza del web e che coinvolge, oltre che esponenti delle forze dell'ordine, i rappresentanti governativi di tutto il mondo[6].

4. Problema trattato a livello nazionale

Dalla questione internazionale si passa successivamente alla trattazione del problema a livello nazionale. Le istituzioni italiane che si occupano ad oggi della tutela dei minori in rete lavorano in sinergia per attuare le policy in linea con l'ambiente internazionale.

La prima tra tutte l'Autorità Garante per l'Infanzia e l'Adolescenza (AGIA) che tratta l'argomento in modo approfondito nel documento *La tutela dei minorenni nel mondo della comunicazione* con un'apposita sezione minorenni e web.

L'AGIA sottolinea l'importanza dell'educazione digitale, focalizzando l'attenzione sulla «capacità di essere soli e non in continua comunicazione» come contrasto alla soluzione alla *dipendenza* menzionata in precedenza.

Insiste sulla cultura della sicurezza, evidenziando la sussistenza in rete di siti Internet i cui contenuti si scontrano con i principi basilari di tutela dei minori, quali siti che esaltano le pratiche di anoressia e bulimia (c.d. "pro-ana" e "pro-mia") e siti che istigano al suicidio e all'autolesionismo ("cutting").

Persiste, secondo l'AGIA, l'esigenza di bilanciare diversi diritti fondamentali menzionati nel trattato internazionale che regola i diritti civili, politici, economici, sociali, culturali dei bambini (*Convention on the Rights of the Child* - CRC). Tra questi diritti vi sono: la tutela dei minorenni nell'ambito dell'uso sicuro delle tecnologie dell'informazione (articolo 17),

il diritto all'informazione e la libertà di espressione (articolo 13); l'obbligo degli Stati di garantire ai genitori di poter svolgere congiuntamente il loro diritto/dovere di proteggere e educare i figli (articolo 18); il diritto di essere protetti da abusi sessuali (articolo 34).

Emerge la necessità di continuo aggiornamento legislativo e l'affinamento delle tecniche investigative e repressive, promuovendo quindi un'azione preventiva che coinvolga la famiglia, le istituzioni, le varie agenzie educative e le organizzazioni che si occupano dell'infanzia e dell'adolescenza che hanno la responsabilità di far sperimentare alle nuove generazioni una dimensione di cittadinanza in cui esercitare "consapevolmente" libertà, responsabilità e democrazia.

È chiaro come i numerosi input provenienti anche dalla UE in materia di crescita "digitale" includono temi importanti e significativi in ordine alla protezione dei minorenni dai rischi connessi alle nuove tecnologie. Fra di essi necessita di menzione il concetto di "consenso digitale", il quale si impone quale tema prodromico ad una tutela che trovi la giusta mediazione tra il diritto di accesso alla rete e il rispetto di altro importante diritto che è quello di una protezione potenziata, in ragione della peculiare fragilità dell'infanzia e dell'adolescenza[7].

Come già anticipato, la sinergia tra le istituzioni è fondamentale per affrontare un argomento così complesso e delicato. Riguardando il mondo delle comunicazioni, il coinvolgimento dell'Autorità Garante delle Comunicazioni (AGCOM) è stato fondamentale nella stesura di diversi provvedimenti e delibere in materia di tutela dei minori online.

Con la delibera n. 481/14/CONS del 23 settembre 2014, l'AGCOM ha istituito l'Osservatorio permanente delle forme di garanzia e di tutela dei minori e dei diritti fondamentali della persona sulla rete Internet al fine di analizzare le problematiche connesse all'utilizzo di Internet e dei social network e di verificare l'efficacia delle procedure adottate dagli operatori.

L'osservatorio si muove seguendo due linee direttrici:

1. la raccolta, l'elaborazione e la pubblicazione dei dati relativi al comportamento degli utenti rispetto a Internet e ai social network;
2. l'analisi delle policies adottate dagli operatori per la salvaguardia dei valori e degli utenti più sensibili e la valutazione della relativa efficacia e ha come oggetto di monitoraggio fenomeni quali: l'istigazione all'odio, le minacce, le molestie, il bullismo, l'hate speech e la diffusione di contenuti deplorevoli.

L'iniziativa dell'AGCOM incentra le sue basi su un quadro giuridico che fa riferimento alle competenze in ambito di tutela dei minori:

- la legge istitutiva (art. 1, comma 6, lett. b), n. 6 della legge n. 249/97): competenza specifica in materia di tutela dei minori (con attribuzione di ruolo specifico anche all'autoregolamentazione e alla co-regolamentazione);
- il Testo unico dei servizi di media audiovisivi e radiofonici: principi fondamentali del sistema radiotelevisivo e rispetto per la dignità umana (art. 32, comma 5);
- il decreto legislativo 9 aprile 2003, n. 70: l'Autorità amministrativa competente può limitare la libera circolazione di un determinato servizio della società dell'informazione proveniente da un altro Stato membro «per l'opera di prevenzione, investigazione, individuazione e perseguimento di reati, in particolare la tutela dei minori e la lotta contro l'incitamento all'odio razziale, sessuale, religioso o etnico, nonché contro la violazione della dignità umana» (Art. 5, comma 1, lett. a).

Anche le autorità di *law enforcement* si sono adoperate nello sviluppo di linee guida e best practice per il contrasto dei fenomeni criminali che si sviluppano nel mondo virtuale coinvolgendo i minori.

Una fra tutte, la pubblicazione di un contributo concreto sulla navigazione sicura e consapevole dei minori su Internet, sviluppato in collaborazione di altre istituzioni ministeriali, che coinvolge i genitori e fornisce loro alcuni strumenti pratici per la formazione, la prevenzione e il monitoraggio.

Un ruolo importante è sicuramente quello del monitoraggio, esaminato dal punto di vista prettamente pratico e di facile comprensione, nel quale vengono esaminati i tipici comportamenti che evidenziano anomalie e devono far scattare il campanello d'allarme al tutore[8].

Il Ministero dello Sviluppo Economico ha espresso la sua posizione sottolineando l'importanza, in un panorama mediatico sempre più ibrido e integrato, del rispetto dell'equilibrio tra la dimensione produttiva-economica e quella etica e delle implicazioni dei messaggi mediali sui minori. Per questo, alla luce dei cambiamenti che portano verso contesti sempre più digitali, occorre l'impegno di tutte le istituzioni coinvolte per allineare la normativa italiana in materia di minori alle sfide poste dai nuovi linguaggi multimediali[9].

5. Conclusioni

Le strategie Europee e Nazionali sono in continua evoluzione per far fronte a minacce sempre più evo-

lute e mutevoli. Una collaborazione istituzionale che si spinga fino al livello locale, coinvolgendo le scuole e le forze dell'ordine può essere una buona pratica per arginare il problema creando un clima di fiducia da parte del minore nei confronti dei formatori.

Questo intervento a livello scolastico però non basta. Molto spesso viene sottovalutato l'ambiente extrascolastico, dove i minori trascorrono la maggior parte del loro tempo. Per questo motivo assumono una particolare rilevanza le iniziative volte al coinvolgimento dei genitori e dei tutori in un processo di apprendimento studiato *ad hoc* per loro. Tale processo dovrebbe includere una formazione di base all'utilizzo dei dispositivi digitali e delle principali tecniche di prevenzione e controllo del traffico dati sul web, oltre che spingere i genitori e i tutori ad acquisire un maggiore spirito di osservazione riguardo i comportamenti dei minori e dell'ambiente virtuale che essi sono abituati a frequentare.

L'*awareness* diventa la parola chiave per affrontare le sfide di un mondo virtuale la cui rapidità di evoluzione viene spesso sottovalutata anche dagli addetti ai lavori.

Note

[1]Cfr. European Commission, *European Strategy for a better Internet for our children*, 2021.

[2]United Nations - Human Rights - Office of the High Commissioner, *Convention of the Rights of the Child*, 1990.

[3]United Nations - Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 2021.

[4]WeProtect Global Alliance, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*, 2016.

[5]Si veda ITU Policy Brief, *Keeping children safe in the digital environment: The importance of protection and empowerment*, 2021.

[6]eNACSO - European NGOs Alliance for Child Safety Online, *The rules governing General Top-Level Domains*.

[7]Autorità Garante per l'Infanzia e l'Adolescenza, *La tutela dei minorenni nel mondo della comunicazione*, 2017.

[8]Si veda Commissariato di P.S. on line, *Per i genitori. Navigazione sicura e consapevole dei minori su internet*.

[9]Cfr. Ministero dello sviluppo economico, *Avviato percorso condiviso per la tutela dei minori sulle multipiattaforme digitali*, 2020.

* * *

Internet: When the net catches children

Abstract: The child online protection is a complex issue that involves institutions of all levels in cascade. There are many initiatives of policies and best practices definition to try to stem the phenomena connected to the relationship, actually unhealthy, that children have with the digital world, with which they become familiar even before schooling. Digital education must be addressed in a capillary way starting from the legislator to the educator, the latter often too slow to keep up with the frenzy of the network to which the new generations are subjected. This paper briefly summarizes some of the main threats present on the net and their repercussions on the health of minors, offering an overview of some of the strategic initiatives undertaken at European and national level, in order to underline the importance of training and prevention at any educational level.

Keywords: Children – Cyberbullying – Strategy – Protection – Abuse

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0059

Il ruolo della governance multi-stakeholder di Internet nella diffusione della connettività in Brasile

Demi Getschko • Carlos Afonso • Alexandre F. Barbosa

Le tecnologie dell'informazione e della comunicazione stanno causando profonde trasformazioni nella nostra società. Tra i principali agenti di queste trasformazioni ci sono, da un lato, il processo di trasformazione digitale che coinvolge governi, organizzazioni e individui e, dall'altro, il consolidamento dell'uso e l'adozione di Internet come infrastruttura critica per i processi sociali, economici, politici e culturali. In questo contesto, la governance di Internet sta ottenendo sempre più spazio nel dibattito pubblico vista la sua rilevanza per l'inclusione digitale e lo sviluppo. Questo articolo discute il ruolo della governance multi-stakeholder di Internet nella diffusione della connettività in Brasile partendo da una prospettiva storica degli eventi legati allo sviluppo di Internet nel Paese. Il modello di governance implementato dal Comitato di Gestione di Internet in Brasile (CGI.br) e dal suo braccio operativo rappresentato dal Nucleo di Informazione e Coordinamento del Punto BR (NIC.br) è un modello che ha contribuito efficacemente alla progettazione di politiche pubbliche volte all'inclusione digitale di persone e organizzazioni nella direzione di una connettività universale e significativa. In tal senso, i meccanismi di governance di Internet stabiliti in un Paese possono favorire processi decisionali – condivisi tra rappresentanti del governo, delle imprese, di organizzazioni della società civile e della comunità accademica – che garantiscano l'espansione della connettività.

Governance di Internet – Comitato di Gestione di Internet in Brasile – Trasformazione digitale – Società dell'informazione – Connettività e inclusione digitale

Sommario: *1. Introduzione – 2. Breve storia dell'accesso a Internet in Brasile – 3. Il modello di governance adottato in Brasile – 4. Il modello duale: CGI.br/NIC.br – 5. Società dell'informazione: governance di Internet e diritti alla connettività – 6. Conclusioni*

1. Introduzione

La società sta attraversando profonde trasformazioni a una velocità sempre più alta. Due dei principali fattori determinanti di tali trasformazioni sono, da una parte, il processo di trasformazione digitale a cui sono soggetti governo, organizzazioni e individui, e dall'altra il consolidamento dell'uso e dell'adozione di Internet quale infrastruttura critica per i processi sociali, economici, politici e culturali.

D. Getschko è stato membro del consiglio direttivo dell'*Internet Corporation for Assigned Names and Numbers* (ICANN) mediante la *Country Code Names Support Organization* (ccNSO), ed eletto all'*Internet Hall of Fame*. È consigliere del *Comitê Gestor da Internet no Brasil* (CGI.br), direttore-presidente del *Núcleo de Informação e Coordenação do Ponto BR* (NIC.br) e professore associato presso la Pontificia Università Cattolica di San Paolo (PUC-SP). C. Afonso è stato consigliere speciale dell'*Internet Governance Forum* (IGF), membro del *Multistakeholder Advisory Group* dell'IGF ed eletto all'*Internet Hall of Fame*. È cofondatore del CGI.br nonché direttore esecutivo dell'*Instituto Núcleo de Pesquisa Estudos e Formação* (Nupef). A.F. Barbosa dirige il *Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação* (Cetic.br), dipartimento del NIC.br.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

La graduale e crescente adozione della rete ha fatto sì che si consolidasse il concetto di società dell'informazione, segnando così il passaggio da un'economia basata sulla produzione industriale a un'economia basata sul flusso di informazioni e dati in reti[1]. La democratizzazione dell'informazione, conseguente all'adozione universale di Internet, ha reso possibile la creazione e la condivisione di conoscenze in grado di promuovere lo sviluppo sociale ed economico delle società[2]. In questo senso, si può osservare che le interazioni sociali avvengono sempre più spesso mediante le tecnologie digitali; inoltre, la connettività a Internet è ormai una componente centrale del processo di trasformazione digitale della società.

La connettività a Internet è al contempo il motore e gli ingranaggi che muovono l'economia digitale e la trasformazione digitale, svolgendo funzioni essenziali per lo sviluppo sociale ed economico, per i diritti umani e per la garanzia dei valori democratici all'interno di una società[3]. Questa nuova realtà rende necessarie la riduzione delle disuguaglianze esistenti e la garanzia di una connettività universale. È per questi motivi che il dibattito in merito all'inclusione digitale non può più incentrarsi esclusivamente sull'accesso fisico alla rete, bensì includere concettualizzazioni complesse, come ad esempio diversi tipi di abilità digitali, motivazioni dietro all'utilizzo della rete e capacità di creazione di opportunità derivanti da tale utilizzo[4]. Le politiche a favore dell'inclusione digitale e dell'universalizzazione della connettività devono insomma spingersi oltre il semplice accesso fisico per garantire lo sviluppo delle abilità digitali del singolo individuo, secondo i nuovi paradigmi imposti dalla società dell'informazione e dell'economia digitale.

Il presente articolo parte da una prospettiva storica per esplorare il ruolo fondamentale attualmente svolto dall'esperienza brasiliana di governance di Internet nell'elaborazione di politiche pubbliche, nonché nelle iniziative di organizzazioni accademiche e società civile volte a garantire l'inclusione digitale di persone e organizzazioni mirando a una connettività universale e significativa. La riduzione delle differenze di opportunità tra gli individui connessi e quelli che ancora non lo sono è una sfida che può essere affrontata migliorando l'infrastruttura di Internet nel paese, mediante ad esempio l'allocazione di risorse per lo scambio e la razionalizzazione del traffico, e migliorando l'efficienza della rete, al fine di favorire la riduzione di eventuali barriere, come il costo dell'accesso o le abilità digitali. Tali azioni sono direttamente collegate alla struttura della governance di Internet nata in Brasile quasi trent'anni fa. Per noi la governance è l'insieme dei meccanismi istituzionali, delle regole e delle norme che riguardano i processi decisionali condivisi tra rappresentanti del governo, delle imprese, di organizzazioni della società civile e della comunità accademica nei diversi domini relativi all'ambiente di Internet.

«La governance di Internet è sempre più presente nell'opinione pubblica. Quanto più la società moderna dipende da Internet, tanto più rilevante è la sua governance»[5]. Da un lato, la governance di Internet è un elemento centrale del processo di sviluppo, data la sua importanza per l'economia globale; dall'altro, è impossibile immaginare sforzi di sviluppo scollegati da Internet. È per questo che il dibattito in merito alla governance di Internet è in grado di influenzare la capacità di un paese di gestire questioni sociali, culturali, ambientali ed economiche riguardanti lo sviluppo. La governance di Internet assume pertanto un ruolo fondamentale nel promuovere l'inclusione digitale e ridurre le disuguaglianze attraverso la diffusione della connettività. Oltre all'universalizzazione della connettività e la conseguente riduzione delle disuguaglianze, tre ulteriori dimensioni della governance di Internet hanno assunto un ruolo centrale nel dibattito attuale: la protezione della privacy, la cybersicurezza e la garanzia dei diritti umani nell'ambiente online.

È evidente che il processo che ha dato origine al modello di governance di Internet in Brasile si è evoluto in modo collaborativo, neutrale e partecipativo, grazie ai contributi di diversi attori che rappresentano svariati settori della società; si tratta inoltre di un processo influenzato da importanti fatti storici che hanno contribuito all'espansione dell'accesso alla rete globale di computer. Il dialogo costruttivo tra governo e società ha dato origine a questo modello, la cui natura multi-stakeholder e la costante ricerca di consensi tra gli attori che lo compongono garantiscono una governance che riesce a influenzare non solo le politiche di universalizzazione della connettività, ma anche i dibattiti politici necessari a gestire l'odierna complessità dell'ambiente online. Secondo l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), la riuscita governance di Internet su suolo brasiliano è un parametro di riferimento a livello mondiale, giacché garantisce una configurazione multi-stakeholder capace di promuovere e coordinare dibattiti rilevanti di interesse nazionale in aree cruciali per la trasformazione digitale, la sicurezza digitale e la protezione dei dati personali, volti a favorire lo sviluppo di normative che includano diritti e doveri in ambito digitale[6]. I risultati positivi di questo modello sono frutto del dialogo multi-stakeholder che ha luogo nell'ambito del *Comitê Gestor da Internet no Brasil* (Comitato di Gestione di Internet in Brasile - CGI.br).

L'auspicio è che gli elementi costituenti dell'esperienza di governance in Brasile presentati in questo articolo possano contribuire all'elaborazione e all'implementazione di processi di governance di carattere multi-stakeholder che abbiano un impatto significativo sulla società.

2. Breve storia dell'accesso a Internet in Brasile

In Brasile, a partire dalla fine degli anni '80, numerosi sforzi sono stati rivolti all'ottenimento della connettività internazionale, soprattutto a beneficio della comunità accademica. Già nel 1988 si formarono su territorio brasiliano alcuni embrioni indipendenti di reti, che collegavano le grandi università e centri di ricerca di Rio de Janeiro, San Paolo e Porto Alegre agli Stati Uniti.

Con l'obiettivo di integrare tali sforzi, coordinare un'iniziativa nazionale per le reti in ambito accademico e favorire un dibattito su tali tematiche, il Ministero della Scienza e della Tecnologia[7] formò un gruppo composto da rappresentanti del *Conselho Nacional de Desenvolvimento Científico e Tecnológico* (Consiglio Nazionale di Sviluppo Scientifico e Tecnologico - CNPq), della *Financiadora de Estudos e Projetos* (Ente per il Finanziamento di Studi e Progetti - FINEP), della *Fundação de Amparo à Pesquisa do Estado de São Paulo* (Fondazione per il Sostegno alla Ricerca dello Stato di San Paolo - Fapesp), della *Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro* (Fondazione per il Sostegno alla Ricerca dello Stato di Rio de Janeiro - Faperj) e della *Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul* (Fondazione per il Sostegno alla Ricerca dello Stato di Rio Grande do Sul - Fapergs)[8]. Il progetto risultante, denominato *Rede Nacional de Ensino e Pesquisa* (Rete Nazionale di Istruzione e Ricerca - RNP), fu istituito formalmente nel settembre del 1989 e limitato agli ambiti federale e internazionale; a livello dei singoli Stati federali sarebbero state attuate iniziative per favorire la nascita di reti locali integrate al progetto nazionale e aumentare così la capillarità della rete.

Il 18 aprile 1989, la *Internet Assigned Numbers Authority* (IANA) delegò il dominio di primo livello .br al team responsabile per le reti accademiche presso la Fapesp[9]. Fu così che il dominio .br divenne il "cognome" di apparecchiature e servizi Internet in Brasile. Già verso la fine di quell'anno era possibile osservare una chiara tendenza di migrazione dalle diverse reti preesistenti a una rete specifica, Internet, la cui architettura (*Transmission Control Protocol/Internet Protocol* - TCP/IP) era stata scelta per l'installazione nel 1986 della *National Science Foundation Network* (NSFnet) negli Stati Uniti. Questa architettura e il suo protocollo divennero il modello di riferimento per l'interconnessione delle reti, in contrasto con la proposta di protocolli basati sul modello denominato *Open Systems Interconnection* (OSI). Gli anni '80 furono caratterizzati dall'espansione delle reti per soddisfare la domanda delle comunità accademiche e di ricerca; di particolare importanza furono le reti BITNET e NSFnet[10].

Quando il *Fermi National Accelerator Laboratory* (Fermilab) si collegò alla rete *Energy Sciences Network* (ESnet), *backbone* collegato alla NSFnet e supportato dal Dipartimento dell'Energia statunitense, anche la connessione della Fapesp passò a trasportare il protocollo TCP/IP. Tale evento fece sì che Internet potesse diventare accessibile in Brasile a partire da gennaio 1991. L'adozione del nuovo protocollo richiedeva l'impiego di router e apparecchiature ancora non disponibili nel paese, ed è per questo che per qualche anno Internet continuò ad essere affiancata da BITNET[11] e HEPnet[12]. Il 7 febbraio 1991, la connessione a Internet fu considerata completamente operativa e iniziò ad essere condivisa dalle istituzioni accademiche interessate a collegarsi alla rete.

Un processo parallelo avviato nel 1987 e gestito dall'*Instituto Brasileiro de Análises Sociais e Econômicas* (Istituto Brasiliano di Analisi Sociali ed Economiche - Ibase), di Rio de Janeiro, si proponeva di promuovere l'impiego di questa nuova tecnologia nell'ambito delle organizzazioni non governative (ONG) in Brasile. È importante sottolineare il ruolo dell'Ibase almeno per quanto riguarda la tappa della creazione della dorsale di rete pilota della RNP, dato che le due iniziative indipendenti si unirono in uno sforzo congiunto per rendere possibile il progetto Internet della UNCED 92 (Eco 92)[13], il che a sua volta favorì in modo decisivo l'impiego dei primi circuiti IP della nuova dorsale di rete accademica brasiliana. Alla fine del 1990, l'Ibase dava inizio al progetto "UNCED Information Strategy Project in Rio" (ISP/Rio), che in seguito fu incorporato nell'Host Country Agreement tra l'Organizzazione delle Nazioni Unite (ONU) e il Brasile per la realizzazione della Conferenza di Rio nel 1992: il progetto consisteva nel montaggio e nella gestione di una rete Internet che collegasse tutti gli spazi dell'evento tra loro e a Internet mediante una rete di microcomputer[14]. Il ruolo della RNP si rivelò fondamentale per il successo di questo progetto[15].

Oltre alla comunità scientifica e accademica, alcuni settori della società civile organizzata erano utenti attivi di reti di computer, che utilizzavano protocolli come *Unix to Unix Copy Protocol* (UUCP), Fido-

net[16] e altri ancora; all'epoca l'accesso era di tipo *dial-up*. Comunità come l'*Association for Progressive Communications* (APC) e, in Brasile, l'Ibase fornivano ai propri membri forme fattibili di intercomunicazione in rete. Mentre il mondo accademico e il terzo settore rappresentarono la prima ondata di utenti di Internet, la migrazione dei vecchi operatori di BBS (*bulletin board system*) – molti dei quali provenienti da un progetto di incentivazione all'interconnessione di BBS con Internet promosso dall'Ibase –, e l'adesione di aziende nel campo dei media determinarono una seconda ondata, che consentì a una grande porzione della società civile di accedere alla rete. Una terza ondata fu segnata dall'inizio della migrazione dei servizi pubblici governativi verso servizi di amministrazione digitale (e-gov), che passarono a essere offerti in rete. Infine, la quarta ondata fu caratterizzata dai fornitori di servizi di telecomunicazioni, che videro in Internet una promettente fonte di nuovi guadagni.

Adottando una prospettiva storica, è possibile identificare un ulteriore punto critico per l'evoluzione di Internet: il dibattito internazionale sulle questioni degli standard di protocolli e dell'architettura di rete. Il Brasile, come la maggior parte dei paesi, aveva adottato l'architettura di rete a strati così come stabilita nel 1977 dal modello OSI, sviluppato congiuntamente dagli enti *International Telecommunication Union* (ITU) e *International Organization for Standardization* (ISO). In Brasile, parte di tale architettura era utilizzata nella *Rede Nacional de Comunicação de Dados por Comutação de Pacotes* (Rete Nazionale di Comunicazione di Dati tramite Commutazione di Pacchetti - RENPAC). La sostituzione e la migrazione dal modello aperto allo standard TCP/IP avvennero in modo graduale, ma anche continuo e costante. Questo anche grazie alla posizione del Ministero delle Comunicazioni brasiliano, che nel 1995[17] definì Internet un "servizio a valore aggiunto"[18] e quindi non soggetto alla regolamentazione di organi legati alla fornitura di servizi di telecomunicazioni.

A partire dal 1995, alcune attività centrali di Internet, come la gestione del DNS (*Domain Name System*) e l'attribuzione di numeri IP, furono soggette a modifiche significative. Il Dipartimento del Commercio statunitense entra in scena e pubblica un *green paper*, seguito da un *white paper* che consente a un'istituzione privata non a scopo di lucro di amministrare nomi (domini) e numeri (indirizzi IP). Grazie a ciò, alcuni domini di primo livello, originariamente statunitensi, passarono ad essere amministrati dalla *Network Solutions, Inc.* (NSI), diventarono a pagamento e si trasformarono in "generici", ovvero dissociati dalla localizzazione geografica del registrante.

Con l'esplosione dei nomi di dominio, e con l'intento di risolvere possibili conflitti con marchi o diritti preesistenti, la *World Intellectual Property Organization* (WIPO) fu invitata a partecipare: l'obiettivo era elaborare una proposta per la risoluzione dei conflitti nell'ambito dei nomi di dominio.

In Brasile, il rapido aumento dei nomi di dominio sotto .br e della quantità di reti che si collegavano tramite Internet fece da catalizzatore per l'espansione delle dorsali di rete nel paese. Fin dalla creazione della RNP, l'espansione della sua stessa dorsale di rete nazionale, così come quella dei fornitori privati di servizi di telecomunicazioni, avvenne in modo esponenziale.

3. Il modello di governance adottato in Brasile

Alla fine del 1994, la principale società di telecomunicazioni brasiliana a livello nazionale, la statale *Empresa Brasileira de Telecomunicações* (Impresa Brasiliana di Telecomunicazioni - Embratel), decide di fornire l'accesso pubblico a Internet per mezzo di connessione *dial-up*, ovvero via rete telefonica. Evidentemente, Internet avrebbe raggiunto un gruppo di utenti più ampio rispetto a quello originale, rappresentato dalla comunità accademica, e ben presto sarebbe divenuta uno strumento a disposizione della società. Alcuni servizi amatoriali di scambio di messaggi tramite rete telefonica, i BBS, avevano deciso di uscire dal proprio isolamento e integrarsi alla rete.

Nel 1995 fu creato il Comitato di Gestione di Internet in Brasile (CGI.br), risultato di un'azione coordinata di vari pionieri della rete nazionale e di un'ordinanza interministeriale congiunta del Ministero della Scienza e della Tecnologia e di quello delle Comunicazioni. Questo comitato innovativo, inizialmente formato da nove membri, non aveva il carattere di "organo governativo", e acquisì il compito di "pensare e formulare raccomandazioni" per favorire lo sviluppo adeguato di Internet in Brasile. Non si trattava di un organo di regolamentazione, principalmente perché Internet era stata definita un "servizio a valore aggiunto" e quindi non soggetta alla regolamentazione delle telecomunicazioni, né si trattava di un organo sanzionatorio: il suo ruolo era quello di definire e diffondere le "buone pratiche" per la rete. Sarebbe stato un *think tank* che potesse indirizzare eventuali iniziative legislative future e partecipare ai dibattiti in merito alle politiche pubbliche considerate importanti per il corretto sviluppo e l'espansione di Internet nel paese. L'organico originale includeva rappresentanti di diversi settori della società: dal governo alla comunità accademica, dalle telecomu-

nicazioni ai fornitori di servizi di Internet, fino agli utenti stessi. Fu così che il CGI.br iniziò ad emettere risoluzioni al fine di indirizzare l'evoluzione e l'universalizzazione della connettività in Brasile[19].

Come già detto, il CGI.br nacque come comitato di individui impegnati per lo sviluppo di Internet nel paese, senza dotazione di risorse finanziarie o sede fisica. Fin da subito furono identificati alcuni punti di particolare rilievo, ad esempio strategie per minimizzare gli abusi della registrazione di quei nomi di dominio che rappresentavano una riserva di nomi buoni relativi a marchi preesistenti e conosciuti, ma che non avevano ancora aderito alla "novità" Internet. Un altro punto cruciale era la sicurezza in rete: già si potevano osservare azioni volte a ingannare utenti della rete, o situazioni in cui le buone pratiche di sicurezza non venivano applicate, o erano semplicemente ignorate.

Fino al 1997, le attività di registrazione per il Brasile furono gestite e sostenute dalla Fapesp. Tuttavia, lo scenario internazionale e la drastica crescita del .br dimostravano che tali operazioni dovevano diventare autosostenibili, così come sarebbe successo in seguito negli Stati Uniti. Il CGI.br decise quindi di fissare un costo per la registrazione e una tassa annua per i domini registrati sotto .br. La transizione durò due anni e fu un successo: le attività divennero autosostenibili e le risorse in eccesso passarono ad essere investite nello sviluppo di Internet nel paese. Nel 2002 fu creata una struttura istituzionale per un ente con personalità giuridica privata non a scopo di lucro: il *Núcleo de Informação e Coordenação do Ponto BR* (Nucleo di Informazione e Coordinamento del Punto BR - NIC.br).

Il CGI.br fu oggetto di una riformulazione importante nel 2003, a seguito del decreto presidenziale che sancì l'ampliamento della composizione del comitato e stabilì linee guida strategiche per l'uso e lo sviluppo di Internet in Brasile[20]. La configurazione attuale prevede 21 membri, e il carattere multi-stakeholder è tuttora un elemento imprescindibile. È prevista un'elezione per la nomina di membri non governativi da parte dei rispettivi settori e il mandato di tre anni è stato mantenuto fino ad oggi. La composizione per settori del CGI.br è illustrata nella Figura 1.

Il dialogo multi-stakeholder in merito alla gestione di Internet sotto l'egida del CGI.br ha contribuito enormemente allo sviluppo di Internet in Brasile, ad esempio generando input importanti per il dibattito pubblico circa le normative applicabili all'ambiente digitale online e per la creazione di leggi e risoluzioni. Tra le tematiche presenti in tale dialogo vale la pena annoverare: inclusione digitale e diffusione della banda larga, sicurezza delle informazioni, privacy, protezione dei dati personali, dati aperti, amministrazione digitale e accesso alle informazioni pubbliche. La produzione di dati ed evidenze per l'elaborazione di politiche pubbliche a favore dell'inclusione digitale e della diffusione della banda larga in case, scuole, strutture sanitarie e centri di servizi telematici è un risultato significativo reso possibile dall'approccio multi-stakeholder del comitato.

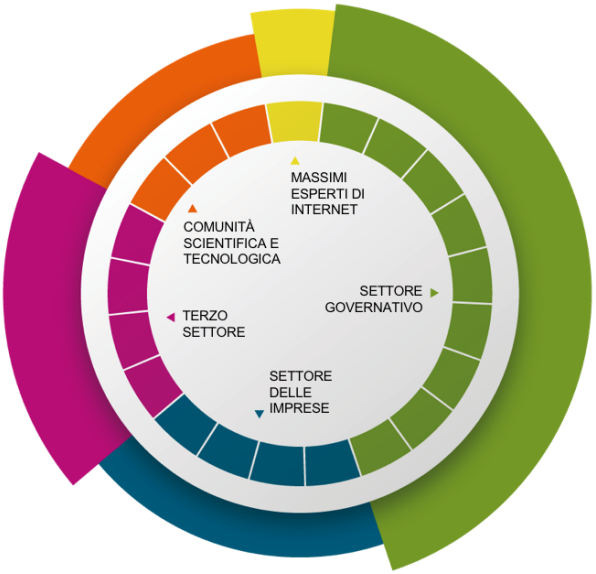

Figura 1: *Composizione del Comitato di Gestione di Internet in Brasile (Fonte: CGI.br, 2003)*

Nel 2009, il CGI.br ha approvato dieci principi per la governance e l'utilizzo di Internet in Brasile, noti anche come Decalogo di Internet[21], spinto dalla necessità di indirizzare le proprie azioni in base a principi fondamentali, per garantire i diritti e i doveri degli utenti della rete. Questa serie di principi è servita da base per la formulazione della legge denominata *Marco Civil da Internet* (Legge Quadro sui Diritti dell'Accesso a Internet)[22] e della *Lei de Proteção de Dados Pessoais* (Legge di Protezione dei Dati Personali - LGPD)[23], ad oggi le principali leggi che governano l'ambiente di Internet in Brasile. I principi del Decalogo del CGI.br sono elencati nella Figura 2.

Il Decalogo del CGI.br ha rappresentato un input fondamentale per la creazione di un quadro legale che regolasse l'utilizzo di Internet in Brasile in base a definizioni chiare di principi, garanzie, diritti e doveri per gli utenti della rete, e che determinasse linee guida per l'azione dello Stato in tale materia. Grazie a questo processo ampio e partecipativo che ha coinvolto l'intera società e grazie alla qualità dei suoi contenuti, la legislazione brasiliana è divenuta un riferimento a livello mondiale.

1. **Libertà, privacy e diritti umani**: L'uso di Internet deve attenersi ai principi di libertà di espressione, di privacy dell'individuo e del rispetto dei diritti umani, riconoscendoli come fondamentali per la preservazione di una società giusta e democratica.

2. **Governance democratica e collaborativa**: La governance di Internet deve essere attuata in modo trasparente, multilaterale e democratico, con la partecipazione dei vari settori della società, tutelando e stimolando il suo elemento di creazione collettiva.

3. **Universalità**: L'accesso a Internet deve essere universale, affinché possa essere un mezzo di sviluppo sociale e umano e contribuire alla costruzione di una società inclusiva e non discriminatoria a beneficio di tutti.

4. **Diversità**: La diversità culturale deve essere rispettata e preservata, e la sua espressione deve essere stimolata, evitando l'imposizione di credenze, costumi o valori.

5. **Innovazione**: La governance di Internet deve promuovere la continua evoluzione e l'ampia diffusione di nuove tecnologie e modelli di utilizzo e accesso.

6. **Neutralità della rete**: Il filtraggio e i privilegi di traffico devono rispettare esclusivamente criteri tecnici ed etici, e non sono ammesse motivazioni politiche, commerciali, religiose, culturali o qualsiasi altra forma di discriminazione o favoritismo.

7. **Non imputabilità della rete**: La lotta agli atti illeciti in rete deve riguardare i responsabili finali e non i mezzi di accesso e trasporto, sempre tutelando i principi fondamentali di difesa della libertà, della privacy e del rispetto dei diritti umani.

8. **Funzionalità, sicurezza e stabilità**: La stabilità, la sicurezza e la funzionalità globale della rete devono essere preservate attivamente adottando misure tecniche compatibili con gli standard internazionali e stimolando l'uso delle buone pratiche.

9. **Standardizzazione e interoperabilità**: Internet deve basarsi su standard aperti che consentano l'interoperabilità e la partecipazione di tutti al suo sviluppo.

10. **Ambiente legale e regolatorio**: L'ambiente legale e regolatorio deve essere volto a preservare la dinamica di Internet come spazio di collaborazione.

Figura 2: *Principi del Decalogo di Internet del CGI.br (Fonte: CGI.br, 2009)*

Il *Marco Civil da Internet* è stato approvato durante l'evento denominato *Global Multistakeholder Meeting on the future of Internet Governance* - NETmundial), organizzato dal CGI.br e dal NIC.br nel 2014[24]. In quell'occasione, furono discusse l'evoluzione futura dell'ecosistema Internet e la necessità di elaborare principi di governance globale di Internet, tema di crescente attualità data l'importanza di Internet e delle reti sociali, delle dispute nel cyberspazio e delle ripercussioni nel dibattito politico e democratico, nella politica, nell'economia e nelle relazioni internazionali. Il NETmundial fece sperare che il processo internazionale di discussione e ricerca di soluzioni per le importanti sfide in ambito di governance potesse finalmente sfociare in proposte concrete, sia per quanto riguarda un consenso sui principi di tale governance che sul cammino da percorrere. Per la prima volta, un dibattito sullo stesso livello riunì tutti i settori per la redazione di due documenti: una dichiarazione universale dei cosiddetti "Internet Governance Principles" e una "Internet Governance Roadmap". L'evento si tenne a seguito di otto edizioni dell'IGF, il forum globale annuale sulla governance di Internet realizzato sotto l'egida dell'ONU, in base a un'agenda che, sebbene fosse stata adottata come coronamento della seconda fase del Vertice Mondiale sulla Società dell'Informazione, non aveva prodotto innovazioni significative[25].

Il CGI.br ha contribuito attivamente e permanentemente ai forum internazionali che trattano delle dimensioni complesse e interdipendenti della governance di Internet. Oltre a occuparsi dell'organizzazione e del finanziamento dell'evento NETmundial, il CGI.br e il NIC.br hanno organizzato e realizzato due edizioni dell'IGF[26], nel 2007 e nel 2015, in Brasile, unico paese ad aver ospitato il forum globale due volte. La Figura 3 mostra alcuni dei forum in occasione dei quali il CGI.br ha svolto un ruolo fondamentale nel dibattito sulla governance di Internet.

4. Il modello duale: CGI.br|NIC.br

La struttura istituzionale che rappresenta il modello brasiliano di governance di Internet è costituita dal CGI.br e dal NIC.br, che insieme formano un modello duale di governance.

Il CGI.br non ha personalità giuridica, svolge un ruolo politico ed è responsabile per il coordinamento e l'integrazione delle iniziative e dei servizi di Internet nel paese, in virtù di un decreto del governo federale. In tale contesto, ha il compito di stabilire linee guida strategiche per l'utilizzo e lo sviluppo di Internet in Brasile, oltre a linee guida per la registrazione di nomi di dominio .br (nomi) e l'assegnazione di indirizzi IP (numeri) a livello nazionale. Inoltre, promuove studi ed emette raccomandazioni su procedure per la sicurezza di Internet, e propone programmi di ricerca e sviluppo che consentano di mantenere il livello di qualità tecnica e innovazione nell'utilizzo di Internet.

Il NIC.br è formalmente un ente della società civile senza scopo di lucro, di diritto privato, istituito nel 2005 con il fine di amministrare e realizzare iniziative sotto la supervisione del CGI.br. L'ente amministra le risorse ottenute con la registrazione di nomi e numeri.

Prima ancora dell'inizio dei lavori del NIC.br, Registro.br ottenne, nel 1994, lo status di *National Internet Registry* (NIR), e passò così a essere il distributore nazionale di indirizzi IP versioni 4 e 6, nonché responsabile per la designazione di Sistemi Autonomi (*Autonomous System* – AS). Le risorse finanziarie ricavate dalla registrazione di nomi di dominio furono inizialmente depositate in un conto separato presso la Fapesp e servirono in un primo momento per sostenere l'infrastruttura di apparecchiature, reti e persone di Registro.br, che, nel 2000, riuscì a ottenere un proprio spazio fisico e un'infrastruttura adeguata. Il percorso verso l'istituzionalizzazione del NIC.br fu intrapreso dall'insieme dei consiglieri del CGI.br nel 2002 e fu concluso nel 2005, anno in cui il NIC.br iniziò a ricevere direttamente le risorse ottenute dalla registrazione dei domini del .br e dalla distribuzione degli indirizzi IP. Da quel momento fu possibile assumere direttamente personale e acquisire apparecchiature e servizi per svolgere in sicurezza le varie attività.

La rapida espansione del dominio .br, una buona amministrazione tecnica e alcune caratteristiche distintive importanti fecero sì che, in breve tempo, si accumulasse un'eccedenza di risorse che poterono essere investite in attività per lo sviluppo e il continuo miglioramento dell'Internet brasiliana. Fu così che il NIC.br, che già ospitava il *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil* (Centro di Studi, Risposta e Gestione di Incidenti di Sicurezza in Brasile - CERT.br), iniziò a pianificare l'inclusione di altre attività importanti: la creazione di un sistema nazionale di scambio di traffico, la misurazione della qualità di Internet nel paese, la promozione del protocollo IPv6, il monitoraggio dell'evoluzione degli standard Web e la produzione di dati statistici riguardanti la penetrazione di Internet in vari settori della società.

Il NIC.br (Figura 4) si strutturò dunque in vari progetti al fine di agire su aree critiche per lo sviluppo di un'Internet di alta qualità e sicura per tutti, approfittando delle risorse acquisite dalla gestione della registrazione di domini .br. Alcuni di questi progetti furono destinati ad alcuni ambiti dell'infrastruttura, come l'implementazione e il funzionamento di Punti di Scambio di Traffico (IX.br), la gestione degli incidenti di sicurezza (CERT.br) e lo studio delle tecnologie di reti e operazioni (Ceptro.br), mentre altri riguardavano lo sviluppo globale del Web (Ceweb.br) e le ricerche per la produzione di statistiche pubbliche su aspetti della diffusione di Internet nella nostra società (Cetic.br). Tutte queste aree generano dati importanti e supportano la formulazione e il monitoraggio di politiche pubbliche, oltre ad essersi rivelate fondamentali per la misurazione dell'impatto di Internet sui diversi strati della società brasiliana. In più, il NIC.br ospita l'ufficio brasiliano del W3C.

Il NIC.br svolge un'ampia gamma di attività per la diffusione e l'adozione dell'IPv6 in Brasile: corsi di formazione, produzione di materiali di supporto tecnico protetti da licenza *Creative Commons*, cicli di conferenze presso università, aziende ed eventi in ambito tecnologico, nonché eventi come i *Fóruns Brasileiros de Implementadores* IPv6 (Forum Brasiliani di Implementatori IPv6) e IPv6 *no Café da Manhã* (IPv6 a Colazione).

Grazie alla qualità e alla sicurezza del funzionamento di Internet su suolo brasiliano, il .br è divenuto il nome di dominio preferito nel paese: nel novembre del 2021, il Brasile risultava sesto nel *ranking* delle

Figura 3: *Partecipazione del CGI.br a forum internazionali sulla governance di Internet (Fonte: elaborata dagli autori)*

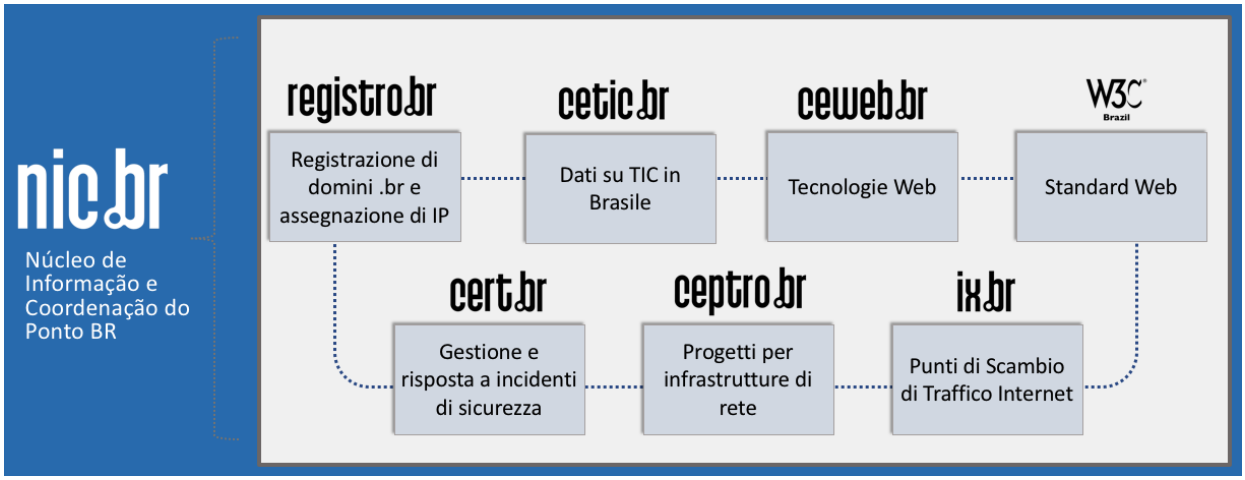

Figura 4: *Aree di attività del NIC.br (Fonte: elaborata dagli autori)*

maggiori basi di nomi di dominio nazionali delle più grandi economie mondiali, con 4,85 milioni di domini. La Figura 5 mostra la posizione del Brasile in relazione ai paesi membri dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) e del G20. Il totale delle registrazioni di nomi di dominio di questi paesi è pari a 89,75 milioni, e il Brasile ne detiene il 5,4%.

Secondo la *Internet Society*[27], il Brasile è secondo solo agli Stati Uniti per quanto riguarda l'allocazione di Sistemi Autonomi (AS)[28], con 8.865 dei 109.046 esistenti sul pianeta al momento della redazione del presente articolo, ovvero l'8,1% degli AS di tutto il mondo.

La quantità di domini e di AS esistenti nel paese è un riflesso dell'efficienza e della qualità del modello di governance adottato in Brasile, che, oltre a garantire il funzionamento delle migliaia di reti AS collegate, ha abbattuto le barriere amministrative per ottenere le designazioni di numeri di rete, incentivando l'interconnessione di rete nei suoi punti di scambio di traffico. Ciò riflette inoltre il livello di cooperazione internazionale con altri DNS e con la *Country Code Names Supporting Organisation* (ccNSO)[29], organizzazione di supporto a nomi di codice nazionali all'interno della struttura della *Internet Corporation for Assigned Names and Numbers* (ICANN)[30], con il fine di sostenere i gestori di nomi di dominio di primo livello nazionali.

Per quanto riguarda il miglioramento della qualità di Internet in Brasile, il NIC.br si impegna per la promozione della diffusione dell'IPv6 e per l'e-

Posizione	Paese	Numero di domini	Data di riferimento	Fonte (sito)
1	Germania (.de)	17.109.697	30/11/2021	https://www.denic.de
2	Cina (.cn)	9.837.644	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
3	Regno Unito (.uk)	9.703.171	01/06/2021	https://www.nominet.uk/news/reports-statistics/uk-register-statistics-2021/
4	Paesi Bassi (.nl)	6.219.806	30/11/2021	https://api.sidn.nl/rest/counters/domains
5	Russia (.ru)	5.025.335	30/11/2021	https://cctld.ru
6	Brasile (.br)	4.858.768	30/11/2021	https://registro.br/dominio/estatisticas/
7	Francia (.fr)	3.874.717	30/11/2021	https://www.afnic.fr/en/observatory-and-resources/statistics/
8	Unione Europea (.eu)	3.666.151	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
9	Italia (.it)	3.456.471	30/11/2021	http://nic.it
10	Australia (.au)	3.401.599	30/11/2021	https://www.auda.org.au/
11	Canada (.ca)	3.214.548	30/11/2021	https://www.cira.ca
12	Colombia (.co)	3.186.901	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
13	India (.in)	2.586.097	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
14	Polonia (.pl)	2.521.965	30/11/2021	https://www.dns.pl/en/
15	Svizzera (.ch)	2.459.804	15/11/2021	https://www.nic.ch/statistics-data/domains_ch_monthly.csv
16	Spagna (.es)	1.980.363	25/10/2021	https://www.dominios.es/dominios/en
17	Belgio (.be)	1.735.833	30/11/2021	https://www.dnsbelgium.be/en
18	Stati Uniti d'America (.us)	1.735.153	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
19	Giappone (.jp)	1.674.481	30/11/2021	https://jprs.co.jp/en/stat/
20	Svezia (.se)	1.508.386	30/11/2021	https://internetstiftelsen.se/en/domain-statistics/growth-se/?chart=active

Dati raccolti il 30 novembre 2021.

Figura 5: *Totale delle registrazioni di nomi di domini nei paesi dell'OCSE e del G20 (Fonte: J.M. Martins Jr., Panorama Setorial da Internet (PSI), n. 4, 2021)*

spansione dello scambio di traffico via IX.br. La rete IX.br presenta quello che attualmente è il più grande punto di scambio di traffico del mondo in termini di volume lordo di dati, quello di San Paolo, il cui picco giornaliero di traffico raggiunge al momento i 21 terabit al secondo[31]. Nonostante sia un valore significativamente alto, è comunque inferiore alla metà della capacità supportata dalla rete IX.br del NIC.br. In più, il NIC.br offre il *Sistema de Medição de Tráfego* (Sistema di Misurazione del Traffico - SIMET), un contatore di velocità Internet completo che verifica, oltre alla banda di *download* e *upload*, svariate metriche di qualità Internet che influenzano direttamente la navigazione e l'utilizzo della rete.

Oltre ai progetti riguardanti l'infrastruttura e la sicurezza, dal 2005 il NIC.br produce regolarmente statistiche sull'adozione e l'utilizzo di Internet e tecnologie digitali nel paese. Il programma complesso e dinamico di trasformazione digitale implica una rilevanza ancor più accentuata per il monitoraggio dell'adozione delle tecnologie da parte dei diversi settori quali salute, istruzione, cultura, trasformazione digitale delle aziende, dei servizi governativi e l'accesso nelle abitazioni, soprattutto da parte di

bambini e adolescenti. La produzione dei dati statistici è realizzata dal *Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação* (Centro Regionale di Studi per lo Sviluppo della Società dell'Informazione - Cetic.br), attivo a livello regionale in America Latina e nei paesi africani di lingua portoghese come Centro di categoria II, sotto l'egida dell'UNESCO. Si tratta di uno sforzo permanente del NIC.br volto a monitorare l'impatto delle nuove tecnologie sull'economia e la società.

5. Società dell'informazione: governance di Internet e diritti alla connettività

Le dinamiche recenti più significative che coinvolgono vari settori della società con lo scopo di definire diritti nella società contemporanea, di fronte ai progressi tecnologici nei campi della comunicazione e dell'informazione, hanno origine in due filoni: quello intergovernativo e quello della società civile organizzata.

Nel 1998, una risoluzione dell'ITU propose all'ONU di occuparsi dell'organizzazione di un Vertice Mondiale sulla Società dell'Informazione (WSIS)[32]. La proposta fu accolta nel 1999 e l'incarico fu assegnato al Segretariato delle Nazioni Unite. Il processo si sarebbe svolto in due fasi: la prima a Ginevra nel dicembre del 2003 e la seconda a Tunisi nel novembre del 2005. La gestione sarebbe stata a carico dell'ITU; un processo preparatorio intergovernativo definì il programma e le modalità di partecipazione, oltre alla bozza di una Dichiarazione di Principi e di un Piano di Azione[33].

Per quanto riguarda invece la società civile, a partire dal 2001 fu organizzata una campagna internazionale denominata *Communication Rights in the Information Society* (CRIS)[34]: l'iniziativa partì da un gruppo di ONG e movimenti sociali coinvolti nella difesa dei diritti nei media e nelle comunicazioni in generale. La CRIS si avvalse dei contributi della Commissione MacBride (1980), dei dibattiti avviati negli anni '60 dal Consiglio Economico e Sociale delle Nazioni Unite (ECOSOC, 1961)[35] e dei risultati dei dibattiti promossi negli anni '70 e '80 nell'ambito dell'UNESCO sul "nuovo ordine mondiale dell'informazione e della comunicazione" (*New World Information and Communication Order* - NWICO) per formulare il concetto di "diritto alla comunicazione". La campagna manteneva relazioni istituzionali con l'ONU, il che favorì una partecipazione multi-stakeholder ai processi della WSIS.

La prima fase del vertice aveva l'obiettivo di sviluppare e favorire una proposta oggettiva di determinazione politica e intraprendere passi concreti per gettare le fondamenta di una società dell'informazione per tutte e tutti, tenendo conto dei diversi interessi di ogni settore. Una delle sfide più importanti era concettualizzare la governance di Internet; a questo scopo fu costituito un gruppo multi-stakeholder chiamato *Grupo de Trabalho sobre Governança da Internet* (Gruppo di Lavoro sulla Governance di Internet - GTGI)[36]. Nel giugno del 2005, a seguito di intensi dibattiti, il gruppo presentò una "definizione operativa" di quella che sarebbe stata la governance di Internet così come adottata dall'ONU: «La governance di Internet è lo sviluppo e l'applicazione da parte dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, di principi, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet»[37].

Nel 2005, a Tunisi, il vertice sviluppò una proposta dettagliata che includeva politiche di stimolo all'accesso universale, attribuendo particolare importanza alle lingue e alle culture locali nel contesto della Società dell'Informazione. Uno dei provvedimenti concreti fu la proposta di creare un forum annuale multi-stakeholder sulla governance di Internet, l'IGF, sotto l'egida del Segretariato dell'ONU, con una scadenza iniziale di cinque anni[38].

L'IGF nacque come uno spazio non vincolante di dialogo sulle politiche, con l'obiettivo centrale di facilitare lo scambio di esperienze e di migliori pratiche per lo sviluppo della società dell'informazione e di Internet. Il primo forum fu realizzato nel 2006 ad Atene. Il forum servì a stimolare il dibattito sulla governance in molti paesi ed ebbe come risultato la creazione, in particolare a partire dal 2008 (anno in cui l'IGF evidenziò in modo esplicito l'importanza dell'accesso universale), di forum nazionali e regionali sulla governance di Internet. Fu così che ebbe origine una rete internazionale informale di istanze di dialogo sulla governance della rete, che influì in molti casi sulle politiche nazionali relative a Internet, relazionandosi in modo più o meno stretto con i processi annuali di organizzazione dello stesso IGF.

Vale la pena sottolineare che, a partire dall'IGF di Istanbul nel 2014, iniziarono a essere lanciati forum di migliori pratiche come parte del processo intersessionale, in un certo qual modo derivati da proposte provenienti dal NETmundial. A partire da allora sono nati svariati forum, diversi tra loro in termini di formato, estensione, obiettivi e forme di partecipazione, e alcuni dei quali temporanei: dopo il 2014 sono state costituite almeno nove istanze di dialogo di questo tipo[39].

L'ecosistema internazionale della governance di Internet fu uno dei motivi per cui venne approvata la continuità dell'IGF dopo i primi cinque anni.

Nell'IGF del 2021, uno dei due argomenti principali di discussione fu il tema "accesso universale e connettività significativa", motivato principalmente dalla necessità della connettività universale, resa palese dalla pandemia. È importante notare che uno dei documenti di base per la WSIS nel 2003, la Dichiarazione di Principi, in pratica definì implicitamente il concetto di "connettività significativa": «[...] costruire una Società dell'Informazione incentrata sulla persona, che sia inclusiva e orientata allo sviluppo, in cui tutti possano creare, avere accesso, utilizzare e condividere informazioni e conoscenze, mettendo in grado individui, comunità e popoli di realizzare appieno il proprio potenziale, promuovendo il loro sviluppo sostenibile e migliorando la loro qualità di vita, basandosi sui propositi e i principi della Carta delle Nazioni Unite e rispettando pienamente e difendendo la Dichiarazione Universale dei Diritti Umani»[40].

La dichiarazione sottolineava inoltre l'importanza della sfida di portare avanti questo impegno, indicando che l'universalizzazione dell'accesso alle TIC va ben oltre la semplice connettività: «La sfida che ci attende è sfruttare il potenziale delle TIC per promuovere gli Obiettivi di Sviluppo del Millennio (OSM/MDG), ovvero: sradicare la povertà estrema e la fame, rendere universale l'istruzione primaria, promuovere la parità dei sessi e l'autonomia delle donne, ridurre la mortalità infantile, ridurre la mortalità materna, combattere l'HIV/AIDS, la malaria e altre malattie, garantire la sostenibilità ambientale e sviluppare un partenariato mondiale per lo sviluppo di un mondo più pacifico, giusto e prospero»[41].

Nel 2015, le mete degli Obiettivi di Sviluppo del Millennio (OSM) sono state sostituite dall'Assemblea Generale delle Nazioni Unite con i 17 Obiettivi di Sviluppo Sostenibile (OSS), da raggiungere entro il 2030. Nel contesto delle discussioni avviate in occasione della Conferenza delle Nazioni Unite sullo Sviluppo Sostenibile nel 2012 (Rio+20), gli OSS rappresentano un approfondimento delle mete originali, dato che prendono in considerazione quelle barriere sistemiche dello sviluppo sostenibile non esplicitate negli OSM, quali disuguaglianza, profili insostenibili di consumo, limiti della capacità istituzionale e degrado ambientale.

Fondamentalmente, si ricerca una caratterizzazione della "connettività significativa" che sia, tra l'altro:

- basata su evidenze di rilevanza fornite dagli stessi utenti;
- universale per tutti i generi, i ceti sociali e le etnie;
- aperta, senza restrizioni o pacchetti di dati limitativi.

In altre parole, si presuppone una velocità sufficiente per gli standard attuali di Internet, funzionalità soddisfacenti del dispositivo dell'utente per la creazione e l'interazione, senza *data caps* e con qualità idonea a soddisfare la domanda di apprendimento a distanza, lavoro in remoto, servizi di telemedicina e uso illimitato di servizi di tipo e-gov, oltre a opzioni di intrattenimento. Si osserva, tuttavia, che universalizzare l'accesso senza *data caps* e con connettività permanente presso tutti i domicili è una sfida che mette in difficoltà la stragrande maggioranza dei paesi, inclusi quelli più avanzati.

Di conseguenza, molte delle iniziative volte ad aggirare o attenuare il problema della connettività sono attuate principalmente da organizzazioni locali, ovvero le molte versioni di reti comunitarie, con o senza l'appoggio dei governi locali. In generale, queste reti dispongono di alternative precarie di accesso a Internet.

Vista la complessità della sfida, l'IGF del 2021 ha proposto la formazione di una rete di politiche riguardanti il cosiddetto "accesso significativo": un termine più ampio rispetto a "connettività significativa", dato che include tutti i livelli della rete e tutte le modalità di uso e applicazioni. A partire da questa visione olistica, l'accesso alla rete è considerato uno degli elementi decisivi per il raggiungimento dei 17 OSS dell'agenda per lo sviluppo sostenibile. Inoltre, nonostante l'accesso all'infrastruttura sia fondamentale, se non è inclusivo, utile, sostenibile, permanente e accessibile, nonché vincolato allo sviluppo delle capacità e all'offerta di contenuti che le rendano fattibili, non raggiungerà mai tale rilevanza.

Una delle condizioni di contorno che tuttora limitano l'accesso universale è la disuguaglianza in termini di sviluppo socioeconomico: le statistiche dimostrano che più della metà della popolazione mondiale dispone di una forma di accesso a Internet, per la maggior parte precario, tramite cellulari prepagati a un costo relativamente alto, con pacchetti di dati estremamente limitati, mentre oltre 3,5 miliardi di persone dispongono di un accesso precario o nullo all'energia elettrica, senza parlare del 20% delle abitazioni nel mondo ancora non dotate di corrente[42].

Secondo Michael Oghia, «come possiamo aspettarci che persone e comunità che non sono nemmeno collegate alla rete elettrica possano partecipare online in lingue che non parlano o con un dispositivo che, quando ne hanno uno, non possono neanche caricare facilmente?»[43]. Tipicamente non esiste un piano strategico per far arrivare le dorsali di rete in fibra a tutti i comuni: di solito questo compito è lasciato al "mercato", il che approfondisce ancora di più le disuguaglianze di accesso. Nessun paese rende universale

(con qualità sufficiente per un pieno utilizzo di Internet) la rete mobile cellulare senza una rete territorialmente universalizzata in fibra a prova di futuro.

Bisogna inoltre tener conto dei costi e della qualità dei dispositivi che rendono fattibile l'accesso. Una connettività stabile di buona qualità e a un prezzo ragionevole che arrivi a un domicilio in cui la famiglia non può permettersi un computer è impraticabile. L'accesso universale è molto più che semplicemente essere connessi a un prezzo ragionevole. È necessario approfondire una nozione di accesso pieno e insistere sulla qualità e sulla permanenza nelle abitazioni. In sintesi: deve essere una connettività a un prezzo ragionevole, permanente e con qualità compatibile con l'Internet multimediale di oggi in tutti i domicili a caratterizzare la connettività significativa.

Internet è una costruzione collettiva il cui accesso deve essere consentito a tutti. Il suo modello di governance ha il compito di assicurare l'equilibrio tra gli interessi dei settori coinvolti, ed è per questo che deve essere di tipo multi-stakeholder. Questa visione è condivisa sia dalle organizzazioni internazionali operanti in questo contesto, sia dai governi democratici.

Il Consiglio per i Diritti Umani delle Nazioni Unite, mediante la risoluzione HRC 20/13 del 5 luglio 2012[44], considera l'accesso a Internet un fattore fondamentale per l'esercizio dei diritti umani e sottolinea che i diritti offline devono essere applicati in egual modo nel mondo online, indipendentemente dalle frontiere e dai mezzi scelti, e garantendo in particolare la libertà di espressione. Questa decisione riconosce inoltre l'importanza della natura globale e aperta di Internet come elemento trainante dello sviluppo.

I dibattiti ampi e partecipativi a proposito della problematica multidimensionale dell'inclusione digitale, stimolati dal modello brasiliano della governance di Internet, hanno prodotto input importanti per l'elaborazione di politiche pubbliche e azioni strategiche del governo volte ad accelerare l'espansione della connettività, mirando alla connettività universale. Attualmente, l'81% della popolazione del Brasile è utente di Internet; negli strati sociali più alti, l'utilizzo è universale[45]. Tuttavia, esistono ancora sfide importanti da affrontare prima di raggiungere la connettività significativa. In primo luogo, esistono restrizioni di accesso imposte da dispositivi che limitano il pieno sviluppo delle abilità digitali; in secondo luogo, esistono restrizioni imposte dalle stesse abilità digitali della popolazione brasiliana.

6. Conclusioni

Sebbene l'accesso a Internet in Brasile sia aumentato notevolmente nel corso degli ultimi anni, è tuttora possibile osservare limitazioni a un accesso pieno alle opportunità offerte da Internet nei segmenti più vulnerabili della società e nelle regioni rurali. La pandemia di COVID-19 in Brasile ha provocato un aumento della connettività determinato dall'inclusione di questa porzione della popolazione, soprattutto per mezzo di dispositivi mobili. Tuttavia, anche considerando solamente le abitazioni collegate, nel paese continuano ad esistere le disuguaglianze storiche, con un nuovo formato: l'aumento della proporzione delle abitazioni collegate, anche se senza computer e con accesso tramite dispositivi mobili, è una realtà nelle classi più svantaggiate della società brasiliana. Per questo, una parte delle abitazioni adesso collegate ha un accesso più ristretto alle possibilità offerte da Internet[46].

Le politiche a favore dell'inclusione digitale e dell'universalizzazione della connettività devono spingersi oltre il semplice accesso fisico e garantire piuttosto una "connettività significativa"[47]. Devono dunque contemplare svariati aspetti, come lo sviluppo delle attività digitali e la frequenza di utilizzo di Internet, con dispositivi adeguati, mediante una connessione di velocità appropriata e con un volume sufficiente di dati[48]. La riduzione delle differenze di opportunità tra i connessi e coloro che ancora non lo sono è una sfida che deve essere affrontata con politiche pubbliche adeguate e azioni intraprese da più attori.

In questo senso, i meccanismi di governance di Internet esistenti in un paese possono favorire processi decisionali, condivisi tra rappresentanti del governo, delle imprese, di organizzazioni della società civile e della comunità accademica, che garantiscano la diffusione della connettività.

Il modello di governance di Internet in Brasile, rappresentato dal CGI.br, è stato in grado di promuovere dialoghi costruttivi tra il governo e la società che hanno influito sull'elaborazione di normative adeguate e politiche pubbliche più efficaci per l'espansione della connettività universale e la realizzazione di una connettività significativa. Il modello di governance brasiliano ha potuto avere insomma un impatto significativo sui dibattiti politici necessari per rispondere alla natura altamente dinamica di Internet. Questo modello si è inoltre dimostrato capace di preservare il dinamismo e la capacità di innovare e creare soluzioni tecniche e normative aderenti all'ecosistema di Internet in un contesto di trasformazione digitale della società.

Il CGI.br è stato creato attraverso processi democratici e multi-stakeholder, e, fin dall'inizio, è stato in grado di garantire la partecipazione attiva e significativa di tutte le parti coinvolte nell'ecosistema di Internet. All'interno di questo modello, i ruoli e le responsabilità di queste parti interessate sono interpretati in modo flessibile, equilibrato e trasparente, con lo scopo di giungere ad accordi di governance di Internet che soddisfino le esigenze della società brasiliana.

Note

[1] M. Castells, *A Sociedade em rede (A era da Informação: economia, sociedade e cultura*, Paz e Terra, vol. I, 2000.

[2] Organização das Nações Unidas para a Educação a Ciência e a Cultura (UNESCO), *As pedras angulares para a promoção de sociedades do conhecimento inclusivas. Acesso à informação e ao conhecimento, liberdade de expressão e ética na Internet global*, UNESCO, 2017.

[3] W. Kleinwächer (ed.), *Human rights and internet governance*, Co:llaboratory Discussion Paper Series n. 1, 2012.

[4] E.J. Helsper, A.J.A.M. van Deursen, R. Eynon, *Tangible Outcomes of Internet Use. From Digital Skills to Tangible Outcomes project report*, Oxford Internet Institute, University of Twente and London School of Economics and Political Science, 2015.

[5] J. Kurbalija, *Uma introdução à Governança da Internet*, CGI.br, 2016.

[6] Organisation for Economic Co-operation and Development (OECD), *A Caminho da Era Digital no Brasil*, OECD Publishing, 2020.

[7] Attuale Ministero della Scienza, della Tecnologia e delle Innovazioni (MCTI).

[8] Il *Laboratório Nacional de Computação Científica* (Laboratorio Nazionale di Computazione Scientifica, LNCC), attualmente vincolato al Ministero della Scienza, della Tecnologia e dell'Innovazione, nacque alla fine degli anni '70 e aveva inizialmente lo scopo di sviluppare ricerche in applicazioni matematiche. Fu questo laboratorio a realizzare la prima connessione di reti di computer del paese, tramite la rete BITNET. Per ulteriori informazioni, visitare la pagina relativa nel sito del Ministero.

[9] La Fapesp è una delle agenzie principali per il finanziamento della ricerca scientifica e tecnologica in Brasile ed è afferente alla Segreteria per lo Sviluppo Economico.

[10] M. Stanton, *A Evolução das Redes Acadêmicas no Brasil: Parte 1 - da BITNET à Internet*, in "Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP", vol. 2, 1998, n. 6.

[11] Acronimo di *Because It's Time to NETwork o Because It's There NETwork* che indica una rete remota creata nel 1981 a partire dal collegamento tra l'Università di New York e l'Università di Yale, con lo scopo di mettere a disposizione del mondo accademico un mezzo di comunicazione rapido ed economico.

[12] Sigla di *High-Energy Physics Network*, una rete di telecomunicazioni per ricercatori di fisica delle alte energie.

[13] *United Nations Conference on Environment and Development (UNCED)*: Conferenza sull'ambiente e lo sviluppo delle Nazioni Unite, chiamata anche Eco 92, Summit della Terra, *Cimeira do Verão* (Vertice Estivo), Conferenza di Rio de Janeiro e Rio 92; conferenza di vari paesi organizzata dalle Nazioni Unite e realizzata dal 3 al 14 giugno 1992 nella città di Rio de Janeiro, in Brasile, con l'obiettivo di discutere i problemi ambientali globali.

[14] Ulteriori informazioni sulla prima connessione Internet in Brasile al di fuori del mondo accademico sono disponibili su C. De Luca, *A primeira conexão internet no Brasil fora da academia acaba de fazer 25 anos*, 2017.

[15] Ulteriori dettagli sulla storia della formazione della RNP e sulla partecipazione multi-stakeholder in Brasile all'inizio di Internet in C.A. Afonso, C.J. Brito, F.Q.S. Kneese, *Avaliação de Projeto: Desenvolvimento Estratégico em Informática (DESI)*, CNPq/PNUD, 1999.

[16] Rete di scambio di messaggi tra BBS, fondata nel 1984 da Tom Jennings a San Francisco, in California, negli Stati Uniti. Il servizio si chiamava Netmail e fu il precursore della posta elettronica di Internet.

[17] L'*Agência Nacional de Telecomunicações* (Agenzia Nazionale di Telecomunicazioni - Anatel), ovvero l'agenzia di regolamentazione brasiliana, fu istituita due anni più tardi, nel 1997.

[18] Il concetto di "servizio a valore aggiunto" è definito dalla norma 04/95 approvata dall'ordinanza n. 148/95 del Ministero delle Comunicazioni.

[19] Per ulteriori informazioni sui principali eventi della storia del CGI.br, visitare la pagina relativa.

[20] Vedi il decreto n. 4.829 del 2003.

[21] Comitê Gestor da Internet no Brasil (CGI.br), Resolução CGI.br/RES/2009/003/P, CGI.br, 2009.

[22] Il Marco Civil fu approvato nel 2014 tramite la Legge n. 12.965/2014.

[23] Vedi il contenuto della *Lei de Proteção de Dados Pessoais*.

[24] Per ulteriori informazioni, visitare il sito di NETmundial.

[25] W. Kleinwächter, *NETmundial: Watershed in Internet Policy Making?*, in W.J. Drake, M. Price (eds.), "Internet Governance: The NETmundial Roadmap", USC Annenberg Press, 2014.

[26] Per ulteriori informazioni, visitare il sito dell'Internet Governance Forum.

[27] M. Ford, *Where Are the Internet Networks?*, Internet Society Pulse Blog.

[28] Gli AS sono gruppi di prefissi di routing, gruppi di reti IP, gestiti in modo indipendente. Il loro volume offre un'indicazione approssimativa della quantità di reti diverse collegate a Internet.

[29] L'organizzazione *Country Code Names Supporting Organisation* (ccNSO), istituita nel 2003, offre ai gestori di dominio di primo livello nazionali (ccTLD) uno spazio di dibattito su questioni riguardanti la gestione di nomi di dominio in una prospettiva globale.

[30] L'ICANN sviluppa politiche relative a una gamma ristretta di questioni globali riguardanti i domini di primo livello nazionali.

[31] Cfr. le informazioni sul traffico della rete IX.br, gestita dal NIC.br, rese disponibili giornalmente.

[32] In inglese, World Summit on the Information Society (WSIS).

[33] Comitê Gestor da Internet no Brasil (CGI.br), *Documentos da Cúpula Mundial sobre a Sociedade da Informação*, ITU, 2005.

[34] Per ulteriori informazioni, visitare il sito dell'Association for Progressive Communication.

[35] Per ulteriori informazioni, visitare il sito dell'ECOSOC.

[36] In inglese, *Working Group on Internet Governance* (WGIG).

[37] Working Group on Internet Governance (WGIG), *Report of the Working Group on Internet Governance*, Château de Bossey, June 2005.

[38] World Summit of Internet Society, *Tunis Agenda for the Information Society*, 18 November 2005.

[39] C.A. Afonso, *The Future of the IGF*, in W. Kleinwächter, M. Kettemann, M. Senges, K. Mosene (eds.), "Towards a Global Framework for Cyber Peace and Digital Cooperation: an agenda for the 2020s", Internet Governance Forum Berlin, 2019, p. 113-114.

[40] World Summit of Internet Society, *Declaration of Principles. Building the Information Society: a global challenge in the new Millennium*, 12 December 2003.

[41] *Ibidem*.

[42] UNESCO, *TIC para o desenvolvimento sustentável. Recomendações de políticas públicas que garantem direitos*, Policy paper, 2019.

[43] M. Oghia, *Interconnected Sustainability on the Agenda*, in "Branch", n. 1, Autumn 2020.

[44] United Nations - General Assembly, Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, 29 June 2012.

[45] Comitê Gestor da Internet no Brasil, *Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros – TIC Domicílios 2020*, CGI.br, 2021.

[46] *Ibidem*.

[47] Alliance for Affordable Internet (A4AI), *Meaningful connectivity: A new standart to raise the bar for Internet access*, 2020.

[48] *Ibidem*.

* * *

The role of multistakeholder governance of the Internet in expanding connectivity in Brazil

Abstract: Information and communication technologies have been effecting profound transformations in our society. Two of the main agents of these changes include the process of digital transformation that governments, organizations, and individuals have been undergoing, and the consolidation of Internet use and adoption as critical infrastructure for social, economic, political, and cultural processes. In this context, Internet governance gains increasingly more space in the public debate because of its relevance to digital inclusion and development. The present article discusses the role of multistakeholder governance of the Internet in expanding connectivity in Brazil from a historical perspective of the events behind the development of the Internet in the country. The model of governance implemented by the Brazilian Internet Steering Committee (CGI.br) and its operational branch, the Brazilian Network Information Center (NIC.br), is a model that has effectively contributed to creating public policies for the digital inclusion of people and organizations in the direction of universal and significant connectivity. Thus, the Internet governance mechanisms established in a country can favor decision making, through the consensus of the government, enterprises, civil society organizations, and the academic community, to ensure increased connectivity.

Keywords: Internet governance – Brazilian Internet Steering Committee – Digital transformation – Information society – Connectivity and digital inclusion

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0080

Contratto sociale e *grundnorm* al tempo degli unicorni

Gian Luca Conti

Questo contributo mira ad offrire un punto di partenza alla comprensione del funzionamento delle istituzioni della rete e delle modalità con cui producono i loro standard, ma anche a cercare di definire la rilevanza costituzionale delle grandi piattaforme della rete, e, infine, a cominciare a partecipare alla riflessione sui profondi mutamenti di paradigma introdotti dall'intelligenza artificiale e dall'articolato mondo degli smart contract.

Infosfera – Standard – Neutralità della rete – Contratto sociale

Sommario: *1. La dimensione costituzionale della infosfera è il contratto sociale – 2. Il processo di formazione degli standard: la realtà della* grundnorm *– 3. Neutralità della rete e contratto per la rete – 4. Verso un nuovo tipo di contratto sociale – 5. Il contratto sociale al tempo dell'asimmetria informativa strutturale*

1. La dimensione costituzionale della infosfera è il contratto sociale

Per queste righe, lo scopo (minimo) del diritto costituzionale è la circoscrizione[1] del potere attraverso norme e procedimenti capaci di razionalizzarlo e di limitarlo salvaguardando i diritti fondamentali delle persone[2], magari agganciandolo alla speranza di una volontà generale.

La rete, intesa come infosfera, può essere considerata come «lo spazio semantico costituito dalla totalità dei documenti, degli agenti e delle loro operazioni»[3]. Il potere nella rete è la capacità di definire le relazioni fra coloro che frequentano questo spazio semantico e che, sempre più spesso, lo abitano[4].

Negli ultimi anni, la rete ha visto il consolidamento di pochi operatori che hanno saputo catturare alcune interrelazioni fondamentali fra i singoli utenti della rete e la rete stessa, costruendovi il proprio mercato[5].

Le interazioni che questi grandi operatori consentono determinano lo sviluppo della rete e, nello stesso tempo, la governano, ma hanno anche a che fare con alcune libertà fondamentali dei loro utenti: la libertà di informazione e, in senso molto più ampio, quella libertà personale che consiste del diritto a formare liberamente la propria personalità[6]; la libertà di corrispondenza; la libertà di circolazione; le libertà economiche che utilizzano la rete per l'esercizio del diritto di creare valore e di metterlo a frutto; la libertà di associazione e così via fino a comprendere probabilmente l'intero spettro delle aspettative costituzionalmente rilevanti degli individui e delle formazioni sociali che gli stessi possono comporre.

Il consolidamento dei grandi operatori e la concentrazione di vasti settori della rete nelle loro mani pone, perciò, un forte problema di diritto costituzionale: è possibile assicurare il pieno diritto di ciascun individuo allo sviluppo della propria personalità evitando che coloro che controllano gli spazi in cui la personalità dei cittadini della infosfera si manifesta possa approfittare del proprio potere?

Il diritto costituzionale, sinora, ha sempre visto la rete come un settore in profonda evoluzione, sebbene

G.L Conti è professore ordinario di Diritto costituzionale all'Università di Pisa.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

– per taluni – votato al medioevo digitale[7], ha perfino cercato di regolare la rete attraverso modifiche al testo della Costituzione formale[8], ma nella realtà ha fatto molto poco, si è limitato a considerare la rete come uno spazio destinato a recepire la forza dei valori costituzionali per come gli stessi esistono indipendentemente dalla rete.

È un punto importante: la Costituzione, probabilmente, non può conoscere un regime specifico dei diritti e delle libertà con riferimento alla rete: il diritto al pieno sviluppo della propria personalità non può essere diverso a seconda che lo si consideri nel prisma della rete o della vita offline[9].

L'ordinamento giuridico sembra considerare la rete come, a suo tempo, la pace di Utrecht ha trattato la questione delle acque territoriali nel 1713 fissando in tre miglia nautiche il limite della sovranità degli Stati nazionali avuto riguardo alla gittata dei cannoni allora in uso. Gli ordinamenti giuridici hanno trovato diversi punti di contatto con la rete: il diritto di autore, ad esempio, ha contribuito a modellare la rete in diversi aspetti, così la libertà di stampa per la dottrina del *safe harbour*, su cui si avrà modo di tornare, o per la problematica delle fake news. Soprattutto la privacy[10], intesa come diritto alla autodeterminazione informativa, rappresenta la manifestazione più evidente di questo tipo di approccio. Manca tuttavia un approccio complessivo alla rete e, forse ma anche probabilmente, non è opportuno.

Le istituzioni della rete, infatti, hanno dimostrato (e stanno dimostrando) una notevole capacità di regolazione e di influenza unita a una certa sensibilità costituzionale. Sanno di essere le *commodities* delle libertà costituzionali dei loro utenti.

Solo che non è un modo di regolare né un linguaggio che parla direttamente agli studiosi del diritto costituzionale: le istituzioni della rete hanno come missione quella di consentire al codice di correre e alla rete di funzionare e, nello stesso tempo, lo sviluppo della rete dipende sempre più da soggetti che hanno come scopo la massimizzazione del proprio valore[11].

Solo le istituzioni del mondo reale possono, in qualche modo, intervenire per regolare efficacemente le piattaforme che si stanno consolidando[12] e dal cui operare con responsabile mitezza e autentico spirito laico dipende sempre di più la capacità degli individui di maturare una propria personalità?

L'obiettivo di queste pagine è di offrire un punto di partenza alla comprensione del funzionamento delle istituzioni della rete, essenzialmente la Internet Engineering Task Force, la Internet Society, la Internet Assigned Numbers Authority, la Internet Corporation for Assigned Name and Numbers, il 3WConsortium, e delle modalità con cui producono i loro standard, ma anche cercare di definire la rilevanza costituzionale delle grandi piattaforme della rete, come Google, Facebook, Twitter etc. e, infine, cominciare a partecipare alla riflessione sui profondi mutamenti di paradigma introdotti dall'intelligenza artificiale piuttosto che dall'articolato mondo degli smart contract.

L'idea di fondo è che solo la democrazia della rete, quel complesso insieme di istituzioni che elaborano standard e protocolli attraverso dei processi di sintesi politica capaci di promuovere il consenso all'interno della stessa rete, una democrazia minima perché fa a meno del concetto di rappresentanza, possa costruire dei limiti al potere delle grandi piattaforme, anche se questo processo è appena all'inizio e non vi è alcuna certezza sulla sua capacità di giungere a compimento[13]. Nello stesso tempo, queste pagine sono convinte che lo spazio a disposizione della sovranità per regolare la rete delle grandi piattaforme sia molto ridotto e, comunque, non distribuito equamente. Le grandi piattaforme si fanno un baffo degli editti provenienti dagli Stati anche quando questi sono accompagnati da multe di straordinaria gravità. In questa situazione in cui le istituzioni della rete tendono a occuparsi solo di codice e le istituzioni della sovranità hanno iniziato il confronto con la rete quando questa era già diventata uno spazio riservato a pochi soggetti in grado di competere con gli Stati nazionali quanto a fatturato e irraggiungibili per la difficoltà strutturale degli Stati contemporanei a comprendere il funzionamento di un ecosistema straordinariamente complesso, il diritto costituzionale appare dover fronteggiare una sconfitta. Non è così se si torna a riflettere sulle categorie fondamentali: in rete, il contratto sociale è una cosa viva, tutt'altro che un espediente retorico e la chiave del contratto sociale è lo strumento per scardinare l'anomia delle grandi piattaforme, le quali sanno benissimo di godere di una situazione di diseguaglianza ma sanno anche che le diseguaglianze per poter durare hanno bisogno di essere giustificate dinanzi a coloro che ne subiscono gli effetti.

2. Il processo di formazione degli standard: la realtà della *grundnorm*

Nel processo di formazione degli standard, la funzione normativa è esercitata al di fuori di qualsiasi condizionamento che non sia deciso su base volontaria all'interno del processo di formazione degli standard stessi. In questo procedimento, la dimensione costituzionale è *octroyée* perché se vi è qualcosa di simile a una costituzione (verrebbe da dire a uno "statuto" nel senso ottocentesco dell'espressione), questo qualcosa è volontariamente concesso dal sovrano ai suoi sud-

diti e non è il punto di arrivo né di una negoziazione, sul modello della monarchia parlamentare, né dell'esercizio della funzione costituente da parte di un popolo, né tantomeno di una revisione costituzionale.

Non è qui che la rete ha iniziato a cercare di costruire una propria identità costituzionale, se così si può dire. Questo è accaduto nel momento in cui si è cominciato a pensare alla infosfera, e più precisamente al potere di stabilire le relazioni fra i diversi contenuti della infosfera e i suoi abitanti, come a un problema costituzionale in senso proprio.

Però è qui che la dimensione costituzionale della rete (non la sua identità costituzionale) comincia a definirsi. Difatti, se ci si chiede quale è la norma che definisce la validità delle norme che vanno a comporre l'ordinamento giuridico della rete, secondo un modello astratto e strettamente gerarchico di ordinamento, che è tipico della scuola formale del diritto[14], questa norma esiste ed è il protocollo TCP/IP, ovvero il protocollo fondamentale che consente a due macchine di comunicare fra di loro.

La scuola della dottrina pura del diritto si fonda letteralmente su di una ipotesi posta come palese finzione: nessuno ha mai pensato che la *grundnorm* kelseniana esista nella realtà, essa costituisce semplicemente la finzione sulla cui base è possibile costruire un sistema estremamente complesso che spiega la propria complessità a partire da questa illusione ideale.

Nella rete, è possibile sostenere che la *grundnorm* esista effettivamente perché la rete è un ordinamento giuridico che si sviluppa a partire da una serie di codici ciascuno dei quali può funzionare solo perché viene riconosciuto dal livello precedente: il mio browser legge la pagina sulla quale riascolto le mie lezioni perché è capace di leggere la programmazione HTML ma la programmazione HTML non servirebbe a niente senza la trasmissione di pacchetti che si basano per non perdersi sul protocollo TCP/IP. L'esempio potrebbe essere sviluppato ulteriormente, ma è sufficiente per consentire di immaginare qualsiasi norma sulla rete come una norma tecnica che definisce un protocollo che può funzionare solo perché viene riconosciuto dal protocollo precedente su cui si fonda, secondo uno schema che può ricordare una cipolla piuttosto che la scala di Merkl, evocata dal principio della *stufenbau*.

Il primo scalino di questa scala, piuttosto che il cuore di questa cipolla, è il protocollo TCP/IP: ogni oggetto sulla rete è contraddistinto da un numero e questo numero consente di identificare solo quell'oggetto, rendendo possibile la trasmissione fra due indirizzi IP.

Ovviamente un concetto di Costituzione di questo tipo è deludente perché manca completamente di valori: dal punto di vista della costruzione scalare dell'ordinamento giuridico non cambia molto se si è in una monarchia assoluta o in una postdemocrazia ordoliberale. Dal punto di vista della *grundnorm*, Repubblica Federale Tedesca e Terzo Reich si assomigliano molto, le formule «bisogna obbedire al Führerprinzip» e «bisogna obbedire al Grundgesetz di Bonn» sono perfettamente equivalenti.

Quello che è importante cercare, perciò, sono i valori che consentono di costruire una comunità attraverso la razionalizzazione della sovranità: si tratta di capire come il potere possa trovare la propria forma per mezzo di un indirizzo politico che si derivi direttamente dalla ricostruzione maggioritaria di un insieme di principi unanimemente e fondativamente riconosciuti come propri da una determinata comunità[15].

Mentre nella rete è possibile trovare ciò che nel mondo reale è impossibile da rintracciare empiricamente perché qui esiste la *grundnorm*, al contrario, quando ci si pone il problema di quali siano i valori costituzionali che trovano nella rete composizione attraverso il principio maggioritario, ciò che nel mondo reale è assolutamente evidente e posto addirittura nero su bianco nelle costituzioni scritte nella rete non può essere facilmente rintracciato.

La rete, in sostanza, si presenta come una Costituzione in senso unicamente formale, perché il codice conosce naturalmente la *grundnorm* ma un tanto pone una questione radicale circa l'esistenza, ma anche la possibilità e comunque l'opportunità, della definizione dei valori che consentano di stabilire se il codice è stato utilizzato correttamente, ovvero la questione della possibilità di elaborare una Costituzione per la rete che vada oltre il codice e che definisca i limiti del codice.

Si tratta di una domanda che non ha allo stato una risposta normativa. Esistono diversi tentativi di consolidare sul piano costituzionale i temi che il codice apre nel tessuto molle del diritto e della politica ma anche della società. Ma soprattutto esiste l'urgenza di addivenire a una definizione di questi temi: sino a che il codice era un programma di posta elettronica, piuttosto che un browser, un motore di ricerca, un social network, una app di messaggistica istantanea, in fondo, la rete aumentava la possibilità di usufruire del mondo reale ma non determinava alcuna soluzione di continuità nella sua percezione.

Adesso che la rete degli smart contract e dei *non-fungible token* è ridefinizione delle stesse idee di proprietà[16] e di autonomia negoziale, che la rete della intelligenza artificiale pone il tema della responsabilità giuridica di un soggetto che è capace di program-

mare se stesso, questa questione diventa centrale e probabilmente non più eludibile, per quanto vaga e complessa da indagare.

L'impostazione tradizionale del problema dipende dalla soluzione di una questione antica quanto le prime riflessioni sulla rete quando ci si chiedeva nei forum se chi abbandonava una conversazione dovesse salutare dicendo "Hello" e quindi rivolgersi agli umani collegati attraverso i loro calcolatori o dovesse dire "Quit" usando la stringa di codice che termina un programma. Secondo la prima impostazione, il diritto della rete è un diritto degli umani perché sono gli umani che utilizzano la rete. Nella seconda, invece, il diritto della rete è il codice e il codice dice che cosa devono fare gli umani, i quali possono tutto ciò che è possibile con le macchine e i loro programmi.

Queste due impostazioni si contrappongono fin dall'inizio della storia della rete, in un dialogo che ha visto prevalere a lungo la seconda, mitizzata nel proclama cyberpunk di John Perry Barlow[17], e che, sul piano ordinamentale ha trovato il proprio apparente trionfo nell'emancipazione di Icann fortemente voluta dall'amministrazione Clinton secondo la dottrina del *Digital Tornado*[18], ma si è trattato di un trionfo che ha assunto i caratteri dell'invasione ostile quando ci si è resi conto che i grandi unicorni cannibali basavano la propria forza sulla capacità del codice di trasformarsi in ordinamento giuridico e di consentire agli stessi di definire le regole di comportamento all'interno di formazioni sociali transnazionali e popolate da oltre la metà della popolazione mondiale. È il codice che permette a Facebook di moderare le discussioni al proprio interno, ma anche di promuovere un determinato comportamento o di definire le modalità con cui i suoi utenti possono interagire fra di loro. Il codice, in questo inquietante modo, diventa ordinamento giuridico, forse suo malgrado. Definisce valori, costruisce un indirizzo politico, modella la società.

Completamente al di fuori del principio maggioritario e secondo logiche che si possono definire autoreferenziali ed elitarie[19].

La lacuna di valori che caratterizza l'ordinamento giuridico della rete consente ad alcuni soggetti di muoversi liberamente, ma questi soggetti non vivono in un mondo privo di valori, definiscono loro i valori del mondo che creano attraverso il codice e, in questo modo, influenzano i valori che diventano il patrimonio dei loro utenti: il social media non è solo uno strumento per manifestare il proprio pensiero ma è anche pensiero e lo è in una maniera estremamente pervasiva. Chiunque ha il vizio di scrivere sa che scegliere lo strumento con cui comunicare influenza il pensiero che si comunica: una cosa è una lettera scritta a mano con la stilografica e una cosa completamente diversa è un messaggio di posta elettronica o di messaggistica istantanea. Il social media conforma il modo di manifestare il proprio pensiero e lo stesso pensiero di una moltitudine di utenti. Non è solo il fatto che su Tik Tok ci si esprime per balletti, ma anche che questi balletti devono ricevere consenso da parte degli altri utenti di Tik Tok e per riuscirci hanno bisogno di essere simili, quasi uguali gli uni agli altri e se ballo come gli altri è facile che finisca anche per pensare come gli altri secondo un modello di *peer pressure* assiologica che può essere considerata estremamente pervasiva.

È qui che lavora l'assenza di valori della rete: il codice non conosce valori ma la rete e i suoi operatori, sì. Ma questi valori sono inevitabilmente strutturati sulla base del "Mi piace" e il "Mi piace" è sempre di più un mi piace perché piace anche agli altri[20].

Diventa una strana forma di democrazia, una forma di democrazia che elabora i propri valori dal basso e che non conosce una vera e propria sintesi politica. Non la può conoscere nei termini tipici della comunicazione politica e della dialettica politica ma la conosce solo attraverso le fluide e incerte leggi del marketing o, forse, come si è accennato in nota, attraverso le logiche algoritmiche con cui gli Unicorni gestiscono i conflitti. Per una macchina, capire che cosa è un albero è analizzare le risposte che gli umani danno quando gli si chiede di dimostrare di non essere un robot e così ciò che è giusto è il risultato della somma dei Mi piace che gli umani lasciano, come una bava distratta della loro navigazione.

Tutto questo assume una dimensione impressionante se si tiene conto dei numeri in gioco. Qualcosa che influenza oltre quattro miliardi di esseri umani[21] può essere considerata indifferente per il diritto?

Soprattutto se questo qualcosa, alla fine, funziona in maniera non molto dissimile da Voice of America, quello strumento formidabile di comunicazione politica con cui l'occidente ha ricordato al mondo oltre la cortina quello che accadeva, una narrazione diversa della realtà. Facebook assomiglia a Voice of America, Tik Tok assomiglia a Voice of America, Google, inteso come motore di ricerca, assomiglia a Voice of America, Amazon assomiglia a Voice of America, Netflix assomiglia a Voice of America. Sono tutti dei meccanismi con cui viene narrato un mondo al mondo, con cui il mondo capace di raccontare se stesso si racconta al mondo che non ha la stessa capacità di rappresentarsi[22].

3. Neutralità della rete e contratto per la rete

La neutralità della rete entra in crisi quando la rete diventa il dominio di unicorni cannibali capaci di uniformare assiologicamente la percezione della realtà di miliardi di persone. Google non è neutrale nel momento in cui utilizza la neutralità del codice per selezionare pertinenza e rilevanza nei risultati di una determinata ricerca e lo stesso vale per Amazon quando propone i suoi prodotti, Netflix quando ci chiede che cosa vogliamo vedere alla fine di una serie, Twitter quando modera una conversazione.

La rete può essere considerata ancora privata? Uno spazio occupato da quasi tre miliardi di persone, gli utenti di Facebook, o un motore di ricerca che totalizza l'86,64% delle ricerche in rete[23], Google, possono essere considerati privati? O diventano spazi che hanno anche una dimensione in qualche modo pubblica?

Un primo tentativo di dare una direzione al potere di definire le relazioni fra i contenuti e i soggetti della infosfera è il contratto per la rete proposto da Tim Berners-Lee e che ha trovato nel mese di novembre del 2019 una sua prima formalizzazione[24], senza poi addivenire a un vero e proprio sviluppo in senso ordinamentale.

È evocativo l'uso dell'espressione *Contract for the Web*: non può non ricordare Hobbes, Locke, Rousseau e Kant ma anche Rawls[25]. Non può non evocare una visione contrattualistica della proprietà in cui il potere è l'oggetto di uno scambio che consente la costruzione delle libertà come autonomie. Ma questo contratto è anche qualcosa di più: non è uno strumento per comprendere un fenomeno, non è il modo con cui la sensibile coscienza di Hobbes reagisce agli scenari terribili della guerra dei trent'anni o Rousseau interpreta il clima culturale che diventerà rivoluzione di lì a pochi anni, è il tentativo di creare coscienza e consapevolezza politica, di sviluppare la consapevolezza della necessaria integrazione "contrattuale" fra privati, società e Governi, dove dire privato significa dire cittadino e quindi portatore di libertà individuali, mentre dire società non è solo libertà di iniziativa economica ma soprattutto formazioni sociali generate dalla libertà di iniziativa economica nel suo combinarsi con il codice e, infine, Governi è, forse, prima che Stati: Costituzioni.

L'idea di un contratto per la rete escogitata dalla intelligente consapevolezza di Berners-Lee rivela un bisogno: la rete si è evoluta, è diventata società, una società assai diversa da quelle sinora sviluppate dalla nostra civiltà, quasi uno stadio ulteriore nella ricerca di relazioni che caratterizza l'evoluzione e questo ecosistema è diverso da quello in cui siamo abituati a vivere, è un mondo nuovo, davvero nuovo, che ha bisogno di una nuova fondazione, di sviluppare i valori che consentono alle persone di costruirlo come comunità, e il contratto per la rete ha rappresentato un primo tentativo di razionalizzare questo ecosistema, farlo diventare un artefatto capace di sviluppare la personalità delle persone, di dare a ciascuno ciò di cui ha bisogno per realizzarsi più pienamente.

Non è facile comprendere quanto vi sia di Rawls o di Kant nel contratto per la rete, ma è ragionevole pensare che questo tentativo dialoghi con le intuizioni anarchiche di Barlow: dopo un lungo periodo in cui la rete ha pensato che il codice fosse la sua unica costituzione, una costituzione fondata esclusivamente su una *grundnorm* di natura tecnologica, è arrivato il momento di costruire la rete come un ecosistema fatto di persone che hanno bisogno di razionalizzare e contrattualizzare i valori che giustificano la formazione sociale di cui fanno inevitabilmente parte.

Ed è qui che viene in gioco il contratto per la rete di Berners-Lee. Nove principi che hanno come scopo la giustificazione dell'esistente ma anche la definizione dei vincoli che condizionano lo sviluppo della rete.

4. Verso un nuovo tipo di contratto sociale

Il contratto per la rete nasce in un contesto che è in sé significativo: il 2019 è l'anno in cui esce il report della Internet Society intitolato *Consolidation in the internet economy*[26]. Questo documento evidenzia la preoccupazione per l'affermarsi sulla rete di pochi, grandissimi *player* – gli unicorni cannibali di cui si è parlato e si parlerà spesso – ciascuno dei quali domina un determinato settore di Internet. La questione, apparentemente, riguarda il diritto della concorrenza, ma in realtà è molto più profonda e coinvolge la stessa logica di costruzione delle regole sulla rete e il modo in cui chi definisce le relazioni fra oggetti e soggetti della infosfera interferisce con la formazione del consenso e le dinamiche del potere nel mondo reale.

Come si è detto, nella rete il "mito" della *grundnorm* si manifesta: l'idea per cui una costruzione logica dell'ordinamento giuridico presuppone una norma fondamentale che si colloca al livello empireo dell'aristotelico motore immobile – una condizione logica di validità trascendente – e determina la validità di tutte le norme che ne discendono[27] è nella rete una realtà immanente.

La rete, per questo, ha bisogno di diventare anche un laboratorio in cui le logiche del contratto sociale possono essere analizzate nel loro divenire, anziché essere ipotizzate in un passato a-storico o in via

di astrazione. A ben vedere, nella rete, nel dibattito sulla sua consistenza giuridica, possiamo osservare la dottrina del contratto sociale al lavoro constatando il passaggio dallo stato di natura a nuovi modelli di razionalizzazione e circoscrizione del potere. Nello stato di natura, tutte le macchine possono fare quello che vogliono. Nella dimensione verso cui ci stiamo muovendo le macchine sono collegate tra di loro e si pongono l'una nei confronti dell'altra in termini che sono vincolati da un protocollo che non consente unicamente la comunicazione ma si avvia a porsi il problema di quanto sia ragionevole il collegamento, che cosa ha un senso dirsi: non manca molto a che queste macchine si pongano la domanda fondamentale di due fidanzati, *perché si sta insieme*?

È un laboratorio in cui dialogano diverse visioni lungo il gradiente che conduce da una dimensione pubblica modellata sulla immagine del guardiano notturno a quella più attenta alle politiche di ridistribuzione del reddito e, più in generale, alle dimensioni sociali del diritto. Il primo approccio si rivela nella visione liberale e libertaria del diritto della rete come diritto composto esclusivamente di protocolli tecnici basati sulla loro capacità di funzionare secondo standard di eccellenza: quello che conta è che ogni computer possa dialogare con qualsiasi altro computer, esattamente come in un ordinamento giuridico conta esclusivamente la definizione del diritto di proprietà e la certezza che gli effetti dei contratti siano assicurati per mezzo del processo. Successivamente, però, ci si è chiesti se alla fine tutte le architetture di rete che vengono costruite o le piattaforme che vengono realizzate abbiano un senso, un senso profondo. Assiologicamente profondo.

Il protocollo TCP/IP, come si è detto, è il principio di validità e di efficacia di tutti i protocolli che vengono utilizzati per la programmazione della rete: lo stesso *robustness principle*, su cui non è facile interrompere la riflessione, è, a ben vedere, espressione di una costruzione scalare dell'ordinamento.

La *grundnorm*, come il protocollo TCP/IP, è assolutamente neutrale. La *grundnorm* consente di riconoscere come valida qualsiasi norma che trovi la sua efficacia nella sua presupposizione e non ne vincola il contenuto. Esiste nello stesso identico significato sia nell'ordinamento della Repubblica Federale Tedesca che in quello della Repubblica Democratica Tedesca, se si possono utilizzare questi punti di riferimento come esemplari, portando innanzi una provocazione. Egualmente, il protocollo TCP/IP non condiziona in alcun modo il contenuto dei protocolli che consente di sviluppare né delle manifestazioni del pensiero che consente di rendere pubbliche o comunque accessibili nello spazio semantico della rete.

È la neutralità della rete, una neutralità direttamente interconnessa alla natura del protocollo, che ha a lungo costituito l'idea costituente della rete stessa. Tuttavia con il consolidamento della rete per effetto delle grandi piattaforme la neutralità ha consentito lo sviluppo e l'affermarsi di soggetti potenzialmente autoritari, ciascuno dei quali titolare di una forza di mercato enorme e difficilmente scalabile. Facebook, considerato come strumento di diffusione del pensiero e come spazio semantico autonomo, considerato come una *commodity* per lo sviluppo della personalità dei suoi utenti, è dotato di un potere pressoché assoluto sulle relazioni che si possono instaurare fra i suoi utenti e i contenuti che gli utenti pubblicano, un potere assoluto sulle relazioni che si instaurano fra gli utenti di questa porzione della infosfera, un potere che ambisce a diventare sovranità con la realizzazione del *Metaverse*[28].

Nel momento in cui la infosfera occupata, in termini potenzialmente autoritari da Facebook interessa un intorno di tre miliardi di persone, la neutralità della rete può essere considerata ancora un valore?

È questo il contesto storico in cui Tim Berners-Lee propone il suo contratto per la rete, un contesto che fa immaginare la necessità di abbandonare il mito della neutralità della rete e di contenere il potere delle grandi piattaforme[29].

I protocolli del contratto per la rete non trovano più il loro fondamento puro e archetipico nel *rough consensus* che li ha generati sinora e che li ha sempre voluti come neutrali, ma diventano giustificati per effetto di un contratto, diventano efficaci per effetto di un potere che nasce dal consenso liberamente espresso dai Governi, le Società[30] e i Cittadini, una sorta di contratto sociale, in cui l'eco di Rousseau è una suggestione forte e che vale la pena seguire per un piccolo tratto. Il contratto sociale di Rousseau è un modello di esercizio della sovranità in cui i cittadini accettano una idea di democrazia nella quale il popolo e il sovrano condividono gli stessi interessi[31] e questi ideali rispondono alla domanda che Rousseau si pone a Venezia nel 1744, quando inizia la sua riflessione: «Qual è la natura del governo più adatto a formare il popolo più virtuoso, illuminato e saggio, insomma il migliore nel senso più ampio del termine?»[32]. Nel contratto sociale, ci sono delle parti e queste parti sanno che cosa devono offrirsi reciprocamente per costruire un sinallagma efficace. Soprattutto, il contratto sociale è l'espediente con cui l'intelligenza di Rousseau reagisce allo stato dell'arte di una oligarchia moderatamente illuminata che bandirà i suoi libri e la sua persona e cerca di superarlo, spiega una realtà delle cose che è perfettamente evidente ai suoi interlocutori. Il contratto per la rete segue questo schema e se ne

allontana nello stesso tempo. Per Tim Berners-Lee è impensabile il mito di un'assemblea popolare che formuli e approvi i protocolli della rete o che si imponga alle grandi piattaforme: il codice è una competenza riservata a una oligarchia illuminata che potrebbe perfino assomigliare al *petit conseil* ginevrino di metà Settecento. Ma il codice può essere considerato giusto se serve effettivamente a costruire una società più giusta[33], senza rispondere alla domanda come si definisce ciò che è giusto? Attraverso il contratto la rete va molto oltre la definizione della propria architettura e degli standard che consentono le relazioni all'interno della infosfera perché definisce in positivo i valori politici che giustificano la costruzione di un discorso giuridico[34].

Si tratta di un approccio nel quale la nozione di contratto sociale e quindi l'idea di costruzione di una società libera perché consapevole del prezzo della rappresentanza è fuorviante e diventa, invece, centrale il movimento verso la rete: Governi, Società e Cittadini si pongono degli obiettivi che hanno come scopo quello di consentire l'affermazione di una Internet più giusta e leale.

Si tratta di un mandato, se si vuole dare un nome a questo contratto. È il mandato che definisce le condizioni alle quali Governi, Società e Cittadini considerano ragionevole lasciare che la rete avanzi per effetto della natura onnivora del codice che la programma.

Questo approccio, a ben vedere, può essere considerato anche come molto conservatore: guarda allo spirito dei primi anni della rete, alle logiche di Werbach e del suo report intitolato *Digital Tornado*[35]. I Governi, le Società e i Cittadini si devono impegnare per una rete che sia più libera e che si muova lungo i canoni della fiducia e della inclusione. Ma fra le parti del contratto mancano la Internet Society e la Internet Engineering Task Force, ovvero i soggetti che più di tutti gli altri guidano lo sviluppo della rete. La ragione di questa lacuna è ambigua: da una parte, il contratto sociale è un contratto per l'indipendenza della rete da coloro che ne potrebbero turbare lo sviluppo. Per questo, si è citato Werbach ma si sarebbe potuto citare John Perry Barlow, che ne costituiva la traslitterazione poetica e scamiciata.

In questa chiave, la logica del contratto per la rete è qualcosa di compreso fra il dono e l'atto di fede: mi impegno a sostenere un terzo che, però, non partecipa al mio negozio giuridico. Ovviamente sia il contratto sociale della filosofia politica che il contratto per la rete di Berners-Lee sono provocanti finzioni, ma mentre la prima è stata una invenzione brillante, la seconda, forse, è andata troppo avanti. Dall'altra parte, l'assenza delle istituzioni più antiche e nobili della democrazia della rete si può anche semplicemente spiegare per la loro riluttanza a un accordo che, in realtà, non dialoga con il potenziale autoritario delle piattaforme.

5. Il contratto sociale al tempo della asimmetria informativa strutturale

Il contratto per la rete è stato sicuramente un passaggio importante ed è difficile capire se il suo mancato affermarsi (perlomeno sinora e con la precisazione che ha avuto comunque una discreta risonanza) sia dipeso dalla mancata adesione della parte più pura della rete o dalla sua costruzione logica che lasciava intravedere la libertà della rete e dei suoi regolatori ma che faceva anche temere la prepotenza degli unicorni.

Il tornado digitale non è stato un vento buono per tutti. I tornado lasciano sopravvivere solo i più forti, quelli che hanno a bordo i migliori equipaggi e i capitani più coraggiosi, quelli che hanno davvero saputo attrezzare le loro imbarcazioni. Nel tornado digitale, la rete non disciplina se stessa senza che i suoi attori principali, i grandi unicorni cannibali che la dominano, società che hanno un fatturato paragonabile al prodotto interno lordo di democrazie avanzate, dimostrino la loro incredibile capacità di influenzarne le regole anche costituzionali di funzionamento.

Di qui, la necessità che gli Stati, gli stanchi Stati che formano la loro volontà secondo schemi logorati dal tempo e costantemente in crisi, democrazie decomposte[36], intervengano sulla rete, portino nella rete il retaggio dei valori di cui sono portatori, valori intrisi del sangue della storia e che hanno un senso perché cercano di costruire un dialogo, di essere la piattaforma che consente a cittadini consapevoli e miti di dialogare e cooperare per una democrazia più consapevole e attenta ai bisogni del futuro.

La rete ha bisogno di una costituzione, di un contratto sociale, perché è sempre più rischiosamente vicina alla democrazia: i referendum nella democrazia italiana hanno rischiato di resuscitare dopo un lungo sonno, di ritrovare lo spirito della democrazia diretta che era al fondamento delle ipotesi di ristrutturazione costituzionale agitate all'inizio della diciottesima Legislatura repubblicana, solo perché la raccolta delle firme è diventata possibile anche per via digitale e subito costituzionalisti di lunga vaglia hanno protestato, hanno chiesto di limitare la deriva referendaria senza interrogarsi sulle sue potenzialità, sulla importanza di consentire al popolo di ritrovare ragioni che giustifichino la partecipazione politica. La rete può essere uno strumento per questo senza bisogno di avvicinarsi ai miti che hanno caratterizzato

un movimento forse non all'altezza delle speranze dei suoi elettori.

Tuttavia la rete è anche un insieme di tecniche formidabili per manipolare il consenso. Il valore economico del *programmatic advertising* è la sua capacità di guidare le abitudini dei consumatori. Piattaforme come Amazon hanno sviluppato un know how assai efficace per vendere un prodotto piuttosto che un altro. Sinora gli unicorni cannibali non sono stati molto interessati alla politica. Se ne sono tenuti lontani: è più conveniente sviluppare le proprie abilità per vendere viti, dadi e bulloni agli artigiani piuttosto che per promuovere un senatore della Repubblica o, persino, un Presidente degli Stati Uniti. Ma durerà a lungo?

Il vero nodo della questione è che la rete non può essere regolata se non da se stessa ma che gli Stati, nello stesso tempo, non possono non introdurre i valori su cui hanno costruito le proprie democrazie e che, probabilmente, possono condurre a un'idea universale di democrazia all'interno della rete. È troppo pericoloso rinunciarci. Pericoloso per gli Stati che possono facilmente essere divorati dagli unicorni, ma pericoloso anche per gli unicorni perché queste organizzazioni sono nate per il profitto non per disegnare la società e nessun imprenditore ha interesse a perdere di vista il cuore dei propri affari.

La soluzione, come ha evidenziato la dottrina più attenta[37], non può che essere un compromesso, nel quale gli Stati rinunciano alla propria sovranità e ascoltano la voce della rete e, nello stesso tempo, la rete si affida agli Stati per regolare quegli aspetti della propria disciplina che hanno più a che vedere con le libertà e i diritti fondamentali delle persone. È la strada avviata dalla Unione europea con il Digital Market Act e con il Digital Service Act, una strada ancora assai lunga e complessa da seguire ma che allo stato delle cose sembra essere la più ragionevole.

Vi è un *caveat* all'inizio di queste pagine da rivolgere a chi avrà interesse a prenderle in mano e sfogliarle, regolare la rete (e quindi anche raccontare la disciplina della rete) è davvero una impresa molto simile a quella di un Governo italiano che intenda ricorrere al decreto legge per dare forma alle nuvole.

La rete cambia continuamente, cambiano continuamente i mondi che apre o che abbandona dopo averli desertificati. Regolare la rete può, se non si pone molta attenzione ai suoi processi evolutivi, condurre a banditori che urlano i loro proclami dove non ci sono più cittadini ad ascoltarli, perché la rete, l'essenza della rete, è la sua frontiera e le frontiere della rete si muovono in continuazione senza che nessuno possa fermarle, sicché il legislatore somiglierà sempre al King Canute che cercava di fermare le onde del mare per salvare la sua flotta anziché cercare una baia più sicura nella Cornovaglia squassata dai vichinghi degli affannati anni che hanno preceduto il secondo millennio[38].

In questo senso, in questo esatto senso, il contratto per la rete rivela la propria ragion d'essere: regolare la rete non può continuare ad essere il punto di arrivo di un *laissez faire* che pigramente si lascia guidare esclusivamente da protocolli tecnici ma neppure di interventi settoriali che hanno a che vedere con quel determinato aspetto (oggi l'*hate speech* o il predominio delle grandi piattaforme sul piano del diritto della concorrenza) ma deve essere lo svolgimento normativo di un nuovo patto sociale che riguarda i governi, le imprese e i cittadini.

Il contenuto essenziale di questo patto sociale che qualche riga fa si è raccontato come un mandato piuttosto che come un contratto muove da un contesto di asimmetrie e risponde con la voce potente del neocontrattualismo di Rawls: le diseguaglianze sono necessarie ma possono essere giustificate solo se sono poste nell'interesse del più svantaggiato[39].

L'asimmetria nella rete non è immediatamente percepibile come una diseguaglianza. È un'asimmetria più profonda, riguarda, come si è detto, l'essenza dello scambio. In rete, l'essenza dello scambio, il suo sinallagma, non è immediatamente percepibile: noi sappiamo perfettamente che cosa chiediamo a Google o Amazon ma non sappiamo che cosa stiamo consegnando nel momento in cui – ad esempio – accettiamo incondizionatamente tutti i cookies che ci vengono proposti.

Il neocontrattualismo impone che questa inevitabile ignoranza non debba tornare a danno dell'ignorante, che le asimmetrie della rete giochino a favore della parte meno avvantaggiata, più fragile[40].

Le asimmetrie della rete sono inevitabili: pochissimi fra gli utenti della rete sono in grado di comprendere il funzionamento dei servizi di cui fanno uso, e non possono essere mitigate attraverso un dovere di informazione che non corrisponde a un desiderio di apprendere. È una finzione, allo stesso modo in cui se è vero che nessuno comprende le informative dei servizi di investimento, è altrettanto vero che ciascuno di noi quando non riceve un risultato apprezzabile da parte del soggetto al quale ha affidato i propri risparmi solitamente lo cambia. Così nella rete non si può pensare che l'utente medio legga con la dovuta attenzione l'informativa sulla privacy di un sito ma che lo abbandoni e che ripulisca il proprio browser nel caso in cui la presenza di cookies renda la navigazione insoddisfacente.

I valori che la rete sviluppa per giustificarsi e per limitare la propria naturale propensione alla

prepotenza e alla arroganza nascono, quindi, da una asimmetria e si giustificano all'interno di una asimmetria.

Servono per giustificare l'asimmetria stabilendo che la stessa non deve tornare a danno dei cittadini e, forse, neppure degli Stati.

È questo il prisma che consente di interpretare il contratto per la rete che è composto di complessivi nove principi, tre per ciascuno dei soggetti ai quali si rivolge.

I Governi devono assicurare a ciascuno la possibilità di connettersi alla rete. La rete deve essere accessibile in ogni sua parte e in ogni tempo, i diritti dei cittadini alla propria privacy e ai propri dati personali devono essere rispettati. Il fatto che la rete sia accessibile a tutti, in ogni sua parte e in ogni momento significa che le diseguaglianze generate dalla rete devono essere utilizzate per renderla accessibile anche a chi ancora non è connesso, anche a chi non è un valore economico per la rete, e questo ha un senso solo se la rete non è sfruttata dagli Stati come strumento di controllo dei cittadini.

Gli operatori della rete devono rendere la rete nel suo complesso accessibile da parte di ciascuno per un prezzo che possa essere considerato ragionevole ed equo perché tale da non determinare irragionevoli discriminazioni e gli operatori devono lavorare perché gli utenti della rete possano maturare il ragionevole convincimento che la loro privacy sarà sempre rispettata e così l'integrità dei loro dati personali in un ecosistema fondato sulla fiducia da parte dei cittadini nella professionalità degli operatori della rete i quali a loro volta sono impegnati nello sviluppo di tecnologie a servizio della parte migliore degli uomini e delle donne perché in grado di contenerne la parte peggiore. Lo scambio che si realizza sulla rete è uno scambio a favore dell'utente, della parte più svantaggiata, perché in questo scambio l'utente ottiene l'accesso a buon mercato a ciò che gli interessa e la protezione dei suoi diritti fondamentali e quello che interessa l'utente deve essere orientato verso il bene, per quanto vi sia di naïf in questa espressione.

Gli utenti finali della rete, infine, sono i destinatari di tre distinte classi di doveri che materializzano quanto necessario a far sì che gli stessi si possano validamente approfittare della asimmetria di cui sono vittime. Devono essere creativi e collaborare fra di loro: l'accesso alla rete ha un senso se la rete serve per sviluppare la personalità del suo utente e questo avviene solo se l'utente usa la rete per la propria creatività e collabora con gli altri utenti. Devono costruire comunità forti, in grado di sviluppare una forma di discorso civile al loro interno: le relazioni in rete sono relazioni umane e le relazioni umane non hanno senso nell'effimero. Devono combattere per la libertà della rete: posso utilizzare consapevolmente la rete solo se la utilizzo anche come lo spazio di una libertà partigiana, in grado di lottare per credere nella libertà della rete[41]. Ciascuna di queste posizioni è a ben vedere lo strumento per consentire agli utenti di fidarsi della rete e di godere di ciò che gli viene offerto, costruendo una cittadinanza attiva, uno *status positivus*[42], in cui il singolo utente è interessato a fare sì che lo scambio sulla rete vada a suo vantaggio e questo accade perché è un utente attivo e creativo, sicché ha interesse a ricevere delle utilità che in questo non possono che riguardare la sfera della conoscenza o del protagonismo virtuale; la sua esistenza non è isolata da quella degli altri utenti sicché le utilità che riceve possono riguardare la sua capacità di condividere relazioni e di approfondirne il senso. Infine, lotta per la rete e quindi con i suoi Mi piace cerca di comprendere quale sia il "bene" dei singoli signori della rete, che cosa consente alla rete di essere utile al progresso della umanità per un Bezos o per uno Zuckerberg deve essere compreso anche dagli utenti della rete. E in questo non ci può essere una intermediazione censoria da parte dello Stato, nello schema di Berners-Lee.

Il mandato sociale che si è cercato di intravedere nasconde anche una libertà negativa che si può leggere in due modi: da una parte l'individuo deve sempre poter fare a meno della rete e dall'altra parte l'individuo deve poter utilizzare la rete per evadere dagli Stati: la rete è anche la diffusione di un modello guidato dai Mi piace, da una parte, ma anche capace di erodere gli indirizzi politici espressi dalle singole sovranità nazionali. Le sovranità consentendo ai cittadini di accedere alla rete consentono anche di accedere a dei valori alternativi a quelli espressi dal singolo Stato.

Il modello di Berners-Lee è fondato sulla idea che la libertà nella rete sia la possibilità di essere proprietari dei dati che ci riguardano. Questi dati non possono essere oggetto di un'aggressione da parte dello Stato, lo Stato consente l'accesso, ma non può utilizzare l'accesso per sorvegliare i cittadini. Questi dati, però, per il singolo utente della rete, esprimono una ricchezza latente, il singolo cittadino non è in grado di valorizzarli: li trasferisce perché per lui non hanno nessun valore positivo. È una proprietà che non ha una vera funzione sociale, esiste solo in una economia molto più grande di quella in cui opera il singolo titolare dei dati. Si ha nella privacy una scissione fra la proprietà e la funzione sociale: la proprietà è degli individui, la funzione sociale è degli Unicorni, o comunque di operatori professionali.

Nella costruzione del contratto per la rete, il punto di riferimento è una cittadinanza attiva ma anche

consapevolmente passiva: attiva perché interessata allo sviluppo della rete come luogo in cui si può affermare la propria personalità ma anche consapevolmente passiva perché cosciente che lo sviluppo della propria personalità in rete dipende dalla fiducia che si può nutrire in chi ha progettato i servizi che utilizziamo e questo significa che il centro del contratto per la rete è la capacità della rete stessa di essere e diventare un luogo in cui le persone si possono esprimere con fiducia[43]. La privacy è il luogo in cui questo si manifesta con maggiore evidenza: perché l'utente della rete ha un pieno diritto sui propri dati personali, una proprietà assoluta, ma questa proprietà assoluta non è funzionalizzabile nell'interesse della rete senza l'intermediazione della rete, e rispetto a questa intermediazione il singolo utente non può che essere consapevolmente passivo, per quanto possa essere interessato a lottare per l'indipendenza della rete o a costruire comunità forti in cui esprimersi.

La logica dell'ordinamento giuridico si inverte: non è lo Stato che protegge i diritti degli individui, ma la protezione dei diritti dipende dalla consapevolezza (un diritto coattivo nel linguaggio giusnaturalista che si è evocato) degli utenti che aderiscono "combattivamente" a un servizio che è indispensabile per la valorizzazione di una utilità altrimenti latente: se Facebook utilizza i dati dei propri utenti in maniera spregiudicata, il vero rimedio non è una sanzione da parte di uno Stato, quanto piuttosto il danno reputazionale che Facebook subisce e la difficoltà per un utente della rete di fidarsi di Facebook per la costruzione della propria identità nel *Metaverse*.

Alla fine di tutto questo ragionamento, viene da interrogarsi sulla natura della rete: siamo in uno spazio pubblico o in uno spazio privato? Ha un senso interrogarsi su qualcosa di evanescente e virtuale come il diritto costituzionale della rete?

Abbiamo la *grundnorm* davanti agli occhi, siamo nel laboratorio di un contratto/mandato sociale "in action", ma tutto questo avviene nel segreto negoziale del rapporto fra l'utente e la piattaforma o in uno spazio che si apre a una dimensione pubblicamente democratica, pressoché costituzionale?

La risposta merita di essere articolata in maniera apparentemente diversa per la rete di coloro che definiscono i protocolli di rete, le regole che si applicano *erga omnes*: questo spazio è naturalmente pubblico.

Ma altrettanto vale per la rete delle grandi piattaforme perché le grandi piattaforme dialogano direttamente con le libertà individuali di una infinità di esseri umani. Sono le grandi piattaforme, gli Unicorni, che possono addivenire all'obiettivo di giustificare le diseguaglianze nell'interesse dei più oppressi, a materializzare l'essenza del contratto sociale per la rete che è quella di far sì che le asimmetrie siano giustificate nell'interesse di chi è meno consapevole. Sono questi soggetti quelli da cui dipende una corretta funzionalizzazione in senso sociale della altrimenti inerte proprietà dei dati individuali.

Quanto questo tipo di rete possa divenire, per mezzo dell'embrione di contratto sociale che vi si intravede, l'incubatrice di un nuovo modello di Stato sociale dipende dalla capacità dei cittadini e dei governi di interagire fra di loro e con gli operatori professionali della rete e questo, ovviamente, allo stato delle cose, non è affatto facile da prevedere.

Quello che invece si può dire è che la rete non è uno spazio pubblico nel senso proprio del termine, non è una istituzione e non risponde a logiche istituzionali. Lo spazio del disordine in rete non è colmato dalla forza degli apparati e delle burocrazie. È uno spazio meta-pubblico, se così si può dire, perché la valorizzazione e lo sfruttamento della inerte proprietà individuale dei dati personali, ovvero la gran parte del plusvalore generato dagli Unicorni, è ammissibile solo se in cambio vengono offerti dei servizi e delle utilità in grado di pareggiare le asimmetrie fra gli operatori della rete e gli utenti della rete.

Questo nuovo modello di contratto/mandato sociale è, e questa è la conclusione di queste pagine, il necessario punto di partenza per qualsiasi riflessione si ponga l'obiettivo di prendere sul serio la rete sul piano costituzionale.

Note

[1]Nelle diverse stesure del manoscritto che ha condotto a queste pagine, si era ipotizzato che lo scopo minimo del diritto costituzionale fosse la definizione giuridica del potere. Ci si è poi chiesti che cosa accade dopo avere definito, che cosa accade se la definizione non riesce a contenere e si è deciso di utilizzare il lemma *circoscrizione*, con l'idea di rappresentare un'azione geometrica, il tentativo di racchiudere una forma all'interno di un perimetro e di classificare quel perimetro come un poligono e, più precisamente, un poligono di cui si conosce il nome, si sa computare l'area e il perimetro. L'idea che tutte le figure geometriche possano essere circoscritte è molto alchemica: J.E. Cirlot, *Il dizionario dei simboli*, ed. it., La Nave di Teseo, 2021, *ad vocem*. In realtà, il diritto costituzionale degli antichi come dei contemporanei ha la cruda ambizione di incarcerare il potere. Lo è riuscito a fare più o meno bene sposando il vapore dell'illuminismo e penetrando il cemento dell'età contemporanea con i suoi valori universali. Vi riuscirà nel freddo impero del silicio?

[2]È l'impostazione di T.E. Frosini, (T.E. Frosini, *Internet, la libertà e la legge*, in "Diritto pubblico comparato ed europeo", 2015, n. 1, part. IX), per il quale: «la *lotta per il diritto a Internet* si svolge su più piani: sociale, politico e giuridico (per tacere dell'economico), da declinare sotto il prisma della comparazione e avvolgere in unico *fil rouge*, che è quello della riduzione del potere politico statuale che schiude nuovi orizzonti alla libertà individuale, quale libera discussione e critica dei problemi ritenuti comuni, il cui fine è di vagliare le soluzioni alla luce delle conseguenze indesiderate che esse direttamente

o indirettamente implicano. L'ordinamento giuridico, ovvero il diritto vivente, è il risultato effettivo dei comportamenti e dell'incontro spontaneo delle "pretese" di innumerevoli individui, ciascuno dei quali persegue i propri scopi sotto l'usbergo del valore della libertà come fine e l'ordine sociale spontaneo come mezzo». Per un'analisi delle diverse posizioni sulla costituzionalizzazione della rete: M. Santaniello, E. De Blasio, N. Palladino et al., *Mapping the debate on Internet Constitution in the networked public sphere*, in "Comunicazione e politica", 2016, n. 3, p. 327 ss.

[3]Vedi L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina, 2017.

[4]Questo potere può essere incarcerato? Può essere guidato? Può essere costretto all'eteronomia? O è un potere in sé costituzionale, che rispetta unicamente le regole che si dà perché è l'unico capace di definire il proprio modo di essere? La vera questione quando si guarda alla rete nella sua dimensione costituzionale è la trasfigurazione della costruzione scalare dell'ordinamento. Vi è nell'astrazione aristotelica presupposta alla *grundnorm* una ragione pratica evidente: alla fine, il potere esiste, è lo spirito del mondo, lo si può intravedere mentre passa a cavallo. Questo potere può essere definito, circoscritto, incarcerato. Perché se ne conoscono le logiche, si sa come si ciba e a che cosa ambisce. Lo stesso vale per la rete? La rete esiste per effetto di un codice e di un protocollo che oramai possono essere considerati adespoti. Solo chi governa questo codice e questo protocollo può imporre un momento, nel senso fisico dell'espressione, alla rete. La *grundnorm* della rete non è una necessità aristotelica, è *lex informatica*, con tutte le ambiguità che caratterizzano questa nozione, su cui volendo: G.L. Conti, *Lex informatica*, in "Osservatorio delle fonti", 2021, n. 1.

[5]In questi termini, Isoc, *Global Internet Report 2019. Consolidation in the internet economy*, dove fra le altre cose si legge: «From the dominance of Facebook in social messaging, Google in search and Amazon in online shopping, the largest Internet platforms are capturing fundamental human interactions. This dominance, and the finances and reach that accompany it, enable the platforms to extend their influence and reach into new market spaces, from autonomous vehicles, to AI, to cloud services and beyond. This leverage is built on unprecedented network effects, vast troves of user data, business agility, and regulatory freedom that few other companies enjoy».

[6]È lo schema della libertà personale intesa anche come libertà psichica o morale, v., P. Grossi, *Libertà personale, libertà di circolazione e obbligo di residenza dell'imprenditore fallito*, in "Giurisprudenza costituzionale", 1962, p. 205; A. Barbera, *I principi costituzionali della libertà personale*, Giuffrè, 1967, per il quale l'art. 13 avrebbe ad oggetto il libero sviluppo della persona umana e non già una mera tutela contro gli arresti arbitrari, ma soprattutto C. Pinelli, *Diritto di essere se stessi e pieno sviluppo della persona umana*, in "Rivista AIC", 2021, n. 4 (il testo riprende la relazione dell'Autore al Convegno AIC che si è svolto a Napoli nel dicembre 2021).

[7]S. Rodotà, *Il mondo nella rete*, Laterza, 2014, part. p. 67 e, già, G. Azzariti, *Internet e costituzione*, in "Politica del diritto", 2011, n. 3, p. 367 ss. nonché D. D'Andrea, *Oltre la sovranità. Lo spazio politico europeo fra post-modernità e nuovo medioevo*, in "Quaderni fiorentini per la storia del pensiero giuridico moderno", 2002, n. 31, I, part. p. 77 ss. Il tema del medioevo digitale è ben presente alle costruzioni di M. Castells, *The rise of network society*, II ed., Wiley Blackwell, 2011.

[8]In questi termini, il disegno di legge costituzionale A.S. (XV Legislatura) 2485, nel quale si prevedeva l'introduzione di un art. 21 bis nella Costituzione del seguente letterale tenore: *Tutti hanno eguale diritto di accadere alla rete internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale. La legge stabilisce provvedimenti adeguati a prevenire la violazione dei diritti di cui al Titolo I della parte I*. Il disegno di legge è stato assegnato alla prima commissione affari costituzionali che tuttavia non ne ha mai iniziato l'esame. Si possono ricordare, nella XVII Legislatura, alla Camera dei deputati le vicende relative alla Dichiarazione dei diritti di Internet, il cui valore giuridico sta nell'affermazione di alcuni principi, invero piuttosto vaghi, sia quanto al loro tenore che alla loro efficacia e validità, ma chi scrive è piuttosto conservatore per quanto riguarda la dogmatica giuridica. Non è stato molto più fortunato l'art. 34 bis che il disegno di legge costituzionale A.S. (XVII Legislatura) 1561 intendeva introdurre e che avrebbe previsto: «Art. 34-bis. – Tutti hanno eguale diritto di accedere alla rete internet, in modo neutrale, in condizione di parità e con modalità tecnologicamente adeguate. – La Repubblica promuove le condizioni che rendono effettivo l'accesso alla rete internet come luogo ove si svolge la personalità umana, si esercitano i diritti e si adempiono i doveri di solidarietà politica, economica e sociale». In questo caso, però, la trattazione in commissione ha visto sia un certo numero di audizioni informali che l'elaborazione di un testo base attraverso la discussione di diversi emendamenti.

[9]È la impostazione di S. Rodotà, *Una costituzione per internet*, in "Politica del diritto", 2010, n. 3, part. p. 348, per il quale: «Si può dire, anzi, che il riferimento a diritti e libertà fondamentali, nel nuovo contesto identificato dalla rete, esige una rilettura proprio dell'insieme dei diritti elaborato dall'intera modernità costituzionale. Se guardiamo, ad esempio, alla nostra Costituzione, non si può sfuggire ad alcune domande: le "formazioni sociali" (art. 2 della Costituzione) possono essere anche le comunità virtuali create nel cyberspazio? Le garanzie della libertà personale (art. 13) devono essere estese anche al "corpo elettronico" seguendo la traiettoria della rilettura dell'*habeas corpus* come *habeas data*? Regge la distinzione fra dati "esterni" e "interni" delle comunicazioni quando queste si svolgono su Internet, modificando i termini in cui deve parlarsi della loro libertà e segretezza (art. 15), come ha fatto la Corte costituzionale tedesca con una sentenza del 2 marzo 2010? Come si atteggia in rete la libertà di associazione (art. 18)? Il diritto di manifestare liberamente il proprio pensiero (art. 21) deve essere messo in rapporto con il diritto all'anonimato nelle comunicazioni elettroniche? L'accessibilità alla proprietà (art. 42.2) deve tradursi nella libera appropriabili di determinati beni per via elettronica, secondo una logica dei *commons* che tende anche ad escludere l'identificazione personale dei soggetti che accedono?».

[10]D. Poletti, *Vere sfide e falsi miti del GDPR*, in "Nuovo diritto civile", 2019, n. 2, part. p. 43 ss.; Id., *Condizioni di liceità del trattamento dei dati personal*i, in "Giurisprudenza italiana", 2019, c. 2783 ss.

[11]C'è differenza fra un soggetto economico che ricerca la massimizzazione del profitto che può conseguire attraverso la creazione di plusvalore e un soggetto economico che ricerca la massimizzazione del proprio valore che può essere indipendente dalla realizzazione di profitti nell'immediato. Le grandi società della rete hanno fondato il proprio valore sull'intelligenza della rete e delle sue potenzialità di sviluppo piuttosto che sulla immediata realizzazione di ricavi e, per questo, hanno sempre sviluppato una visione politica della rete, in senso ampio.

[12]Le grandi piattaforme, tutte, tendono in primo luogo a consolidarsi estendo via via il loro potere ad altri mercati. Lo schema del Digital Market Act parla esplicitamente di società *entrenched*, espressione che rende davvero l'idea perché fa pensare a una fortezza che occupa una posizione di dominio su una valle sorvegliandone l'accesso. Notoriamente le questioni di antitrust devono essere sempre osservate non tanto sul piano della posizione di mercato che in un certo momento una determinata impresa occupa quanto piuttosto dei mercati

ai quali questa impresa impedisce o condiziona l'accesso. La concentrazione delle grandi piattaforme non rileva tanto per lo spazio di mercato che le grandi piattaforme occupano ma per quelli che condiziona definendone le condizioni di sviluppo. La posizione di Google sul mercato dei motori di ricerca non ha impedito ad altri operatori di entrare nel mercato della pubblicità on line. Ma si può dire che se Google non fosse stato nello stesso tempo il loro formidabile concorrente e fornitore queste imprese sarebbero egualmente profittevoli? Non sono discorsi astratti se si pensa all'impatto dell'antitrust sul futuro della rete e del mercato del software nel caso IBM: una guerra persa (il Vietnam dello Sherman Act), milioni e milioni di dollari sprecati ma che hanno determinato un comportamento da parte di IBM maggiormente attento alle necessità della concorrenza, meno aggressivo, inducendola ad esempio a firmare un accordo di fornitura non in esclusiva per il sistema operativo fornito da un Bill Gates assai giovane. Sul tutto, J.W. Cortada, *IBM. The Rise, the Fall and the Reinvention of a Global Icon*, 2019, MIT University Press.

[13]Il patrimonio genetico del processo di formazione ed elaborazione degli standard non ha molto a che fare con la democrazia e, soprattutto, con la stessa idea di rappresentanza. È il patrimonio di signorie assolute, in cui il fatto che un determinato soggetto sovraintenda una certa funzione (Jon Postel per IANA, Tim Berners-Lee per il W3C) è ciò che assicura la coerenza degli standard che vengono via via elaborati e la loro aderenza alla logica complessiva della rete. Questo modello si fonda sulla neutralità dello standard rispetto ai contenuti di cui consente la diffusione. Gli standard sono lo spazio in cui si tessono infinite connessioni semantiche. Le piattaforme hanno sviluppato spazi ulteriori in cui la programmazione rende semplice alle persone comuni condividere il proprio pensiero. Qui la programmazione non è più neutrale. È lo strumento di una impresa commerciale. Nel punto di incontro fra questi due modelli, vi è la necessità costituzionale della rete, perché il codice smette di essere neutrale e la sua mancanza di neutralità impone di riflettere sulle ragioni che consentono di determinare il senso delle relazioni che si sviluppano nella rete intesa come spazio semantico, secondo la ricostruzione di Floridi.

[14]In questo modello, la validità è validità in un determinato ordinamento giuridico. Allo stesso modo in cui la coscienza è la coscienza di un determinato soggetto. La validità è relativizzata per effetto di metaregole costitutive che ne definiscono le condizioni di validità (*Gültigkeitsbedingungen*), le quali sono disgiuntamente necessarie e congiuntamente sufficienti, di talché una regola può essere considerata valida in un determinato ordinamento giuridico solo se rispetta le regole di validità di quel determinato ordinamento giuridico. La metaregola costitutiva principale è la *Grundnorm*. Per una semplificazione di questi concetti: A.G. Conte, *Condizioni di antinomia*, in "Materiali per una storia della cultura giuridica", 2006, n. 2, part. p. 461 ss., ma vedi anche C. Luzzati, *A che cosa serve la norma di riconoscimento? Un'analisi funzionale*, in "Ragion pratica", 2003, n. 2, p. 449 ss.; R. Guastini, *Gerarchie normative*, in "Materiali per una storia della cultura giuridica", 1997, n. 2, p. 463 ss.

[15]La dottrina dei valori è intuitivamente tirannica: ogni valore porta con sé una visione del mondo che vuole essere univoca nella misura in cui esso per esistere non tollera il bilanciamento con altri valori che ne diminuirebbero l'importanza. Ciascun valore ambisce a essere primario e assoluto e la Costituzione lo riconosce come primario e assoluto perché è primario e assoluto nel momento in cui viene definito. Su tutto questo, anche come punto di partenza per ulteriori sviluppi della ricerca: T. Gazzolo, *"Valore" e "limite" in Carl Schmitt. Per una lettura della "Tirannia dei valori"*, in "Materiali per una storia della cultura giuridica", 2010, n. 2; P. Becchi, *La critica schmittiana alla filosofia dei valori e il dibattito giusfilosofico italiano nell'immediato dopoguerra*, in "Filosofia politica", 2009, n. 2; M. Benini, *Confrontarsi col nemico. Analisi della ricezione del pensiero di Carl Schmitt nella cultura politica anglosassone*, in "Filosofia politica", 2013, n. 2. La funzione di indirizzo politico – oltre lo Stato autoritario – presuppone una Costituzione laica, nella quale convivono diversi valori, tutti egualmente primari e assoluti, i quali trovano un equilibrio grazie alla intermediazione del principio maggioritario, perché nel momento in cui l'unico valore che consente ai valori primari e assoluti di convivere in uno stesso testo contemporaneamente senza generare delle antinomie insuperabili è il principio di eguaglianza per cui nessun cittadino ha in sé il diritto di portare dei valori che siano incompatibili con quelli degli altri cittadini ma tutti i cittadini hanno il diritto di essere portatori di valori reciprocamente incompatibili, secondo uno schema che rammenta molto l'*overlapping consensus* liberale, allora si ha che l'equilibrio fra i valori diventa una questione di cui può essere arbitro unicamente il principio maggioritario e che l'essenza dell'indirizzo politico come strumento per dare senso all'attività dello Stato è l'esatta misura di un determinato punto di equilibrio fra valori reciprocamente incompatibili determinata dal principio maggioritario e dall'an-archia della funzione di governo. In questo caso, possono tornare utili: E. Rossi, *Legitimacy and Consensus in Rawls' Political Liberalism*, in "Iride", 2014, n. 1; A. Pisanò, *Overlapping consensus e diritti umani*, in "Rivista di filosofia del diritto", 2014, n. 2.

[16]Sulla proprietà, è interessante consultare: C. Salvi, *Teologie della proprietà privata. Dai miti delle origini ai nuovi dei della finanza*, Rubbettino, 2017, su cui vedi la *recensione* di L. Nonne, in "Osservatorio del diritto civile e commerciale", 2019, n. 1. Niente come la rete degli smart contract e dei *non-fungible token* determina il definitivo venire meno della semplicità immaginaria alla base della nozione di proprietà che ha caratterizzato il pensiero di Portalis, per come esposto al corpo legislativo: la proprietà non può più essere considerata la conseguenza della natura delle cose. Ma nello stesso tempo, viene anche meno una delle caratteristiche fondamentali della codificazione della proprietà: la sua natura di *instrumentum regni*.

[17]Vedi F. Musella, *Legge, diritti e tecnologie. Approcci a confronto*, in "Politica del diritto", 2010, n. 3, ma anche F. Amoretti, *Il cyberspazio tra Stati, corporation e... pratiche democratiche*, in "Comunicazione politica", 2009, n. 1; A. Tursi, *Cartografare contrade tecno-politiche*, in "Politica & Società", 2018, n. 1; J. Swiatkowska, *Cyberspace as a Domain of Complex and Multilayer Influence. A Case Study of Poland*, *ivi*.

[18]La nozione è stata sviluppata da Werbach in un suo famoso paper, invero rivoluzionario non solo per le idee esposte ma anche per l'esplosiva influenza che ha avuto a livello politico sugli orientamenti dell'amministrazione Clinton: K. Werbach, *Digital Tornado: The Internet and Telecommunications Policy*, FCC, 1997. Su Werbach si tornerà più innanzi, ma già adesso vale la pena ricordare: R. Collins, *Online and legacy media in the UK. Part One. The changing: data & doubts*, in "Economia della Cultura", 2008, n. 4.

[19]Vedi M. Betzu, G. Demuro, *I big data e i rischi per la democrazia rappresentativa*, in "Media laws", 2020, n. 1 ma il tema sarà affrontato più innanzi. Qui per un viatico introduttivo, si può ricordare: M. Boneschi, *Vietato pensare*, in "Psiche", 2021, n. 1.

[20]Sul *Peer Behaviour*, ovvero quel modello di analisi del comportamento sociale in cui si analizzano gli effetti della pressione generata dal comportamento di un leader all'interno di un gruppo di altri soggetti i quali sono naturalmente indotti a fare propri i suoi atteggiamenti, com'è quando tutti gli adolescenti di uno stesso ambiente indossano abiti simili e perciò trovano una loro identità, vedi A. Palmonari, *Autobiography through Adolescence*, in "Psicologia sociale", 2018, n. 1;

C. Mazzanti, *Un nuovo approccio all'inclusione e socializzazione nel gruppo in età prescolare fondato sul modello di Levine e Moreland*, in "Psicologia sociale", 2009, n. 2. Il modello ha assunto una rilevanza normativa con l'introduzione delle *fiscal rules* nel contesto della governance economica della Unione europea: vedi J.P. Fitoussi, F. Saraceno, *Peer Pressure and Fiscal Rules*, in J.P. Fitoussi, J. Le Cacheux, "Report on the State of the European Union", 2010, Palgrave Macmillan. Questo modello si applica molto bene al comportamento in rete, dove la stessa struttura algoritmica dell'analisi comportamentale, del giudizio etico, si presta a modellarsi sui Mi piace e i Mi piace determinano un singolare atteggiarsi del principio maggioritario.

[21] 4,88 miliardi di persone nell'ottobre 2021, che corrispondono al 62% dell'intera popolazione umana. Questo ammontare è impressionante se si tiene conto che nel 2000 gli esseri umani connessi alla rete erano poco più di 400 milioni e che erano 3,66 miliardi nel 2016. La potenza di internet si palesa nella sua capacità di influenzare uniformemente la popolazione mondiale. Greg Woolf (G. Woolf, *Roma. Storia di un impero*, ed. it., Einaudi, 2016) scrive che al tempo dell'Impero Romano una pratica agricola si diffondeva al ritmo di 20 chilometri per generazione. A che velocità si diffondono le nuove pratiche economiche? Quanto impiega la prassi degli NFT nella riproduzione delle opere d'arte per raggiungere tutti i musei del mondo?

[22] M. Price, *Public Diplomacy and Transformation of International Broadcasting*, in "Comparative Media Law Journal", 1 gennaio-giugno 2003, p. 72-73, dove si legge: «International broadcasting is the elegant term for a complex combination of State-sponsored news, information, and entertainment directed at a population outside the sponsoring State's boundaries. It is the use of electronic media by one society to shape the opinion of the people and leaders of another. [...] The Voice of America, Deutsche Welle and the Bbc World Service are the best-known exemplars». È evidente la distanza fra una informazione guidata da uno Stato e funzionale a un suo discorso politico orientato in senso imperiale, con tutte le ambiguità connesse a questa espressione, e lo stesso fenomeno con dei contenuti che hanno come fondamento i Mi piace dei loro utenti.

[23] Questo significa che un intorno di 4,23 miliardi di esseri umani (se l'86,64% delle ricerche avviene su Google, non si può pensare che ogni ricerca sia un utente: ci sono utenti che fanno molte ricerche ma ci sono anche utenti che non ne fanno perché magari usano solo i social, ma non è irragionevole immaginare che fra le due grandezze vi sia un rapporto di proporzionalità) dipende dall'algoritmo di Google per la ricerca delle informazioni di cui ha bisogno o, anche, per soddisfare le proprie curiosità.

[24] Il processo costituente avviato da Berners-Lee ha avuto una grande eco presso i grandi operatori della rete, come si può facilmente vedere nel sito dedicato. Al processo hanno aderito, fra gli altri, il W3Consortium e la World Wide Web Foundation. Non hanno aderito, invece, ISOC e IETF. Significativamente.

[25] Sul contratto sociale, la letteratura è sterminata, una riflessione che vale anche come una prima guida bibliografica in H. Hofmann, *La dottrina classica del contratto sociale e il "neo-contrattualismo"*, in "Filosofia politica", 1997, n. 3.

[26] Lo si trova facilmente sul sito della Internet Society, nella parte dedicata ai cd. Global Internet Report.

[27] Vedi A. Scalone, *Impossibile purezza. Kelsen fra scienza del diritto, politica e scienze umane*, in "Filosofia politica", 2017, n. 2, p. 315 ss., in cui si sostiene che la dottrina pura del diritto di Kelsen è, in realtà, intrisa di una visione laica della lotta politica che è intrinsecamente politica. Qualcosa che fa riflettere: se la laicità della dottrina pura del diritto ha generato l'interpretazione dell'art. 48 della Costituzione di Weimar che ha bruciato il Reichstag nel 1934, la neutralità della rete sta generando gli autoritarismi delle grandi piattaforme sottesi al consolidamento della rete? È il quesito che genera il bisogno di una Costituzione per la rete, che non si può muovere sul piano della *grundnorm*, dove le regole della rete sono neutrali rispetto al contenuto che ospitano o, invece, deve riuscire a permeare di valori esattamente queste regole secondo un fenomeno che si è indagato in G.L. Conti, *Lex informatica*, cit.

[28] Nella lettera con cui Zuckerberg ha illustrato il *metaverse* si legge: «We are at the beginning of the next chapter for the internet, and it's the next chapter for our company too. – In recent decades, technology has given people the power to connect and express ourselves more naturally. When I started Facebook, we mostly typed text on websites. When we got phones with cameras, the internet became more visual and mobile. As connections got faster, video became a richer way to share experiences. We've gone from desktop to web to mobile; from text to photos to video. But this isn't the end of the line. – The next platform will be even more immersive — an embodied internet where you're in the experience, not just looking at it. We call this the metaverse, and it will touch every product we build. – The defining quality of the metaverse will be a feeling of presence — like you are right there with another person or in another place. Feeling truly present with another person is the ultimate dream of social technology. That is why we are focused on building this. – In the metaverse, you'll be able to do almost anything you can imagine — get together with friends and family, work, learn, play, shop, create — as well as completely new experiences that don't really fit how we think about computers or phones today. We made afilm that explores how you might use the metaverse one day. . . ».). Si deve osservare che negli stessi giorni, l'app spotland ha messo on line una piattaforma di realtà virtuale in cui si può diventare proprietari di un determinato spazio virtualmente fisico e la sovranità è prima di tutto la possibilità di definire i confini dello spazio.

[29] Cfr. Contract for the web. La visione su cui si fonda può essere così riassunta: «The Contract for the Web lays out a vision for the web we want and provides a roadmap for the policies and actions we need to get there. It sets standards, rooted in human rights, for the development and implementation of new technologies, and the policies and laws we need to support them. Critically, it calls for people everywhere to join the fight for the web we want, because the best way to change the priorities and actions of those in power is to speak up and demand that change». Il contratto contiene I seguenti principi: «(1) Ensure everyone can connect to the internet; (2) Keep all of the internet available, all of the time; (3) Respect and protect people's fundamental online privacy and data rights; (4) Make the internet affordable and accessible to everyone; (5) Respect and protect people's privacy and personal data to build online trust; (6) Develop technologies that support the best in humanity and challenge the worst; (7) Be creators and collaborators on the web; (8) Build strong communities that respect civil discourse and human dignity; (9) Fight for the web». Nello stesso tempo, il contratto suddivide i diversi principi a seconda del soggetto cui si rivolge, di talché ciascuno di questi principi esprime una precisa opzione assiologica del soggetto che ne è destinatario nei confronti della rete. Questi soggetti sono, in primo luogo, i Governi, intesi come Stati e, perciò, come una sorta di sindacato dei propri cittadini, considerato come il soggetto in grado di rappresentare i propri cittadini nei confronti della rete, ma anche colui che deve garantire a tutti i suoi cittadini il diritto di evadere dalla gabbia statuale per mezzo della rete; le Società, i.e. *Companies*, le imprese che proiettano in rete la propria libertà di iniziativa economica; i

cittadini, i.e. *Citizen*, che svolgono un ruolo di chiusura perché la libertà della rete è l'oggetto di un discorso politico attivo e di "lotta". Su tutto questo, il ragionamento prosegue nella prossima nota. È interessante osservare come ogni principio sia stato elaborato a partire da affermazioni provenienti da Organizzazioni Internazionali e che hanno per oggetto i diritti universali dell'uomo. Queste affermazioni nel contratto per la rete sono state considerate la base su cui elaborare un diritto costituzionale globale della frontiera tecnologica.

[30]Il contratto per la rete parla genericamente di *companies*, forse si sarebbe potuto utilizzare l'espressione, più polemicamente liberal, *corporations*. Ma la vera espressione, quella più corretta a rappresentare la parte del contratto che intende limitare il proprio potere per sopravvivere è *platforms*, perché se si è ben compreso il fenomeno la questione non riguarda le società che occupano la rete per offrire i propri servizi ma quelle che occupano la rete piegando la neutralità delle sue logiche istitutive in senso potenzialmente autoritario. Non si dice che le piattaforme siano autoritarie. Non lo sono nella realtà. Ma non lo sono perché sono guidate da imprenditori illuminati, non perché rispondono a una logica normativa che non ne consente la deviazione in senso autoritario. Lorenzo Il Magnifico è stato il Signore illuminato di una Firenze meravigliosamente civile per merito suo, non per merito delle istituzioni repubblicane fiorentine che avrebbero potuto ospitare e generare un signore assai più sanguinoso e crudele.

[31]Scrive Rousseau: «Vorrei essere nato in un paese dove il sovrano e il popolo potessero avere un solo interesse [...] Sarei voluto nascere sotto un governo democratico saggiamente temperato» (J.J. Rousseau, *Discours sur l'origine de l'inegalité*, in Id., "Oeuvres complètes", a cura di R. Dératé et al., Bibliothéque de la Pléiade, 1966, III, part. pp. 404-406.

[32]J.J. Rousseau, *Confessions*, I, IX, in Id., "Oeuvres complètes", cit., I, part. p. 405.

[33]Con timidezza di nota, vale la pena suggerire che il sinallagma della rete si muove nella oscurità: il sinallagma della rete è lo scambio fra la privacy degli utenti e i benefici che gli utenti ottengono attraverso i servizi che sottoscrivono o semplicemente utilizzano. Questo scambio solo apparentemente è chiaro: perché se il cittadino di Rousseau sa esattamente a quanto ammontano le tasse che deve pagare, qual è la durata del suo servizio militare, quali sono i dazi che le sue merci devono scontare per essere messe in vendita, nessuno degli utenti della rete conosce con la stessa esattezza il valore dei suoi dati per coloro che li utilizzano. Conosce i benefici che ottiene da Whatsapp per usare il suo smartphone come un sistema di messaggistica evoluto o come un telefono vero e proprio senza dover pagare la bolletta del traffico telefonico ma pagando solo il traffico dati, ma non sa quale uso farà Whatsapp dei dati che l'utente gli affida e, perciò, non conosce il valore della privacy alla quale rinuncia. Il contratto per la rete, perciò, non può essere un vero e proprio contratto perché non vi è un contratto quando le parti non conoscono il valore dei beni che si scambiano, al più vi è un negozio giuridico aleatorio e, perciò, è consapevolmente composto di principi, ciascuno dei quali può essere considerato espressione dei valori che animano una visione della rete libera e capace di funzionare come strumento di realizzazione della personalità umana.

[34]È l'impostazione di S. Rodotà, *Una costituzione per internet*, cit., part. p. 351: «proprio riflettendo su Internet possono essere individuate le vie di un costituzionalismo globale possibile, non affidato a una *vertical domestication*, con norme sovrastatuali incorporate nei diritti statuali, né semplicemente translocale. Dunque una costruzione del diritto per espansione, orizzontale, un insieme di ordini giuridici correlati, quasi una costituzione infinita». Molto criticamente G. Azzariti, *Internet e Costituzione*, cit., part. pp. 372-373.

[35]Vedi: K. Werbach (ed.), *After the Digital Tornado: Networks, Algorithms, Humanity*, Cambridge University Press, 2020, dove significativamente in premessa si legge: «Networks powered by algorithms are pervasive. Major contemporary technology trends – Internet of Things, Big Data, Digital Platform Power, Blockchain, and the Algorithmic Society – are manifestations of this phenomenon. The Internet, which once seemed an unambiguous benefit to society, is now the basis for invasions of privacy, massive concentrations of power, and wide-scale manipulation. The algorithmic networked world poses deep questions about power, freedom, fairness, and human agency. The influential 1997 Federal Communications Commission whitepaper Digital Tornado hailed the "endless spiral of connectivity" that would transform society, and today, little remains untouched by digital connectivity. Yet fundamental questions remain unresolved, and even more serious challenges have emerged. This important collection, which offers a reckoning and a foretelling, features leading technology scholars who explain the legal, business, ethical, technical, and public policy challenges of building pervasive networks and algorithms for the benefit of humanity».

[36]Si veda, volendo, G.L. Conti, *La potenza del fato: crisi o decomposizione della democrazia*, in "Consulta online", 2021, n. 3, dove, fra le altre cose, si sostiene: «Democratic backsliding is a commonplace in the contemporary constitutional language. Duly elected governments which are able to reform formal constitutions in a counter democratic way. That is common said about Poland or Hungary and the cause, as common said, is populism. In Italy, or in other Eu countries which can be considered as advanced democracies, if this expression can be used or sounds good, this is not the problem. There is populism but populism is not a problem in Italy, USA or UK and so on. The real problem, in the opinion explained in this essay, is biopolitcs. The Foucault idea for which the power of surveillance is governance by pleasure is the actual power and this power is not in the hands of a government or a State or a democracy, it is in the hands of net corporations, big as a modern State and surely not democratic. So the aim of a constitutional scholar who wants to defend democracy is not a discourse about populism, or the crisis of representation. The real discourse is about the real essence of internet and how we can make available fundamental rights in the code».

[37]C.T. Marsden, *The Regulated End of Internet Law, and the Return to Computer and Information Law?*, in K. Werbach (ed.), "After the Digital Tornado: Networks, Algorithms, Humanity", cit., dove si legge (part. p. 37): «It is often forgotten that the Werbach's 'Digital Tornado' paper heralded a model of limited state regulation, but very substantial responsible collective self-regulation ('consensus and running code') within transnational law. When that pact was broken by 4Chan script kiddies and two billion Facebook users, it moved regulation away from the responsible collectivism of the pioneers' Internet. – There were three views of regulation in 1997: the type of self-regulation I have described; a belief in state regulation by those existing vested interests in broadcast, telecommunications and newspapers; and a third view that state regulation was inevitable as the Internet became ubiquitous but needed to be as reflexive and responsive as could be maintained with human rights responsibilities. – The perspective of today allows us to rethink the apparent triumph of the first view. If 2018 can in retrospect be seen as the year that the 'Tech Bros' view of regulation faltered and was replaced (to some extent) by state and supranational intervention, then the third option, of what I describe as co-regulation, appears to be supplanting that self-regulation option. The state intervention was most notable in both scale and scope in European Union law, for data protection, consumer/prosumer protection, and also for competition enforcement».

[38]S. Brett, *Privacy and injunctions: the law according to King Canute*, in "IP Draughts", 2011, dove si legge, fra le altre cose: «Mr Justice Eady, in a judgment given in April 2008 during the Max Mosley saga, said that "the Court should guard against slipping into playing the role of King Canute" and should avoid "vain gestures". It is trite law that the Courts will only protect information that retains some element of confidentiality».

[39]G. Levi, *Aequitas vs fairness. Reciprocità ed equità fra età moderna ed età contemporanea*, in "Rivista di storia economica", 2003, n. 2; A. Ferrara, *Contrappunti rawlsiani intorno alla società giusta*, in "Parolechiave", 2015, n. 1; I. Salvatore, *Ingiustizia e instabilità sociale. Gli impegni teoretici della giustizia sociale*, in "Rivista di filosofia", 2021, n. 1.

[40]Nessuno sa che cosa succede esattamente quando accetta le informative sui cookies e quindi è ragionevole ipotizzare che questo consenso non sia perfettamente libero ma, al contrario, assolutamente condizionato e comunque viziato da una sorta di incapacità di intendere. Questa incapacità è tanto più evidente nel momento in cui la controparte contrattuale sa benissimo come valorizzare i dati personali che le vengono trasferiti. Non è qui che si deve guardare. Qui, lo scambio è chiaramente inaccettabile. Lo scambio diventa accettabile in funzione di che cosa si riceve. La logica del neocontrattualismo obbliga l'acquirente dei dati ad erogare un servizio in termini soddisfacenti per il loro venditore. Lo scambio funziona solo nella misura in cui può essere considerato a vantaggio della parte più ignorante. Questo soggetto, per un verso, cede dei dati che per lui non sono di vitale importanza. In cambio riceve un servizio che per lui è di quasi vitale importanza. Il rapporto fra ciò che viene trasferito non può andare a detrimento di colui che non ha alternative allo scambio. Tutto questo torna a vantaggio della collettività perché consente la valorizzazione di potenzialità (i dati personali) che altrimenti resterebbero inespresse. Sulla proprietà e la funzione sociale, fra i tantissimi, F. Macario, *Aspetti giuridici e forme di tutela della proprietà collettiva tra categorie del passato ed esigenze attuali*, in "Archivio giuridico Scialoja-Bolla", 2012, p. 30 ss.; Id., *Sub art. 832 – Contenuto del diritto*, in A. Jannarelli, F. Macario (a cura di), "Della Proprietà", vol. I, "Commentario del codice civile", dir. da E. Gabrielli, Milano, 2012, p. 367; M. Comporti, *Relazione introduttiva*, in Id. (a cura di), "La proprietà nella Carta europea dei diritti fondamentali", Giuffrè, 2005, p. 5; A. Federico, *La proprietà tra «funzione sociale» ed «interesse generale»*, in G. D'Amico (ed.), "Proprietà e diritto europeo", ESI, 2013, p. 138. Per una impostazione generale di questi temi: C. Castronovo, *Eclissi del diritto civile*, Giuffrè, 2015.

[41]Il richiamo a una concezione illuminista del diritto di resistenza è davvero evidente. Fra i diritti naturali, i diritti coattivi, uno spazio essenziale è riservato al diritto insopprimibile di ribellarsi al sovrano quando questi fa mostra di non avere a cuore i propri sudditi: L. Scuccimarra, *Obbedienza, resistenza, ribellione. Kant e il problema dell'obbligo politico*, Jouvence, 1998. Sul tema, evidentemente, il richiamo essenziale è a Feuerbach: P.J.A. Feuerbach, *Anti-Hobbes, oder über die Grenzen der höchsten Gewalt und das Zwangsrecht der Buerger gegen den Oberherrn*, Erfurt: 1798, rist. Darmstadt, 1967, trad. it. *Anti-Hobbes, ovvero i limiti del potere supremo e il diritto coattivo dei cittadini contro il sovrano*, Giuffrè, 1972. In questa riflessione, l'aspetto principale è che il potere del sovrano è quello che gli deriva dalla legge e dalle lettere, per usare una espressione dell'epoca, e il diritto di resistenza è un diritto teso a salvaguardare l'efficacia delle norme e delle lettere che definiscono i poteri del sovrano. Lo stesso vale nella logica del contratto (o mandato) sociale che si è tentato di definire e tratteggiare. L'utente della rete deve lottare perché la rete sia libera e questo accade quando lotta perché la rete si prenda cura di coloro che la utilizzano senza approfittarsi delle proprie asimmetrie.

[42]Il riferimento è alla lettura di Jellinek fatta da Häberle (P. Häberle, *Una prima lezione di «diritto costituzionale»*, in "Quaderni costituzionali", 2012, n. 1).

[43]Vedi L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in "Politica del diritto", 2017, n. 2; D. Poletti, *Comprendere il Reg. UE 2016/679: un'introduzione*, in D. Poletti, A. Montelero (a cura di), "Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna", Pisa University Press. Il tema della difficoltà di costruire un consenso consapevole perché basato su una informativa effettivamente in grado di sorreggerlo è emerso più volte nel convegno "Nodi virtuali, legami informali: Internet alla ricerca di regole" tenuto presso l'Università di Pisa il 7-8 ottobre 2016 organizzato da Dianora Poletti e nel corso del quale è stato esposto l'intervento della Gatt, Montanari e Caggiano che si è citato sopra.

* * *

Social contract and grundnorm in the age of unicorns

Abstract: This paper aims to offer a starting point to understand how network institutions operate and the ways in which they produce their standards. It also aims to try and define the constitutional relevance of big platforms operating in the network and to begin to contribute to the reflection on the profound paradigm shifts introduced by artificial intelligence and the complex world of smart contracts.

Keywords: Infosphere – Standard – Network neutrality – Social contract

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0055
Articolo sottoposto a peer review

Intelligenza artificiale, big data e nuovi diritti

Agata C. Amato Mangiameli

Il presente è il risultato di vecchie e nuove riorganizzazioni e intuizioni. Mentre si moltiplicano gli studi su algoritmi, reti neurali e intelligenza artificiale, mutano le velocità e si assiste a cambi di paradigma. Con la rivoluzione dei big data, infatti, il paradigma logico-deduttivo cede il passo all'approccio statistico, che tra i vari scopi ha quello fondamentale di elaborare modelli predittivi e selettivi, nel frattempo che raggruppa gli oggetti in classi il più possibile omogenee. Al di là degli indiscutibili vantaggi, legati alla possibilità di processare una gran mole di dati senza un particolare dispendio di tempo e di energie, l'odierno sviluppo tecnico-scientifico solleva molteplici e serie domande. Queste ultime riguardano soprattutto la sfera dei diritti, che si arricchiscono di nuovi contorni e significati, sino al punto di tutelare istanze pressoché inedite. Emblematico è quanto avviene riguardo al diritto alla privacy, che evolve oggi nel diritto di proteggere i dati personali. Proprio quei dati che costituiscono oramai il primo motore dell'economia contemporanea.

Intelligenza artificiale – Algoritmi – Reti neurali – Big data – Protezione dati

Sommario: *Prima Parte – 1. Dai moderni meccanismi... – 2. ...alle moderne intuizioni – 3. ...e al dilemma: intelligenza e/o coscienza artificiale? – Seconda Parte – 4. A partire dalle reti neurali artificiali – 5. Algoritmi e non-neutralità – 6. Intelligenza artificiale e big data – 7. Ci vuole una regola! Una Carta dei diritti 4.0! – 8. Dal Regolamento europeo sul trattamento e la libera circolazione dei dati personali*

Prima parte

1. Dai moderni meccanismi...

La storia delle macchine pensanti è anche la storia di grandi rivolgimenti e riorganizzazioni. Prima ancora che si potesse progettare, costruire e programmare il calcolatore intelligente, per avviare gli studi sull'intelligenza artificiale[1] è stata necessaria la c.d. invenzione della mente[2], in particolare: a) la visione moderna dell'essere umano come entità distinta dal mondo, scandita dalla ri-concettualizzazione della ragione come strumento per l'esame delle parole (Hobbes), delle idee (Locke), delle rappresentazioni (Leibniz); b) l'affermarsi della nuova matematica e la ricerca di regole logiche che vengono espresse mediante il linguaggio, quali le verità di ragione di Leibniz, le leggi del pensiero di Boole, fino al calcolo dei predicati di Frege, Russell e Whitehead; c) lo sviluppo, dapprima, delle macchine da calcolo meccaniche (oltre all'orologio calcolatore di Schickard, la scatola di Pascal e il calcolatore di Leibniz), in seguito, il progetto della macchina alle differenze (di Babbage) e la costruzione del calcolatore differenziale (di Scheutz), sino poi ai calcolatori automatici elettronici[3].

Sono così costruiti meccanismi che riproducono singole funzioni intelligenti, dapprima i semplici regolatori e selettori automatici e poi i diversi dispositivi atti a memorizzare, apprendere, riconoscere forme. Dagli analizzatori differenziali ai sistemi di tabulazione elettronica, dal calcolatore a relè per nu-

A.C. Amato Mangiameli è professore ordinario di Filosofia del diritto, informatica giuridica e biogiuridica presso il Dipartimento di giurisprudenza dell'Università degli Studi di Roma "Tor Vergata".

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

meri complessi ai calcolatori giganti e, inoltre, all'automa degli scacchi, dall'Univac I[4] al Powerbook di Negroponte[5], quel che più rileva è il passaggio dalla semplice automazione «delle primordiali macchine per tabelle alla sua attuale condizione di versatile macchina informatica, [...] la potenza del computer [...] [viene] proiettata sull'ordito già elaborato dalla ricerca operativa e dall'analisi dei sistemi»[6].

Quanto più lo sviluppo scientifico e tecnico avvicina la macchina al pensiero artificiale[7], tanto più l'elaboratore si trasforma da calcolatrice in calcolatore. La prima svolge funzioni aritmetiche, il secondo funzioni logiche di confronto. Nella prima è l'uomo a inserire i dati operandi, a determinare la sequenza delle operazioni, a valutarne il risultato; nel secondo è un'altra macchina, cioè l'unità di governo, che durante lo svolgimento delle operazioni necessarie e grazie alla memoria centrale di volta in volta controlla, archivia, trasforma.

E intanto che si costruiscono dispositivi sempre più raffinati, si attiva un dibattito sull'intelligenza del calcolatore – si pensi al dialogo radiofonico tra il filosofo della scienza Richard Braithwaite, il matematico Max Newman, il neurochirurgo Geoffrey Jefferson e il logico Alan Turing[8] –, e via via si modifica l'immagine che noi abbiamo della macchina: dapprima "conduttore e trasmettitore di *potenza*", ora "trasformatore di *informazione*"[9].

2. ...alle moderne intuizioni

Quella dell'intelligenza artificiale è la storia di grandi intuizioni. Nel saggio *Computing machinery and intelligence*[10], Turing si chiede se sia possibile per ciò che è meccanico manifestare un comportamento intelligente. La risposta è nota: la macchina universale, equivalente logico di una macchina a stati finiti, è equiparabile al cervello e può dunque essere programmata in modo da imitare il funzionamento cerebrale[11]. Ciò che infatti è rilevante, sia del cervello che della macchina universale, è soltanto lo schema logico degli stati discreti, lettura e scrittura. Non è invece rilevante la chimica o la fisica, poiché qualsiasi cosa faccia un cervello, esso lo fa in virtù della sua struttura in quanto sistema logico e non già perché posto nella testa di una persona o perché tessuto spugnoso costituito da un tipo particolare di formazione biologica cellulare. E se questo è vero, se cioè la descrizione dei processi mentali è indipendente dal corpo: «ci proponiamo [...] di vedere cosa possa essere fatto con un "cervello" che sia, più o meno, senza un corpo, provvisto al massimo di organi di vista, parola e udito»[12], allora la struttura logica del cervello può essere rappresentata altrettanto bene in qualche altro elemento, incorporata in qualche altra macchina fisica.

Oltrepassando, per un verso, l'idea secondo cui solo l'intelligenza umana sarebbe capace di trovare metodi per superare gli errori, e per l'altro, l'idea secondo cui l'intelligenza della macchina sarebbe nulla più che un riflesso dell'intelligenza del suo creatore, è aperta la strada per la costruzione di macchine con risorse analoghe a quelle di un operatore umano. In primo luogo, la memoria: deposito di informazioni, alla stregua della carta sulla quale l'operatore umano scrive i suoi calcoli o alla quale si richiama quale libro delle regole. In secondo luogo, l'unità operativa: parte dove sono compiute le varie operazioni singole che un calcolo comporta (e quali siano queste singole operazioni dipende dalle diverse macchine). In terzo luogo, il governo o controllo: nella macchina il libro delle regole dell'operatore umano è sostituito dalla tavola delle istruzioni presente in una parte della memoria. È compito quindi del governo verificare che le istruzioni siano eseguite correttamente e nell'ordine giusto. Va da sé che il libro delle regole, appena accennato, è una comoda immagine, giacché il calcolatore umano si ricorda di ciò che deve fare. E tuttavia, se si vuole che una macchina riproduca in modo fedele il comportamento di un calcolatore umano nello svolgimento di una serie di operazioni, è necessario chiedere all'uomo come andrebbero risolte quelle operazioni e la sua risposta deve essere tradotta nella forma di una tavola di istruzioni. Inserire tavole di istruzioni in una macchina significa dunque programmare una macchina in modo che compia l'operazione x[13].

La macchina di Turing costituisce un sistema formale automatico. In particolare, il sistema formale è come un gioco nel quale i segni (i pezzi, le occorrenze[14]) sono manipolati in accordo con delle regole, al fine di vedere quali configurazioni possono essere ottenute. E come in ogni gioco, bisogna specificare che cosa sono i segni, qual è la posizione iniziale e quali mosse sono permesse in ogni posizione data. Vanno subito notate tre caratteristiche (del gioco o sistema formale): 1) il sistema è interamente auto-contenuto, nel senso che solamente i pezzi con le loro mosse contribuiscono a mutarlo; 2) è perfettamente definito, ovvero non vi sono ambiguità, approssimazioni, casi intermedi, per determinare una certa posizione o la correttezza della mossa; 3) è controllabile entro un lasso finito di tempo, ossia per valutare la validità della mossa in una posizione deve essere verificato solo un numero finito di cose[15]. Il sistema formale automatico, poi, non è altro che un congegno fisico, una macchina, «che manipola automaticamente le occorrenze di un qualche sistema formale in accor-

do con le regole di quel sistema. È come una partita di scacchi che muove e gioca *da sola* [...], o come un sistema assiomatico che scrive le proprie dimostrazioni e teoremi senza nessun aiuto da parte di un matematico»[16].

Pertanto nel costruire un sistema formale automatico è necessario risolvere due problemi di fondo. Da un lato, far sì che il congegno obbedisca alle regole, dall'altro, automatizzare il meccanismo per decidere tra diverse opzioni valide quale mossa eseguire. E la macchina di Turing[17], con un numero illimitato di caselle di memoria, con un numero finito di unità di esecuzione e con un indicatore di unità, fa sì che i due problemi (cioè quello dell'obbedienza alle regole e del controllo) vengano risolti.

3. ...e al dilemma: intelligenza e/o coscienza artificiale?

Non è detto che giocare contro una tale macchina dia la precisa sensazione di stare scontrandosi contro qualcosa di vivo[18], quel che però è certo è che la macchina diventerà sempre più intelligente. L'11 maggio 1997 è una data importante: il calcolatore Ibm Rs/6000, Deep Blue, batte Garry Kasparov, campione del mondo di scacchi. Nel febbraio del 2011 Watson della Ibm batte alcuni campioni nel gioco televisivo Jeopardy e nel 2015-2016 il sistema AlphaGo batte due dei giocatori di dama più forti al mondo; nel gennaio del 2019, i campioni di Starcraft sono stati battuti dall'intelligenza artificiale di DeepMind.

Queste sfide mettono in evidenza gli importanti livelli raggiunti dalle macchine, ormai in grado di gestire simboli e predisporre mosse, così da vincere. Non annullano però la diversità che esiste tra l'esperienza di giocare, attributo tipico dell'essere umano, e lo stesso comportamento intelligente, che l'umano può condividere con diversi programmi e vari sistemi. Nonostante gli sviluppi resta perciò inattuata quella storia della narrativa fantastica e della fantascienza popolata da esseri artificiali dotati di coscienza: Frankenstein di Mary Shelley, i robot di Karel Čapek, Robbie di Isaac Asimov, come pure HAL di Stanley Kubrick che, diverso dagli altri citati, è privo del corpo. Resta inattuata poiché è indubbio che il tema della coscienza è di approccio particolarmente complesso, poteva non suscitare immediato interesse dal punto di vista ingegneristico, anche se ormai si assiste all'affermarsi della disciplina *Artificial Consciousness* (riecheggia l'altra: *Artificial Intelligence*) e al diffondersi di convegni sulla Scienza della coscienza (si pensi alle tante edizioni che hanno luogo a Tucson in Arizona), convegni e centri che riuniscono diversi studiosi con approcci e ragioni differenti (filosofi e scienziati, farmacologi e fisici, neuro-scienziati e neuropsicologi, ecc.).

Di qui l'attenzione per i tanti significati che l'espressione *coscienza* comunica e per i diversi fenomeni che le scienze cognitive tentano di spiegare, dai più o meno semplici (ad esempio, le capacità di integrare le informazioni, di reagire agli stimoli, di controllare i comportamenti) ai più complessi, quale può essere la spiegazione scientifica del perché sentiamo dolore, gioia, angoscia. Si tratta di un interrogativo fondamentale, anche alla luce degli attuali sviluppi tecnici e dei progressi nel campo delle neuroscienze, sempre più attente alla coscienza, ai suoi contenuti e alla sua interazione con l'ambiente. C'è in gioco la grande questione della decisione (libera) che distingue l'essere umano da ogni altro ente, ma che via via sembra poter essere spiegata da considerazioni che sottolineano l'*errore di Cartesio*[19], ovvero la separazione tra la razionalità e la regolazione biologica, tra la decisione e l'emozione.

Quanto accennato ha delle particolari ricadute. L'attenzione verso i processi mentali, prima descritti indipendentemente dal corpo, si rivolge ora a tutte quelle dimensioni che concorrono a prendere le decisioni e a determinare i comportamenti. D'altra parte, come nel caso della macchia nera il nostro cervello integra l'informazione visiva a nostra insaputa e grazie al combinarsi di altri dati[20], le nostre scelte e le nostre azioni dipendono da una serie di circostanze e dai marcatori somatici, esempi questi di «*sentimenti generati a partire dalle emozioni secondarie*. Quelle emozioni e sentimenti *sono stati connessi, tramite l'apprendimento, a previsti esiti futuri di certi scenari*. Quando un marcatore somatico negativo è giustapposto a un particolare esito futuro, la combinazione funziona come un campanello d'allarme; quando invece interviene un marcatore positivo, esso diviene un segnalatore di incentivo»[21].

Se così, una svolta si rende necessaria: gli studi sull'IA devono potere essere integrati da tutte quelle ricerche per meglio comprendere il formarsi della coscienza, ormai oggetto di studio scientifico visto che essa può essere letta come quell'aspetto ausiliare della nostra dotazione biologica di adattamento all'ambiente. Ancora una volta, altro approdo e altra riorganizzazione: non più la mente distinta dal corpo, bensì l'organismo che partecipa dell'esperienza cosciente. Il che vuol dire, dal punto di vista tecnologico, la previsione che si sia in grado di intervenire nei suoi meccanismi e che questi stessi possano essere riprodotti.

Seconda parte

4. A partire dalle reti neurali artificiali

Il presente è il risultato di vecchie e nuove riorganizzazioni e intuizioni. Nel presente gli studi su algoritmi, software, app, si moltiplicano e si rafforzano. Intanto mutano le velocità e si assiste a cambi di paradigma. Pochi anni per fare quel che si è fatto in secoli: è sufficiente qui considerare il tempo trascorso tra la rivoluzione della stampa e quella informatica, tra quest'ultima e la rivoluzione dei big data (cioè dati di varia natura, generati da algoritmi in tempo reale e il cui volume è impressionante). D'altra parte, anche le teorie dei 6-12 gradi di separazione per entrare in relazione sono oggi – nell'era della connessione – sostituite da quella secondo la quale ogni persona sarebbe collegata a qualunque altra grazie a soli 3-4 contatti. Inoltre, nell'era della crescita esponenziale di dati, il paradigma logico-deduttivo cede il passo all'approccio statistico, che tra i vari scopi (ad esempio: fare previsioni, verificare delle ipotesi e suggerirne di nuove, facilitare l'analisi dei dati e ridurre la loro mole) ha quello fondamentale di raggruppare gli oggetti in classi, il più possibile omogenee, e di determinare il numero e le caratteristiche delle classi.

Algoritmi, intelligenza artificiale, big data, tre espressioni-chiave attorno alle quali ruota l'odierno sviluppo tecno-scientifico che prosegue sulla via dell'evoluzione delle reti neurali, avendo come riferimento quelle biologiche, e che utilizza i c.d. algoritmi di apprendimento: ora algoritmi di apprendimento supervisionato (a partire da un insieme di input ai quali corrispondono output noti, la Rete apprende il nesso che li unisce e impara a generalizzare, ossia a calcolare nuove associazioni corrette input-output processando input esterni al *training set*), talaltra di apprendimento non supervisionato (a partire da un insieme di variabili di input, la Rete crea dei cluster rappresentativi per categorizzarle), ora algoritmi di apprendimento per rinforzo (è dall'interazione con l'ambiente che i circuiti neurali imparano ed eseguono una serie di azioni, delle quali quelle che si avvicinano al risultato sono considerate di rinforzo, mentre le altre sono eliminate perché foriere di errore). Le reti neurali artificiali presentano diversi vantaggi, di qui la loro diffusione nei più disparati settori laddove sono richiesti data mining, elaborazione di modelli predittivi e simulativi, classificazione ecc. Con queste, infatti, si possono processare senza particolare dispendio di tempo ed energie grandi moli di dati, si può operare assai spesso in modo corretto nonostante input imprecisi o incompleti, e quando invece sono ben implementate sono in grado di auto-aggiornarsi in presenza di modifiche ambientali. Com'è intuitivo, le reti neurali artificiali presentano pure dei limiti, ad esempio la loro computazione non è analizzabile in modo completo, gli output somministrati non rappresentano assai spesso la soluzione perfetta, non sono idonee per il momento a risolvere determinate categorie di problemi.

Al di là dei vantaggi e dei limiti delle reti neurali artificiali, le tre espressioni chiave ricordate propongono una domanda fondamentale: l'attività svolta dai sempre più sofisticati software può considerarsi neutrale, ovvero, quell'insieme di algoritmi e di big data, entro la cornice di una intelligenza artificiale capace di riconoscere, classificare, ragionare, diagnosticare, agire, può essere ritenuto di per sé in ogni caso obiettivo?[22]

5. Algoritmi e non-neutralità

Gli esseri umani scrivono gli algoritmi, analizzando innanzitutto il problema, descrivendo la specifica funzionale, come pure i passi da eseguire per giungere al risultato, traducendo infine il diagramma di flusso in programma. Ipotesi di partenza, parametri, dati, funzioni di un programma possono essere di volta in volta diversi: non c'è quindi un unico modo di produrre un algoritmo e d'altra parte una variazione anche semplice di un parametro o di un dato conduce a risultati diversi. Alcune volte, poi, l'algoritmo può persino muovere da pregiudizi: basti pensare a quello di Google Photo che ha catalogato sotto il termine "gorilla" l'immagine di due persone di colore, altre volte l'algoritmo serve a raccogliere dati sui (bravi/cattivi) cittadini, come ad esempio il programma Sesame Credit del governo cinese.

In *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia* Cathy O'Neill[23] mette in guardia dall'affidabilità e oggettività degli algoritmi, poiché questi possono esprimere pregiudizi a causa di una programmazione che si presenta sotto il segno della superficialità, possono altresì essere ricondotti a previsioni alquanto singolari (si pensi al software di predizione della criminalità PredPol della polizia di Los Angeles) o essere utili per vere e proprie truffe (si pensi al software che ha consentito alla Volkswagen di alterare le rilevazioni delle emissioni inquinanti).

Oltre a Cathy O'Neill, anche Dominique Cardon[24], Wolfie Christl e Sarah Spiekermann[25], e molti altri ancora mettono in guardia dagli algoritmi. Dietro formule e modelli matematici, dietro diagrammi e procedimenti formali, si celano meccanismi di alterazione dell'informazione e di condizionamento dell'azione. Ad esempio: il successo commerciale può

dipendere dall'ordine con cui Google posiziona i risultati delle ricerche; il like dipende dalla selezione predisposta dagli algoritmi del social network, per cui solo alcuni messaggi possono essere marcati dal "mi piace"; il prezzo di un biglietto aereo dipende dal profilo del viaggiatore ricostruibile attraverso l'uso di un certo dispositivo, l'orario d'accesso, le ricerche già effettuate; l'accesso al prestito e i tassi di rientro dipendono da formule matematiche i cui parametri non sono riconducibili soltanto alla capacità finanziaria; anche il destino politico di un paese, o di più paesi, può dipendere dal software e da chi possiede i dati sugli elettori.

Già questi pochi esempi confermano gli aspetti critici, ovvero: l'asimmetria informativa tra una società che offre un servizio e l'utente, l'assenza di trasparenza relativa ai princìpi e ai parametri alla base del funzionamento dell'algoritmo, la creazione di una sorta di *filter bubble*, così che siano mostrate all'utente soltanto quelle informazioni che l'algoritmo ha calcolato gli possano interessare, o al contrario, che ha ritenuto per varie ragioni di non dovere fornire. Di qui, l'inesistenza di algoritmi neutrali, di algoritmi che si limitano a riflettere la realtà, essi anzi propongono una loro versione fatta dalle formule classificanti, dal peso attribuito ai singoli parametri inseriti, dalle procedure che determinano il risultato. E intanto aumentano in modo esponenziale i dati, ogni soggetto è classificabile e ogni nuovo dispositivo raccoglie dati[26], dal like si risale con margini d'errore minimi al colore della pelle, all'orientamento sessuale, all'appartenenza politica, come pure al quoziente intellettivo, alla religione e a tanto altro ancora, accade così che gli algoritmi generino sempre più messaggi personalizzati e stratagemmi per orientare la condotta.

6. Intelligenza artificiale e big data

Di grande rilievo, in quest'ambito, è l'ormai acquisita capacità di auto-apprendimento delle macchine, grazie all'applicazione delle citate reti neurali artificiali. I computer capaci di apprendere in modo automatico costituiscono la vera grande svolta e con essa evidenziano il possibile rischio di un sistema non controllato, tale da richiedere una sorta di *Algorithm Liberation Front* per rendere trasparenti i criteri decisionali alla base dei diversi strumenti.

L'intelligenza artificiale opera in vario modo, quel che però va innanzitutto sottolineato è l'importanza che essa riveste in tutte quelle attività che richiedono decisioni a partire da enormi quantità di dati. A tal proposito si consideri Google Street View e in particolare l'elaborazione dei dati qui raccolti da parte dei sistemi di IA. Le informazioni ricavabili, anche dal c.d. rumore, sono certo interessanti per lo studio delle città e delle persone che le abitano.

Significativa è stata la ricerca di un team della Stanford University: a partire da più di 50 milioni di immagini su 200 città mappate da Google Street View, immagini elaborate con una tecnica di riconoscimento degli oggetti così da permettere al software di individuare le auto (ben 22 milioni) e di classificarle (secondo la marca, il modello, l'anno), il team è stato in grado di fornire alcune indicazioni demoscopiche. Per la ricerca si è usato un algoritmo a rete neurale *convoluzionale* (*convolutional neural network*, ConvNet) in grado di processare 50 milioni di immagine in due settimane, contro i circa quindici anni dell'intelligenza umana, e con la caratteristica essenziale di ricavare dati reali, poiché in due settimane i 22 milioni di veicoli individuati restano indicativi del patrimonio di veicoli circolanti in quelle città.

Muovendo da questa grande mole di dati, i ricercatori hanno utilizzato queste informazioni al fine di capire le inclinazioni politiche, hanno così osservato come con più pick-up l'area urbana aveva una probabilità dell'82% di votare repubblicano, e invece con più berline c'era l'88% di possibilità che il quartiere votasse democratico. In questo caso, l'algoritmo usato è quello tipico del *machine learning*, e cioè l'analisi della regressione con la quale si stima un'eventuale relazione funzionale tra la variabile dipendente e le variabili indipendenti. Simile tecnica fornisce delle informazioni parecchio accurate, non limitate naturalmente alle foto di auto e alle previsioni di voto, di qui l'importanza di questi nuovi strumenti (in questo caso, la rete neurale in grado di gestire al meglio le immagini) per gli scienziati sociali e per le loro previsioni.

Intelligenza artificiale e big data, ovvero database che raccolgono enormi quantità di informazione di vario tipo (dalle immagini ai video, dai testi all'audio, dai like su Facebook alle transazioni monetarie) e che richiedono l'utilizzo di calcolatori di grande potenza per la raccolta di questi dati eterogenei e sterminati, come pure per l'individuazione di relazioni (collegamenti, connessioni) e per l'estrapolazione di previsioni. Si tratta di una nuova era, nella quale il paradigma dei big data riporterebbe il discorso sul piano dell'oggettività, visto che sarebbero gli stessi dati, senza alcuna pregiudiziale e senza essere condizionati dall'orizzonte di attese dell'osservatore, a dirci del benchmark, del modello, e della correlazione significativa fra un numero tendenzialmente infinito di variabili. Tutto ciò sarebbe reso possibile, oltre che dalla straordinaria potenza di calcolo, dal

tipo di apprendimento che in quanto statistico non richiederebbe una reale comprensione dei fenomeni.

Per il vero, i dati non sono oggettivi e i modelli statistici rappresentano la realtà modificandola, e cioè orientando i comportamenti. Secondo Dominique Cardon[27], le misurazioni statistiche servono a fabbricare il futuro, poiché la società si orienta secondo le informazioni che le sono prospettate. D'altra parte, è da sottolineare come i big data non siano a disposizione di chiunque, bensì di pochi, che detengono e organizzano i dati sulla spinta di interessi commerciali, e che le caratteristiche degli algoritmi in uso (ad esempio, di Google, Facebook, Amazon) restano per lo più ignote[28].

7. Ci vuole una regola! Una Carta dei diritti 4.0!

Tim Berners-Lee, inventore del World Wide Web, ritiene ormai necessaria una Costituzione che protegga l'indipendenza di Internet e i diritti dei suoi utenti. Di qui la campagna *The web we want*, volta a sollecitare la redazione di una carta dei diritti digitale in ciascun paese, dal momento che se non si ha «un Internet libero [...] non possiamo avere un governo libero, una buona democrazia, un buon sistema sanitario, comunità connesse e diversità di culture [...] è ingenuo pensare di poter rimanere a braccia conserte e ottenerlo [...] I nostri diritti vengono violati sempre più da ogni parte e il pericolo è che ci si possa abituare a tutto questo. Per questo voglio usare il 25esimo compleanno perché ci si impegni tutti a riportare nelle nostre mani il Web e a stabilire quale rete vogliamo per i prossimi 25 anni».

Nonostante resti un ottimista[29], Berners-Lee sottolinea in molteplici occasioni come il Web sia ormai popolato da guardiani digitali sempre più potenti, le cui armi sono algoritmi in grado di manipolare le persone e di limitarne la libertà.

«*The system is failing. The way ad revenue works with clickbait is not fulfilling the goal of helping humanity promote truth and democracy. So I am concerned*»[30].

Di qui la richiesta della regolamentazione della pubblicità politica online, così da evitare usi impropri e eticamente non giustificati.

«*We urgently need to close the "internet blind spot" in the regulation of political campaigning*»[31].

Riportare quindi il Web, quale spazio aperto e luogo delle opportunità, lontano da quel che effettivamente lo minaccia, e cioè la perdita di controllo dei dati personali, la diffusione di disinformazione e di fake news, la sinuosa pubblicità politica. La via è in parte obbligata. Si tratta di garantire in senso proprio il consenso informato, che in molti casi manca, specie in quelli in cui, in cambio di contenuti o servizi gratuiti, si cedono dati personali; si tratta inoltre di rendere trasparenti gli algoritmi, così da capire come si formano le informazioni (e le disinformazioni), come si determinano al contempo gli orientamenti degli attori sociali.

L'odierna quantità di dati è realmente abnorme, una raccolta questa che utilizza dispositivi di vario tipo e nei più diversi ambiti: dalla televisione ai telefoni e ai computer, dalle carte di credito alle smart card, dai sensori delle case alle infrastrutture intelligenti delle città. Il flusso è continuo, l'ordine dei byte segna record incredibili, ma quel che lascia per certi versi stupiti è la capacità di usare ogni singola informazione di questa quantità indicibile per analizzare, elaborare, suggerire e orientare modelli di interpretazione e di azione. La rivoluzione big data consiste proprio in ciò: trattare le tante variabili in poco tempo e con poche risorse computazionali, e questo è ovviamente importante in ogni settore. Si pensi per il marketing ai c.d. metodi di raccomandazione (Netflix, Amazon) per indurre all'acquisto di un bene o un servizio, metodi questi che muovono dai dati provenienti dalla navigazione dell'utente (pagine visitate, prodotti ricercati, acquisti) e ne individuano il profilo, lo status, la condizione, l'attendibilità, ecc. Si pensi inoltre per la sfera pubblica alle statistiche di rilevanza penale, che muovono ormai da una enorme quantità di dati e connessioni anche inusuali e che possono essere usate per prevedere il verificarsi dei reati e per dispiegare le forze di polizia. Si pensi ancora al rilievo che i dati hanno in medicina e all'apporto dei big data che, se condivisi, potrebbero ad esempio realizzare sistemi in grado di analizzare e combattere tempestivamente focolai epidemici, ma anche di predirli e prevenirli.

8. Dal Regolamento europeo sul trattamento e la libera circolazione dei dati personali

Diventa allora necessario avere delle regole, una dichiarazione di principi da osservare, al momento della raccolta, della classificazione, dell'analisi, della sintesi dei dati.

Nel 2016 il Parlamento europeo e il Consiglio hanno adottato il regolamento 679 che si applica al trattamento interamente o parzialmente automatizzato di dati personali, come pure al trattamento non automatizzato di dati personali contenuti in archivi o destinati a figurarvi (art. 2). Qui è l'art. 6 a preve-

dere la presenza di almeno una delle seguenti condizioni quale fondamento di liceità del trattamento, e cioè che (a) l'interessato abbia espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; che (b) il trattamento sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; che (c) il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; che (d) il trattamento si renda necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; che (e) il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; che (f) il trattamento sia essenziale per il conseguimento del legittimo interesse del titolare del trattamento o di terzi, ove non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il regolamento prevede innanzitutto una idonea richiesta del consenso, in particolare tale richiesta deve contenere le informazioni relative al titolare del trattamento, agli eventuali destinatari e alle finalità (natura e durata) che ci si propone con la raccolta e l'uso dei dati. Per una raccolta e un uso dei dati improntati alla correttezza e alla trasparenza, la richiesta dovrà inoltre contenere le informazioni circa i diritti dell'interessato di intervenire sull'uso e sul periodo di conservazione dei dati. Pur variando a secondo dell'utilizzo o meno di strumenti elettronici, e a secondo del servizio che si intende offrire, formule e informazioni utilizzate per chiedere il consenso devono essere espresse in modo comprensibile, semplice e chiaro, oltre che distinguibili da altre richieste rivolte all'interessato per ulteriori questioni (art. 7.2). All'idonea richiesta del consenso segue la volontaria accettazione al trattamento dei dati. Il consenso deve, infatti, essere espresso attraverso un atto positivo libero, specifico, inequivocabile e informato, non è ammesso il consenso tacito o presunto, può essere comunicato sia per iscritto o oralmente, sia mediante mezzi elettronici.

Poiché i dati personali rappresentano il cittadino, prima, durante e dopo il trattamento, bisogna in base all'art. 5 che siano osservati i seguenti principi, ovvero: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza"); b) raccolti per finalità determinate, esplicite e legittime, e trattati in maniera che non sia incompatibile con tali finalità ("limitazione della finalità"); c) proposti perché adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati"); d) considerati esatti rispetto alle finalità per le quali vengono trattati e, quindi, corretti se necessario ("esattezza"); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione"); f) trattati in modo da garantire una adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti, e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza"). A questi diversi e importanti principi va aggiunto quello di "responsabilizzazione" del titolare del trattamento, proprio in quanto competente e in grado di comprovare il rispetto dei principi ricordati.

Quanto ai diritti, ai c.d. *diritti tecnologici*, l'interessato ha il diritto (art. 7.3) di revocare il proprio consenso in qualsiasi momento e con la stessa facilità con la quale lo ha prestato. Ciò non pregiudica la liceità del trattamento (basata sul consenso) prima della revoca stessa, e di questo l'interessato deve essere consapevole grazie a idonea informazione. L'interessato ha inoltre il diritto di ottenere dal titolare del trattamento la conferma che sia in corso un trattamento dei propri dati e, in caso positivo, il diritto di accedere (art. 15) ai dati personali e alle diverse informazioni, ovvero il diritto di sapere per quali fini sono stati adoperati i dati, quale categorie di dati sono state utilizzate, a chi sono stati comunicati, il periodo di tempo entro cui i dati saranno conservati (di sicuro o anche presumibile), la logica utilizzata nel processo decisionale automatizzato, e il diritto di proporre reclamo presso l'autorità di controllo. Di qui, la possibilità per l'interessato di esercitare i diritti di rettifica (art. 16), di cancellazione (c.d. "diritto all'oblio" art. 17), di limitazione (art. 18), di portabilità dei dati (art. 20), come pure i diritti di opposizione al trattamento stesso (art. 21) o il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida significativamente sulla sua persona (art. 22). Com'è chiaro, perché siano riconosciuti questi diritti, in modo da controllare sempre le conseguenze del proprio consenso, occorre che il titolare del trattamento fornisca senza ingiustificato ritardo le informazioni richieste. Si configurano così veri e propri doveri (quali quelli di rettificare, di integrare, di limitare, di sospendere, di cancellare, di non trattare) corrispondenti sia ai diritti dell'interessato, sia ai divieti di trattare alcune specifiche categorie di dati personali (art. 9), sia ai più generali obblighi

in capo al titolare e al responsabile del trattamento (artt. 24-31), in modo da garantire un adeguato livello di sicurezza dei dati (artt. 32-34) anche alla luce di valutazioni dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35).

Da ultimo, si aggiunga che il 19 novembre 2021 il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato delle nuove linee guida[32], atte a fornire utili delucidazioni e preziose interpretazioni proprio in ordine al concetto di "trasferimento internazionale di dati personali" e in merito alla relativa disciplina da applicarsi alla luce del GDPR.

Note

[1]Si veda P. McCorduck, *Storia dell'intelligenza artificiale*, (trad. it.), Muzzio, 1987.

[2]L'espressione è di R. Rorty, *La filosofia e lo specchio della natura*, (trad. it.), Bompiani, 1988.

[3]Si vedano: H.H. Goldstine, *Il computer da Pascal a Von Neumann. Le radici americane dell'elaboratore moderno*, (trad. it.), Etas, 1981; V. Pratt, *Macchine pensanti. L'evoluzione dell'intelligenza artificiale*, (trad. it.), il Mulino, 1990.

[4]Si tratta del primo calcolatore elettronico messo in commercio e acquistato nel 1951 dall'ufficio del censo degli Stati Uniti, che rinnovò le tecniche di elaborazione dati e più in particolare automatizzò la produzione di tabelle che avveniva nelle cosiddette *tab rooms*.

[5]N. Negroponte, *Essere digitali*, (trad. it.), Sperling & Kupfer, 1996, p. 1.

[6]Così J. Weizenbaum, *Il potere del computer e la ragione umana. I limiti dell'intelligenza artificiale*, (trad. it.), Gruppo Abele, 1987, p. 48.

[7]E oggi al pensiero *tout court*, a sentire le riflessioni sul futuro di Ray Kurzweil. Grazie ad una crescita esponenziale *esplosiva*, molto presto i supercalcolatori di nuova generazione, e cioè i *cluster* (insiemi di processori a basso costo, uguali a quelli dei comuni PC, collegati tra loro per spartirsi il carico di lavoro), saranno in grado di simulare il funzionamento del cervello e le sue funzioni neuronali di apprendimento. Ed entro qualche decennio, le tecnologie informatiche includeranno tutte le conoscenze e competenze umane, comprese le tecniche di *pattern recognition*, come pure le capacità di risolvere problemi e di rispondere appropriatamente alle emozioni (la cosiddetta intelligenza emotiva, tipica del cervello umano) (R. Kurzweil, *La singolarità è vicina*, (trad. it.), Apogeo, 2008).

[8]Alla BBC il 14 gennaio 1952, pubblicato in "Sistemi intelligenti", aprile 1998.

[9]J. Weizenbaum, *op. cit.*, pp. 54-55.

[10]A.M. Turing, *Computing Machinery and Intelligence*, in "Mind", vol. 59, 1950, n. 236, p. 433-460.

[11]Si veda in particolare A.M. Turing, *Macchine intelligenti*, in Id., *Intelligenza meccanica*, (trad. it.), Bollati Boringhieri, 1994, p. 88 ss.

[12]*Ivi*, p. 103.

[13]V. A.M. Turing, *Proposta per lo sviluppo nella divisione matematica di una macchina calcolatrice elettronica (Ace). Parte I: presentazione descrittiva* e Id., *Macchine calcolatrici e intelligenza*, entrambi in Id., *Intelligenza meccanica*, cit., p. 29 ss. e p. 125 ss.

[14]«Le *posizioni* di un sistema formale possono funzionare come *occorrenze* in un altro sistema (di "livello superiore") [...]. Ogni occorrenza del gioco dell'algebra è una posizione valida in un altro gioco, che potremmo chiamare il "gioco delle formule ben formate"» (così J. Haugeland, *Introduzione*, in Id. (a cura di), "Progettare la mente. Filosofia, psicologia, intelligenza artificiale", (trad. it.), il Mulino, 1989, pp. 15-16).

[15]Il che equivale a dire: «un gioco o un sistema che ha tutte e tre le proprietà è *digitale*. In questo senso tutti i sistemi formali sono digitali. La proprietà di essere digitali ha, per ciò che riguarda i sistemi formali, le seguenti importanti conseguenze: due sistemi che sembrano essere assai differenti possono, nonostante ciò, essere essenzialmente il medesimo sistema» (*ivi*, p. 13).

[16]*Ivi*, p. 17.

[17]Nel 1936 lo scienziato dimostrò come costruire una macchina secondo i suoi principi: A.M. Turing, *On computable numbers, with an application to the* Entscheidungsproblem, in "Prooceedings of the London Mathematical Society", series II, vol. 42, 1937, n. 1, p. 230 ss.

[18]Come invece sosteneva A.M. Turing, *Macchine intelligenti*, cit., spec. pp. 91 e 97.

[19]V. A. Damasio, *L'errore di Cartesio. Emozioni, ragione e cervello umano*, (trad. it.), Adelphi, 1995.

[20]Si tratta della c.d. macchia cieca nel nostro campo visivo, corrispondente all'innesto del nervo ottico nella retina. In quella zona dovremmo vedere una macchia nera, eppure il nostro campo visivo è privo di interruzioni.

[21]Così A. Damasio, *op. cit.*, pp. 245-246.

[22]Un interrogativo, questo, che fa da sfondo e al quale – a suo modo – cerca di dare risposta la recente *Proposta di Regolamento del Parlamento europeo e del Consiglio europeo che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione* (COM/2021/206 final).

[23]C. O'Neill, *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, (trad. it.), Bompiani, 2017.

[24]D. Cardon, *Che cosa sognano gli algoritmi*, (trad. it.), Mondadori, 2016.

[25]W. Christl, S. Spiekermann, *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*, Facultas, 2016

[26]V. in tal senso Michal Kosinski, esperto di psicometria, branca della psicologia fondata sull'analisi delle tracce digitali, e in particolare studioso dei profili psico-demografici degli utenti di Facebook. È uno dei principali protagonisti della vicenda Cambridge Analytica.

[27]D. Cardon, *op. cit.*

[28]Cfr. F. Pasquale, *The black box society: The secret algorithms that control money and information*, Harvard University Press, 2015.

[29]«I'm still an optimist, but an optimist standing at the top of the hill with a nasty storm blowing in my face, hanging on to a fence» (T. Berners-Lee, *Tim Berners-Lee on the future of the web: 'The system is failing'*, in "The Guardian", 15 November 2017).

[30]*Ibidem*.

[31]Così si legge in occasione del 28° anniversario della sua invenzione (T. Berners-Lee, *Three challenges for the web, according to its inventor*, in "Web Foundation", 12 March 2017).

[32]Si tratta delle *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*. Le Linee guida sono state aperte alla consultazione pubblica fino al 31 gennaio 2022.

Artificial intelligence, big data and new rights

Abstract: The present is the result of old and new reorganizations and insights. As studies of algorithms, neural networks, and artificial intelligence multiply, speeds change and paradigm shifts occur. With the big data revolution, in fact, the logical-deductive paradigm gives way to the statistical approach which, among various purposes, has the fundamental one to develop predictive and selective models, meanwhile grouping objects into classes. Beyond the indisputable advantages linked to the possibility of processing a large amount of data without a particular expenditure of time and energy, today's technical-scientific development raises many serious questions. These concern, above all, the sphere of rights, which are enriched with new contours and meanings, to the point of protecting almost unprecedented instances. Emblematic is what happens about the right to privacy, which today evolves into the right to protect personal data. Precisely those data that are now the first engine of the contemporary economy.

Keywords: Artificial intelligence – Algorithms – Neural networks – Big data – Data protection

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0062
Articolo sottoposto a peer review

Data retention e privacy in rete: verso una regolazione conforme al diritto UE?

Veronica Palladini

Con il decreto legge n. 132 del 2021, convertito in legge con modificazioni, è stato offerto riparo alla bistrattata disciplina della "Conservazione di dati di traffico per altre finalità" al fine di renderla conforme alla normativa europea in materia di protezione dei dati personali ed alle decisioni della Corte di giustizia in questo ambito. La novella legislativa – intervenuta sull'aspetto procedurale della materia, con la previsione di ulteriori condizioni e limiti per l'acquisizione dei dati di traffico telefonico e telematico – per quanto apprezzabile pare non essere stata in grado di superare tutte le lacune presenti nella disciplina della *data retention*. Ne è un esempio il mancato intervento sui tempi di conservazione dei dati, riforma auspicata dal Garante per la protezione dei dati personali, ma, ad oggi, inattuata. Altro aspetto su cui il legislatore è rimasto silente è la delimitazione dell'ambito soggettivo dell'acquisizione dei dati di traffico per fini di giustizia, ovvero l'opportunità di individuare, con maggior specificazione, i soggetti nei confronti dei quali l'organo giudicante potrebbe autorizzare il conseguimento dei tabulati, dal momento che il fenomeno coinvolge non solo il diritto alla riservatezza dell'indagato ma anche delle persone con cui questi entra in contatto. Ciò premesso, con il presente contributo si intende offrire una rilettura del mezzo di ricerca della prova in esame che – nell'equo contemperamento dei diritti in gioco – si soffermi sulla nuova fisionomia assunta dalla *data retention* nell'era della digitalizzazione, riflettendo, in particolare, sui traguardi già varcati dal legislatore e su quelli che, a gran voce, chiedono, ancora, di essere raggiunti.

Tabulati telefonici e telematici – *Data retention* – Utilizzo dei dati nel processo penale come elementi di prova

Sommario: *1. Il volto dei tabulati (telefonici e) telematici nell'era digitale: il (delicato e necessario) bilanciamento tra protezione dei dati personali e tutela della sicurezza collettiva – 2. Verso una disciplina (quasi) conforme al diritto UE: il decreto legge n. 132 del 2021 e la sua conversione – 3. Le occasioni mancate dalla novella legislativa – 4. Conclusioni*

1. Il volto dei tabulati (telefonici e) telematici nell'era digitale: il (delicato e necessario) bilanciamento tra protezione dei dati personali e tutela della sicurezza collettiva

Nell'era della quarta rivoluzione industriale, ossia della telefonia digitale e dei big data analizzati da sistemi intelligenti, l'accesso alla rete è considerato un diritto fondamentale della persona, condizione per il suo pieno sviluppo individuale[1]. Per questa ragione nel 2015 la Commissione parlamentare per i diritti e i doveri relativi ad Internet ha elaborato la "Dichiarazione dei diritti in Internet"[2]. Il documento, dal significativo valore politico e culturale, pur descrivendo la rete come una risorsa globale e defi-

V. Palladini è dottoranda in Lavoro, sviluppo, innovazione presso l'Università di Modena e Reggio Emilia - Fondazione Marco Biagi.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

nendone l'"accesso" come un diritto fondamentale da assicurare nei suoi presupposti sostanziali, evidenzia come la risorsa non sia indenne da rischi. Vi è infatti il pericolo, tra gli altri, che i poteri pubblici e privati se ne servano per aprire la strada ad una società della sorveglianza, del controllo e della selezione sociale. Per garantire, quindi, una specifica tutela dei diritti in Internet e affinché, invero, questi possano dirsi fondamentali devono parimenti essere anche inviolabili. A tal proposito, sull'impronta di quanto previsto dall'art. 15 della Costituzione, l'art. 7 della Dichiarazione richiede che la segretezza delle informazioni e delle comunicazioni elettroniche ed informatiche sia rispettata e garantita. Deroghe possono essere ammesse solo nei casi e modi stabiliti dalla legge e con l'autorizzazione motivata dell'autorità giudiziaria. Questa puntualizzazione nasce dal fatto che le straordinarie opportunità offerte dalla tecnologia si stanno rivelando utilissime anche nel campo investigativo: la digitalizzazione bussa oramai anche alla porta delle aule di tribunale, stravolgendo il sistema di acquisizione delle prove, con inevitabili ripercussioni in punto di privacy[3]. A dimostrazione del ruolo decisivo assunto dalla prova digitale, si può ricordare il sempre maggior impiego processuale dei dati di traffico telefonici e telematici che ha favorito l'ingresso nel procedimento penale di elementi probatori che consentono di acquisire numerosissime informazioni sull'utente[4]. Se, infatti, per lungo tempo, i dati di traffico sono stati ritenuti meramente "esteriori", oggi non è più così, ragion per cui si richiedono sempre maggiori garanzie e forme di tutele più specifiche per la loro acquisizione. Come affermato dal recente studio della Corte di Cassazione sulle modifiche apportate alla disciplina dei tabulati si tratta, infatti, di informazioni particolarmente "ricche" e di varia natura che consentono di acquisire, a posteriori, non tanto il contenuto, ma tante altre informazioni relative alle telefonate su apparecchi fissi o mobili (fax, sms, mms, e-mail) e, in senso estensivo, i dati relativi ai siti Internet visitati, la geolocalizzazione di un'utenza mobile *ex post*, ma anche in *real time* (mediante la costante rilevazione delle celle di aggancio delle stazioni mobili) effettuando così il *positioning*, un vero e proprio "pedinamento satellitare" del possessore del telefono mobile[5].

I dati di traffico rappresentano, dunque, delle "impronte elettroniche"[6] capaci di fornire notizie di significativa rilevanza come il tempo, la durata, la frequenza delle chiamate, le utenze contattate, i codici IMEI, gli intestatari delle schede SIM e l'ubicazione dell'utenza[7]. Tutto questo permette di mappare le abitudini, le preferenze di una persona con la possibilità di desumere notizie relative alla vita privata che possono avere inevitabilmente natura anche sensibile, in quanto riferite alla personalità e alla sfera intima degli utenti[8]. Non si può quindi certamente negare – come affermato dall'Avvocato Generale UE Cruz Villalón nel giudizio relativo alla vicenda conosciuta come *Digital Rights Ireland*, capostipite in materia di *data retention* – che questi mezzi consentano di creare una «mappatura tanto fedele quanto esaustiva [...] di una persona [...], se non addirittura un ritratto completo della sua identità personale»[9]. Questo accade, come afferma il Garante per la protezione dei dati personali [di seguito "Garante"], perché «il dato apparentemente "esterno" a una comunicazione (ad esempio una pagina web visitata o un indirizzo IP di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: può permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati»[10]. Inoltre, occorre considerare che, con l'avvento dell'intelligenza artificiale, si è diffusa la capacità di analisi attraverso procedure di indagine correlata[11] e queste ultime, tramite la combinazione e la rielaborazione dei dati, sono in grado di realizzare una dettagliata profilazione dell'utente. Per queste ragioni, come sostenuto dalla Corte di Cassazione, può, quindi, risultare opportuno considerare i dati di traffico non solo (o non più) come dati "meramente esterni" dal momento che con essi «si possono ottenere informazioni talora ancora più sensibili delle captazioni»[12].

Proprio traendo spunto dalle parole del giudice della nomofilachia, ma in un senso ancor più ampio, conviene riflettere su quanto possano essere "perigliose e temibili" le informazioni acquisite mediante i tabulati e quante incognite possano presentare. Se da un lato, infatti, i tabulati consentono di conoscere molto degli utenti, dall'altro, paradossalmente, non svelando i contenuti delle conversazioni e quindi le ragioni dei contatti, degli spostamenti e delle ricerche, finiscono con l'essere ancora più insidiosi, per certi versi, di strumenti investigativi storicamente considerati assai intrusivi come le intercettazioni telefoniche che, al contrario, offrono la possibilità di rinvenire più agevolmente possibili spiegazioni contrarie rispetto a quelle incriminanti. Le informazioni così raccolte sono parziali, incomplete ovvero necessitano di contestualizzazione e, se ciò non avviene, il rischio è quello di avere a che fare con risultati orientativi, ma non necessariamente univoci e, soprattutto, soltanto approssimativi. I tabulati, dunque, permettono, di venire a conoscenza di dati che tanto dicono, ma, allo stesso tempo, tanto non dicono. Questo aspetto, di per sé apparentemente poco significativo – nell'ipotesi in cui si consideri il tabulato come "mero" mezzo di ricerca della prova

– assume una certa rilevanza se, in giudizio, il dato di traffico non viene assistito da corroboranti e chiarificatori elementi probatori. Quest'ultima considerazione merita di essere evidenziata – fin d'ora e più ampiamente in seguito – in ragione della recente novella legislativa che ha riguardato la *data retention*. In quest'occasione il Parlamento è intervenuto, su impulso europeo, introducendo nuove condizioni per l'acquisizione dei dati di traffico per fini di giustizia; inoltre, per i *soli* tabulati acquisiti ante riforma – ovvero per i dati acquisiti in assenza delle nuove condizioni procedurali – è stata prevista una tutela più specifica: affinché possano essere utilizzati in giudizio occorre che siano supportati da altri elementi di prova. Ebbene, a nostro avviso, detta specificazione – proprio in ragione dell'incompletezza dei dati di traffico – desta perplessità. È, infatti, nostra opinione che il limite di utilizzabilità introdotto con la novella debba essere esteso a tutti i tabulati, ovvero sia a quelli acquisiti prima che a quelli acquisiti dopo la modifica normativa, dal momento che nessun dato di traffico può spiegarsi da solo. Vieppiù il tabulato espone non solo la persona sottoposta ad indagini preliminari, ma anche le persone con cui l'indagato entra in contatto. Ne deriva che anche per queste ultime le informazioni, indirettamente acquisite, per quanto invasive, non possono che risultare parziali e dunque ipotetiche, in questo modo i tabulati possono rappresentare un temibile strumento inquisitorio.

Alla luce della descritta fisionomia assunta dai dati di traffico nell'era della digitalizzazione non v'è dubbio che, in un quadro tanto complesso, sia necessario individuare stringenti mezzi di tutela che, pur non impedendo l'uso di questi moderni strumenti investigativi, li contenga entro un ambito di assoluta necessità e presidiato da garanzie rafforzate, dal momento che l'acquisizione dei dati di traffico presenta evidenti ripercussioni sul piano dei diritti fondamentali. Il tema della *data retention* assume, infatti, un rilievo costituzionale[13] poiché se, da un lato, soddisfa l'interesse pubblico a reprimere i reati e a perseguire in giudizio coloro che delinquono, dall'altro si scontra con il diritto alla protezione dei dati personali, riconosciuto come inviolabile ai sensi degli artt. 2, 14, e 15 Cost[14]. Al diritto di vivere in una società libera, che non faccia uso della digitalizzazione come strumento di sorveglianza, si affianca, d'altra parte, la necessità che l'accertamento giudiziale sia garantito attraverso i più efficaci sistemi a disposizione e, in questo, l'acquisizione dei dati di traffico è certamente essenziale. Le esigenze di giustizia e di repressione dei reati sono, dunque, tanto forti quanto la loro frizione con la protezione della privacy, intesa come il diritto alla riservatezza non solo della persona sottoposta ad indagini bensì di tutti coloro che vi entrano in contatto[15].

Ciò premesso, ovvero preso atto della fisionomia assunta dai tabulati nell'era della digitalizzazione ed evidenziate le temibili incognite che il tema della *data retention* presenta, è ora possibile, con un'indagine di maggior dettaglio, riflettere sulle recenti modifiche che il legislatore, su impulso sovranazionale[16], ha apportato alla disciplina dell'acquisizione dei dati di traffico per motivi di giustizia. Nonostante, infatti, la travagliata esperienza legislativa vissuta dall'art. 132 d.lgs. n. 196 del 2003 – ad oggi si contano ben undici aggiornamenti – la disciplina mantiene intatte alcune criticità che la recentissima modifica, tesa a risolvere l'annosa *querelle* che per anni ha coinvolto la giurisprudenza, nazionale e non solo, non è stata pienamente in grado di superare.

2. Verso una disciplina (quasi) conforme al diritto UE: il decreto legge n. 132 del 2021 e la sua conversione

Il 22 luglio 2021 il Garante per la protezione dei dati personali ha inviato al Parlamento e al Governo una segnalazione sulla disciplina della conservazione, ai fini di giustizia, dei dati di traffico telefonico ed informatico[17]. L'oggetto della nota riguardava l'opportunità di riformare la *data retention* (art. 132 Codice per la protezione dei dati personali [da ora in avanti indicato anche come Codice]), intervento già più volte sollecitato, ma divenuto impellente a seguito della sentenza della Corte di giustizia dell'Unione europea del 2 marzo 2021 (causa C-746/18 *H.K.*). Quest'ultima ha consolidato, con alcune novità, un orientamento già affermatosi[18] a partire dalla sentenza *Digital Rights Ireland* del 2014 (cause riunite C-292/2012, C-594/2012), con cui la CGUE ha sancito l'illegittimità della direttiva 2006/24/CE sulla conservazione dei dati di traffico, per violazione del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta[19], nel bilanciamento tra protezione dei dati ed esigenze di pubblica sicurezza[20].

A seguito della segnalazione del Garante, l'Esecutivo è intervenuto con il decreto legge n. 132 del 2021, poi convertito con modificazioni dalla legge n. 178 del 2021, nell'ottica di una conformazione del diritto nazionale alla pronuncia della curia europea e quindi alla disciplina unionale. L'intervento d'urgenza è stato mosso dalla ritenuta necessità di garantire la possibilità di acquisire i dati relativi al traffico telefonico e telematico per fini di indagine penale nel rispetto dei principi enunciati dalla Grande sezione della Corte di giustizia dell'Unione europea nella sentenza citata ovvero, in particolare, di circoscrivere le

attività di acquisizione ai procedimenti penali aventi ad oggetto forme "gravi" di criminalità e, inoltre, di assicurare che dette attività fossero soggette al controllo di un'autorità giurisdizionale. La revisione della *data retention* è risultata, poi, quanto più necessaria ed impellente per lo stato di confusione in cui versava la giurisprudenza nazionale, di legittimità e di merito che, nonostante il verdetto europeo, non pareva essersi uniformata. A dimostrazione, il rinvio pregiudiziale del Tribunale di Rieti (sez. pen., 4 maggio 2021, ordinanza di rinvio alla Corte di giustizia)[21], volto a chiarire la compatibilità della disciplina interna prevista dall'art. 132 del Codice con la disciplina unionale a seguito della sentenza della Corte di giustizia 2 marzo 2021 e la carrellata di pronunce che, in pochissimi mesi, hanno affannato i tribunali di tutta Italia[22].

In particolare, tra le questioni che hanno assillato maggiormente la giurisprudenza nazionale, occorre soffermarsi su quella relativa al ruolo da riconoscere alla pronuncia interpretativa della Corte di giustizia. Se per alcuni[23], infatti, questa poteva ritenersi direttamente applicabile, per altri[24], la tesi maggioritaria a dire il vero, *a contrario* era necessario un intervento normativo volto ad armonizzare la disciplina, come poi avvenuto.

Altri dubbi hanno riguardato gli effettivi esiti a cui quella interpretazione avrebbe dovuto condurre, anche in riferimento alle attività di acquisizione già compiute, tema poi chiarito da una specifica disciplina transitoria inserita nella legge di conversione del decreto legge n. 132 del 2021, sulla quale avremo modo di soffermarci ampiamente in seguito.

Il dibattito ha poi coinvolto ulteriori aspetti quali l'individuazione dei reati definiti "gravi" dalla Corte di giustizia ed il concetto di "autorità giudiziaria" come inteso dalla Corte di Lussemburgo. Quest'ultima ha richiesto, infatti, che l'accesso ai dati provenisse da un'autorità non solo indipendente, ma anche imparziale, ovvero terza e neutrale, ponendo in luce la necessità che l'intrusione nella vita privata dei cittadini fosse assistita da una riserva di giurisdizione oltre che di legge. Orbene, se nel nostro ordinamento è pacifico che il pubblico ministero, l'organo che fino alla novella era preposto all'acquisizione dei tabulati, sia indipendente, maggiori dubbi nascono in merito agli altri requisiti dal momento che la pubblica accusa è parte processuale[25].

La Corte di Giustizia è invero intervenuta anche su ulteriori aspetti. Nella sentenza del 2 marzo i giudici di Lussemburgo hanno infatti ribadito l'esigenza – già affermata nelle sentenze *Digital Rights* e *Tele 2 Sverige* del 21 dicembre 2016 (C-203/15) – di delimitare soggettivamente l'ambito dei destinatari. Specifica, infatti, la Corte che «un accesso generale a tutti i dati conservati, indipendentemente da un qualche collegamento, almeno indiretto, con la finalità perseguita, non può considerarsi limitato allo stretto necessario. [...] Un accesso siffatto può [...] essere consentito [...] soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere»[26].

A seguito della sentenza *H.K.* e tramite la segnalazione del 22 luglio, di cui già si è detto, anche il Garante nazionale si è mosso, al fine di sollecitare il legislatore ad ottemperare alle istanze sovranazionali. In questa occasione, l'Authority ha rilevato, oltre alla necessità di adeguarsi alle previsioni della sentenza *H.K.*, anche l'urgenza di intervenire sul differente rimedio offerto ad "accusa" e "difesa" in caso di inerzia del fornitore dei servizi, capace di pregiudicare le esigenze probatorie della difesa, a detta del Garante, in occasione della segnalazione del 22 luglio 2021 di cui si è parlato poc'anzi, «talora irrimediabilmente». Accade spesso, infatti, che l'inottemperanza dei fornitori alle richieste avanzate dalle difese determini un grave pregiudizio per gli interessati, come dimostra anche una recente ordinanza ingiunzione che il Garante ha emesso nei confronti di una società telefonica per non aver soddisfatto la richiesta di tabulati da parte dell'imputato e quindi aver pregiudicato la sua difesa[27].

Infine, come si approfondirà meglio in seguito, il Garante ha evidenziato che, a seguito degli interventi della Corte di giustizia, il legislatore avrebbe dovuto rivedere il termine di conservazione dei tabulati (attualmente particolarmente lungo).

Ebbene, alla segnalazione del Garante è seguito un intervento decisivo del legislatore che, come vedremo qui di seguito, ha modificato sensibilmente – ed effettivamente nell'osservanza di quanto statuito dalla Corte di giustizia – la disciplina dell'art. 132 del Codice, similmente a quanto previsto in materia di intercettazioni.

Passando, dunque, in rassegna le novità apportate alla disciplina della *data retention* è bene precisare che innanzitutto sono stati introdotti, e quindi individuati, i reati per così dire "gravi" per i quali è consentito procedere all'acquisizione dei dati di traffico, al fine di sottrarre ai giudici il potere/dovere di individuare in concreto i reati idonei a soddisfare il requisito di gravità richiesto dalla CGUE. Oggi, infatti, la legge prevede che i tabulati possano essere acquisiti per la persecuzione dei soli reati puniti con la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni ovvero per i reati di minaccia, molestia o disturbo alle persone col mezzo del tele-

fono, quando la minaccia, la molestia e il disturbo possano dirsi "gravi".

Poi è stata recepita un'ulteriore fondamentale istanza – pure di provenienza europea ma ribadita dall'Authority nazionale nella sua segnalazione – ovvero la necessità che l'accesso ai dati provenga da un'autorità non solo indipendente, ma anche imparziale, ovvero terza e neutrale. In questo modo, se prima l'acquisizione avveniva per decreto motivato del pubblico ministero, ora è stata introdotta la giurisdizionalizzazione della procedura: i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore, della persona sottoposta a indagini, della persona offesa e delle altre parti private, non dissimilmente da quanto avviene per le intercettazioni di comunicazioni.

Allo stesso tempo, per mitigare tale previsione, è stato consentito, in caso di urgenza, e dunque quando il ritardo nell'acquisizione dei dati possa provocare un grave pregiudizio alle indagini, che il PM possa acquisire direttamente i dati con proprio decreto motivato, che dovrà essere comunicato entro quarantotto ore al giudice affinché lo convalidi (nuovo comma 3-*bis* dell'art. 132 del Codice). In questo caso la disciplina, per quanto simile a quella in materia di intercettazioni, prevede un limite temporale più esteso, ossia di quarantotto ore, anziché ventiquattro.

È stato poi introdotto il requisito della "rilevanza" dell'acquisizione dei dati di traffico "ai fini della prosecuzione delle indagini", specificazione prima non contemplata.

Ancora, come richiesto dal Garante nella segnalazione del 22 luglio, è stata equiparata la disciplina per accusa e difesa: oggi, infatti, devono entrambe passare dal vaglio del giudice per le indagini preliminari, e, nell'ottica di garantire il principio di parità delle armi, con la novella legislativa è stata anche abolita la facoltà del difensore di acquisire direttamente i dati presso i fornitori ex art 391-*quater* c.p.p.

Infine, è stata prevista, in sede di conversione in legge, una norma transitoria con la quale si introduce una duplice condizione per l'utilizzo dei dati già acquisiti: i tabulati, a carico dell'imputato, saranno utilizzabili solo unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei medesimi reati per i quali il nuovo art. 132 del Codice consente la loro acquisizione.

Emerge, da questo rapido affresco, come, per quanto la disciplina sia stata avvicinata, in termini di maggiori tutele, a quella delle intercettazioni, la novella mantiene comunque delle differenze: per i tabulati, infatti, la legge richiede che gli indizi di reato "siano sufficienti" e non "gravi" e che siano "rilevanti" anziché "assolutamente indispensabili" ai fini investigativi. Ancora, rispetto alle intercettazioni differisce la categoria dei delitti per i quali si ammettono le operazioni e, infine, un'ulteriore differenza riguarda i termini per la convalida nei casi d'urgenza. Tali misure, secondo il parere espresso dal Garante sullo schema di decreto legge, sono giustificate in ragione della minore invasività del mezzo[28].

In conclusione, è possibile affermare che il legislatore si sia allineato alla disciplina UE da un lato individuando i reati per cui è consentito procedere all'acquisizione dei dati di traffico, dall'altro giurisdizionalizzando la procedura, cioè attribuendo la valutazione sulla fondatezza della richiesta ad un organo imparziale ovvero terzo e neutrale.

Manca, tuttavia, ancora all'appello un ulteriore aspetto su cui ha insistito la Corte di giustizia: quello relativo alla delimitazione dell'ambito soggettivo, ad oggi inattuato. Così come non possiamo neppure dire che il legislatore si sia conformato alle istanze del Garante relative alla riduzione del termine di conservazione dei tabulati e questo nonostante l'Authority abbia reiterato la richiesta oltre che nella segnalazione del 22 luglio 2021 anche nel parere sullo schema di decreto legge del 10 settembre 2021[29].

3. Le occasioni mancate dalla novella legislativa

Il decreto legge n. 132 del 2021 e la relativa legge di conversione, per quanto apprezzabili, non hanno avuto, come si è visto, la capacità di superare tutte le insidie presenti nella previgente disciplina della *data retention*. A tal proposito, intendiamo, dunque, concentrare l'attenzione sulle, a nostro parere principali, zone d'ombra che presenta la novella legislativa, ovvero: a) la questione relativa ai tempi di conservazione dei dati; b) la disciplina intertemporale che il legislatore ha introdotto in sede di conversione, con la quale – derogando al principio processuale del *tempus regit actum* – si ammette l'utilizzabilità, dei dati acquisti ante riforma soltanto unitamente ad altri elementi di prova (e solo per l'accertamento dei reati per i quali ora la legge consente l'acquisizione); c) la mancata delimitazione dell'ambito soggettivo di applicazione della *data retention*. Approfondiamo ora singolarmente ciascuno di questi aspetti.

a) I tempi di conservazione dei dati

Come evidenziato dal parere del Garante sul decreto legge n. 132 del 2021, la novella legislativa non si è adeguata alla giurisprudenza di Lussemburgo laddove richiede, affinché l'acquisizione dei tabulati possa dirsi lecita, che il termine di conservazione non

ecceda il principio di proporzionalità (come già chiarito dalla sentenza *Tele2 Sverige*). E, a tal proposito, la disciplina attuale certo non può dirsi proporzionata perché, se da un lato prevede che i tabulati telefonici siano conservati per un termine massimo di 24 mesi, che scende a 12 per quelli telematici, e a 30 giorni per le chiamate senza risposta, dall'altro stabilisce anche, per i reati di competenza delle procure distrettuali o per i quali la durata delle indagini preliminari è ampliata a due anni (artt. 51, comma 3-quater e 407, comma 2, lett. a, c.p.p. ovvero delitti, consumati o tentati, con finalità di terrorismo, associazioni di tipo mafioso anche straniere, strage, omicidio, rapina, etc.) un termine di conservazione di settantadue mesi (così come previsto dalla legge n. 167 del 2017). Nonostante tale ultimo termine sia limitato a specifiche categorie di reati particolarmente efferati, l'impossibilità da parte del provider di effettuare una valutazione e quindi una selezione, a priori, sul reato per il quale, in un momento successivo, gli potrà essere richiesta la consegna dei dati conservati (considerato il fatto che i dati di traffico hanno natura retrospettiva) comporta che, inevitabilmente, la conservazione di tutti i dati sia generalizzata a sei anni, salvo poi limitarne l'utilizzabilità processuale ai soli casi normativamente considerati. Questo aspetto, come rilevato in passato dalle associazioni di categoria dei fornitori di accesso e di servizi su Internet (Assprovider e Aup), comporta un serio problema: la creazione di archivi vastissimi, utilizzabili come dossier a carico di un soggetto con importanti ripercussioni in tema di privacy e quindi di diritti fondamentali[30], aspetto che, certamente, non può essere tollerato. Urge, dunque, un intervento immediato sulla disciplina che, nel bilanciamento degli interessi coinvolti, assicuri una tutela immediata al diritto alla riservatezza.

b) La disciplina transitoria

Come noto, la disciplina dei tabulati ha natura processuale e questo significa che ad essa non si applica il principio della retroattività della *lex mitior*, caposaldo del diritto penale sostanziale, bensì il più rigido *tempus regit actum*. Ordunque, nel caso di specie, l'applicazione esclusiva di quest'ultimo principio avrebbe dato adito ad una rilevante incertezza e rimesso nelle mani degli organi giudicanti la scelta della disciplina applicabile nell'asse temporale tra la decisione della Corte di giustizia (2 marzo 2021) e l'intervento del decreto legge n. 132 del 2021 (30 settembre 2021), tema sul quale, come abbiamo potuto notare, non vi era in giurisprudenza unanimità di vedute[31]. Sennonché, è giunto in soccorso l'Esecutivo inserendo, nel primo schema di decreto legge, una disciplina transitoria modulata sul principio del *tempus regit actum* che prevedeva, tuttavia, un correttivo importante: l'utilizzabilità dei tabulati acquisiti prima della data di entrata in vigore della novella era subordinata alla ricorrenza dei presupposti delineati dal decreto legge oggetto di vaglio da parte del giudice in sede di convalida. Tutto bene fin qui, se non fosse che la norma transitoria è scomparsa nella versione approvata definitivamente, sollevando rilevanti perplessità in dottrina[32], per poi riapparire nella legge di conversione. Il legislatore – con la legge n. 178 del 2021 – ha, infatti, previsto una disciplina transitoria, tra la precedente versione dell'art. 132 del Codice e la successiva, con la quale è stato specificato che i dati acquisiti prima dell'entrata in vigore delle nuove disposizioni possano essere comunque utilizzati ma «solo unitamente ad altri elementi di prova» e soltanto nell'ipotesi in cui si perseguano specifici reati, per i quali la legge, oggi, ammette l'acquisizione.

Ebbene, sulla base delle considerazioni poc'anzi svolte[33], in merito alla parzialità delle informazioni contenute nei tabulati, ci si dovrebbe chiedere se non sarebbe più opportuno che il legislatore estendesse quanto previsto dalla disciplina transitoria – ovvero la necessità che la valutazione dei dati avvenga unitamente ad altri elementi probatori – anche alle informazioni acquisite con la procedura novellata. Vero è che l'interpolazione legislativa ha inserito due ulteriori elementi, ovvero, da un lato, il vaglio del giudice per le indagini preliminari sulla richiesta del pubblico ministero e, dall'altro, la possibilità di disporre l'acquisizione dei tabulati solo se rilevanti ai fini della prosecuzione delle indagini relative a specifici reati, indicati dalla legge. Ciononostante, la normativa sembra trascurare che i tabulati, per quanto pervasivi, rivelano informazioni pur sempre incomplete, ovvero tracce che, attraverso sofisticati strumenti informatici, possono essere artificiosamente correlate ricavando ipotesi, anche logiche, ma pur sempre ipotesi che, per quanto orientativamente utili, possono essere anche ingannevoli, presuntive e quindi necessitano di essere assistite e corroborate da altri elementi probatori. L'esigenza, sentita dal legislatore, di specificare che le informazioni acquisite secondo la previgente disciplina devono essere affiancate da altri elementi probatori, solleva quindi inevitabilmente un interrogativo: se i tabulati acquisiti prima della novella devono essere valutati alla luce di altri elementi probatori, per quale motivo quelli acquisiti successivamente non devono rispettare il medesimo rafforzamento probatorio, lo stesso standard di garanzia? La giurisdizionalizzazione del procedimento acquisitivo è di per sé idonea a consentire che l'intera valutazione si erga su dati "esteriori" che, per quanto invasivi, rimangono parziali, e necessitano di essere interpretati più che dedotti?

A nostro parere tale specificazione non solo risulta ingiustificata, ma pure illogica. Proprio in ragione della funzione meramente orientativa che i tabulati assolvono e a maggior ragione se si considera che le limitazioni all'utilizzabilità operano nella sola ipotesi in cui i tabulati siano acquisiti – e quindi le informazioni siano utilizzate – a carico dell'imputato, questa precisazione doveva essere estesa anche ai dati acquisiti a seguito della riforma legislativa: essa, insomma, doveva riguardare tutti i tabulati o, in alternativa, nessuno.

c) La mancata delimitazione dell'ambito soggettivo

L'ultima delle questioni che solleva perplessità riguarda l'omissione da parte della novella dell'individuazione dei "soggetti" nei confronti dei quali è possibile accedere ai dati. Aspetto sul quale, a ritmo incessante, la giurisprudenza europea con le sentenze *H.K.*, ma anche *Tele2* e ancora prima *Digital Rights Ireland*, è intervenuta prevedendo che l'acquisizione dei dati di traffico sia ammessa nei soli confronti di chi sia sospettato di reato e solo in casi eccezionali – per la tutela di interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica, minacciati da attività di terrorismo – anche nei confronti di altre persone e sempre che sussistano elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta ad attività criminali. Per i giudici europei tale specificazione è irrinunciabile: occorre circoscrivere i soggetti nei confronti dei quali questi dati possono essere acquisiti e lo si deve fare secondo canoni oggettivi, che – in un'ottica di proporzionalità, ma anche di minimizzazione[34] – garantiscano un equo bilanciamento tra la tutela della sicurezza collettiva e il rispetto dell'altrui riservatezza e dignità. Ragion per cui la Corte di giustizia nella sentenza del 2 marzo 2021 richiede espressamente che si acquisiscano i dati (solo) di persone sospettate di progettare, di commettere o di aver commesso un grave illecito.

Nonostante il legislatore nazionale sul tema sia rimasto silente, la questione è di particolare rilevanza e diviene ancor più delicata se si considera, come poc'anzi anticipato, che i dati di traffico non coinvolgono solo l'indagato, bensì, inevitabilmente, tutte le persone con cui questo entra in contatto[35] e, dunque, la mancata restrizione dell'ambito soggettivo della disciplina può avere sensibili ripercussioni oltre che in punto di diritto alla riservatezza anche in tema di trasformazione del mezzo di ricerca della prova in mezzo di acquisizione di notizie di reato. Per queste ragioni, a nostro avviso, risulta oramai indifferibile un intervento normativo che adegui il diritto nazionale a quello unionale. È nostra opinione, infatti, che a nulla valga l'affermazione secondo cui la delimitazione soggettiva sia implicita nella novella legislativa. Certo, il comma terzo dell'art. 132 del Codice, nel fare riferimento all'acquisizione dei tabulati «ove rilevanti ai fini della prosecuzione delle indagini», specifica, in questo modo, indirettamente, che questi possono essere utilizzati non per iniziare le indagini, ma soltanto per proseguirle, ovvero soltanto nei confronti di chi sia già sottoposto ad indagini per i reati, oggi, previsti dall'art. 132 del Codice. A nostro parere, tuttavia, questa precisazione riguarda un momento processuale successivo, ovvero fa riferimento all'utilizzabilità in giudizio dei dati già acquisiti; quello che invece reclama il diritto europeo è un intervento normativo sulla fase precedente ovvero quella dell'acquisizione dei dati di traffico.

Neppure si può condividere l'assunto che la mancata delimitazione dell'ambito soggettivo soddisfi un'altra esigenza: utilizzare detto strumento per i procedimenti nei confronti, almeno in una prima fase, di ignoti, dal momento che, argomenta una certa dottrina, se così non fosse, si imbriglierebbero le mani delle procure nella persecuzione di reati non bagatellari[36]. Quest'ultima ricostruzione, per quanto soddisfi l'esigenza di assicurare l'efficiente esercizio dell'azione penale, *ex* art. 112 Cost., presta, tuttavia, il fianco a critiche, in un'ottica di conformità al diritto unionale.

A nostro avviso, l'unica soluzione prospettabile è quella sostenuta da un certo orientamento dottrinale che ha suggerito, a ragion veduta, di sollevare questione di legittimità costituzionale in rapporto all'art. 117, comma 1, Cost., che vincola la potestà legislativa dello Stato al rispetto, tra l'altro, dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali[37]. Tale soluzione pare, infatti, l'unica prospettabile, nell'attesa che il legislatore intervenga per colmare la lacuna offrendo la miglior soluzione nell'ottica di un corretto bilanciamento tra esigenze di giustizia e di tutela della riservatezza.

4. Conclusioni

Traendo le fila di questa ricostruzione, non si può negare che la recente revisione normativa sul tema qui analizzato possa considerarsi apprezzabile: il Governo prima ed il Parlamento poi, come si è visto, hanno, seppur parzialmente, accolto le istanze espresse dalla giurisprudenza europea ed hanno offerto una disciplina che ha tenuto conto non solo dell'esigenza di assicurare una tutela alla sicurezza collettiva e all'esercizio dell'azione penale, ma anche al diritto alla riservatezza della persona sottoposta ad indagini e/o dell'imputato. E lo hanno fatto alla luce della consapevolezza che oggigiorno i dati di traffico sono

mezzi di ricerca della prova tanto efficienti quanto invasivi. È quindi possibile affermare che la rivoluzione tecnologica che stiamo vivendo e, dunque, la sempre maggiore pervasività degli strumenti digitali con cui dobbiamo fare i conti e, ovviamente, le incessanti richieste in tal senso da parte delle istituzioni europee, hanno indotto le autorità nazionali ad offrire maggior riparo alla tutela della privacy.

Ciononostante, permangono ancora significative perplessità, innanzitutto per quanto riguarda i tempi di conservazione dei dati, sui quali nulla si è detto e che risultano ancora eccessivamente dilatati e, quindi, non proporzionati in un'ottica di minimizzazione. La conservazione generalizzata a sei anni di dati tanto dettagliati, invasivi ed intimi non può infatti dirsi un sacrificio accettabile.

Ancora, un'altra perplessità riguarda la specificazione, introdotta dalla disciplina transitoria, che i soli dati acquisiti ante riforma debbano essere valutati "unitamente ad altri elementi di prova", precisazione che invero, a nostro parere, deve essere estesa anche ai dati acquisiti a seguito della riforma legislativa in ragione di un aspetto di cui spesso ci si dimentica: l'incompletezza delle informazioni raccolte tramite i tabulati che, come si è affermato, tanto dicono e tanto non dicono e che, per questa ragione, necessitano di essere corroborate da altri elementi probatori. Ed infine, l'ultima delle considerazioni precedentemente avanzate: come ampiamente dimostrato, i tabulati sono, oggi, capaci di coinvolgere, seppur indirettamente, anche coloro con cui le persone sottoposte ad indagini entrano in contatto. Se questo lo si considera unitamente al fatto che i dati di traffico offrono una lettura dei fatti incompleta, meramente orientativa che, già ora e sempre di più in futuro, sarà fornita da sistemi di analisi plausibilmente non umani ma di intelligenza artificiale, risulta impellente delimitare soggettivamente i destinatari di tali misure, anche sulla scorta di quanto espressamente indicato, a più riprese, dalla giurisprudenza dell'Unione europea.

Note

[1]A tal proposito preme dar conto che esiste un dibattito risalente sul diritto di accesso ad Internet ed in particolare sul suo "controverso" fondamento costituzionale, *ex plurimis*, i contributi di M. Pietrangelo, *Oltre l'accesso ad Internet, tra tutele formali ed interventi sostanziali. A proposito dell'attuazione del diritto di accesso ad Internet*, in M. Nisticò, P. Passaglia (a cura di), "Internet e Costituzione. Atti del Convegno, Pisa 21-22 novembre 2013", Giappichelli, 2014, pp. 169-188; M.R. Allegri, G. D'Ippolito (a cura di), *Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee*, Aracne, 2017; P. Costanzo, *Miti e realtà dell'accesso ad Internet (una prospettiva costituzionalistica)*, in "Consulta Online", 2012, pp. 1-14; G. De Minico, *Accesso a Internet tra mercato e diritti sociali nell'ordinamento europeo e nazionale*, in "federalismi.it", 2018, numero speciale 4, pp. 126-146; S. Scagliarini, *I diritti costituzionali nell'era di Internet: cittadinanza digitale, accesso alla rete e net neutrality*, in T. Casadei, S. Pietropaoli (a cura di), "Diritto e tecnologie informatiche", Wolters Kluwer, 2021, pp. 3-15; infine, in tempi recentissimi, G. D'Ippolito, *La tutela dell'effettività dell'accesso ad Internet e della neutralità della rete*, in questa Rivista, 2021, n. 2, pp. 33-42. Aldilà del dibattito dottrinale, occorre comunque ricordare che, nonostante siano state presentate proposte di riforma costituzionale per il riconoscimento del diritto di accesso ad Internet, il Parlamento non è ancora intervenuto sul tema, salvo alcuni eccezionali esempi, tra cui la "Dichiarazione dei diritti in Internet" di cui si parlerà in questo paragrafo.

[2]D'ora in avanti, anche semplicemente "Dichiarazione".

[3]Sul tema, O. Pollicino, *Costituzionalismo, privacy e neurodiritti*, in "Medialaws", 2021, n. 1, p. 9 ss., che analizza il conflitto tra privacy e avvento delle tecnologie digitali, ma anche G. De Gregorio, R. Torino, *Privacy, tutela dei dati personali e big data*, in E. Tosi (a cura di), "Privacy Digitale", Giuffrè, 2019, pp. 447-484.

[4]C. Domenicali, *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in "federalismi.it", 2018, n. 7, pp. 2-3; le considerazioni che l'autrice svolge sulle perquisizioni online possono essere estese anche al tema dei tabulati telematici.

[5]Cfr. Corte di Cassazione, Ufficio del massimario, *Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale (art. 1. d.l. 30 settembre 2021, n. 132)*, 13 ottobre 2021, pp. 5-6 in cui è richiamato lo scritto di G. Busia, *Elenco tassativo delle informazioni da archiviare*, in "Guida al Diritto", 17 gennaio 2004, n. 2, p. 28 ss., che mette in luce il rischio che le informazioni acquisite rivelino non solo i dati esteriori delle comunicazioni elettroniche.

[6]Cfr. Corte di Cassazione, Ufficio del massimario, *Relazione su novità normativa*, cit., p. 6.

[7]Più nel dettaglio, il d.lgs. n. 109 del 2008, rubricato "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE", specifica quali sono le informazioni reperibili con l'acquisizione dei tabulati telematici.

[8]Cfr. S. Marcolini, *L'istituto del data retention dopo la sentenza della Corte di Giustizia del 2014*, in A. Cadoppi, S. Canestrari, A. Manna, (a cura di), "Cybercrime", Utet Giuridica, 2019, pp. 1581-1585.

[9]Si richiamano le conclusioni (par. 65 e 74) dell'Avvocato Generale UE Cruz Villalón nel giudizio relativo alle cause riunite C-293/12 e C-294/12, che fanno riferimento alla vicenda *Digital Rights Ireland*. In quell'occasione la Corte di giustizia ha dichiarato l'invalidità della Direttiva 2006/24/CE in materia di conservazione dei dati per violazione degli artt. 7, 8, 52, paragrafo 1, della Carta, per violazione del principio di proporzionalità in tema di *data retention*.

[10]Garante per la protezione dei dati personali, *Provvedimento per la sicurezza dei dati di traffico telefonico e telematico* del 17 gennaio 2008.

[11]Sulle problematiche che l'intelligenza artificiale crea in materia di *data protection* si veda F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018; più in generale sul tema della tutela della privacy nella rivoluzione tecnologica si veda S. Scagliarini, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in "Consulta Online", 2021, pp. 489-532.

[12]Corte di Cassazione, Ufficio del massimario, *Relazione su novità normativa*, cit., p. 7.

[13]Cfr. Corte cost., 11 marzo 1993, n. 81. Nell'occasione la Consulta, nel dichiarare non fondata la questione di costituzionalità relativa all'art. 266 c.p.p. sollevata in riferimento all'art. 15 Cost., afferma come i dati anche esteriori delle conversazioni (destinatario, tempo, luogo della chiamata) rientrino nella materia dell'art. 15 Cost. ovvero siano coperti dalle garanzie di libertà e segretezza. Cfr. a commento della pronuncia, S. Di Filippo, *Dati esteriori delle comunicazioni e garanzie costituzionali*, in "Giur. it.", 1995, n. 1, p. 107 ss.

[14]Sul tema si veda Corte cost., 21 febbraio 2019, n. 20, sulla quale, tra gli altri, si vedano i commenti di I.A. Nicotra, *Privacy vs trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte*, in "federalismi.it", 3 aprile 2019; nonché O. Pollicino, F. Resta, *Trasparenza amministrativa e riservatezza, verso nuovi equilibri: la sentenza della Corte costituzionale*, in "Agenda Digitale", 2019, n. 7.

[15]Sulla contrapposizione privacy e sicurezza si vedano, *ex plurimis*, M. Orofino, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in "MediaLaws", 2018, n. 2, pp. 82-104; G. De Minico, *Costituzione, Emergenza e Terrorismo*, Jovene, 2016, p. 205 ss.; S. Scagliarini, *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni pro e alcuni contra*, in "Il diritto dell'informazione e dell'informatica", nn. 4-5, 2014, pp. 873-886; L. Califano, *Privacy e sicurezza*, in A. Torre (a cura di), "Costituzioni e sicurezza dello Stato", Maggioli, 2013, pp. 563 ss.

[16]Sugli effetti della sentenza di Lussemburgo del 2 marzo 2021 sul tema sicurezza pubblica in connessione con la riservatezza cfr. F. Guella, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in "DPCE Online", 2017, p. 350; F. Torre, *Data retention: una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della Corte di giustizia 2 marzo 2021, C-746/18)*, in "Consulta Online", pp. 540 ss., ed in particolare i paragrafi dedicati al giudizio di proporzionalità, pp. 545-547.

[17]Garante per la protezione dei dati personali, *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*.

[18]Cfr. G. Formici, *La data retention saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in "DPCE Online", 2021, p. 1368.

[19]Sulla sentenza *Digital Rights*, *ex plurimis*, cfr. R. Flor, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla cd "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine*, in "Diritto Penale Contemporaneo", 2014, pp. 178-190; S. Scagliarini, *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni pro e alcuni contra*, cit., pp. 873-886. Per una ricostruzione, invece, della giurisprudenza nazionale successiva alla sentenza *Digital Rights Ireland*, si vedano M. Riccardi, *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in "Diritto Penale Contemporaneo", 9 dicembre 2016, n. 3, p. 156 ss.; S. Marcolini, *L'istituto del data retention dopo la sentenza della Corte di Giustizia del 2014*, cit., pp. 1581-1585.

[20]Per quest'ultimo aspetto si veda F. Resta, *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna*, in "Giustizia Insieme", 6 marzo 2021.

[21]V. il testo della ordinanza.

[22]A mero scopo esemplificativo si ricordano, l'ordinanza del Trib. Milano, VII Sez. penale, 22 aprile 2021, che ha rigettato l'eccezione di inutilizzabilità relativa all'utilizzo dei tabulati telefonici non individuando alcun contrasto tra l'art. 132 del Codice e la normativa europea; il decreto del Tribunale di Roma, (G.i.p. Roma, 29 aprile 2021) che ha stabilito, in assenza di un intervento legislativo, l'impossibilità di garantire una omogenea individuazione di quelli che, a parere della Corte europea, dovevano essere i «i gravi crimini» che avrebbero giustificato la *data retention*. Sul disorientamento della magistratura nazionale a seguito della sentenza *H.K.*, si veda il contributo di C. Parodi, *Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge*, in "ilprocessotelematico.it", 25 maggio 2021.

[23]Tribunale di Roma (decreto 25 aprile 2021, Sez. G.i.p.), in cui il giudice romano ha ritenuto direttamente applicabile, e con effetti vincolanti *erga omnes*, la decisione della CGUE, rilevando quindi il sopravvenuto contrasto tra l'art. 132 del Codice e l'art. 15 della direttiva n. 2002/58/CE, come interpretata dalla CGUE nella pronuncia *H.K.*

[24]Sul punto, ad esempio, Corte d'assise Napoli (Sez. I, ord. 16 giugno 2021) secondo cui l'interpretazione della direttiva contenuta nella sentenza CGUE non poteva avere effetti applicativi immediati e diretti per l'eccessiva indeterminatezza; negli stessi termini, Tribunale di Tivoli, (sez. G.i.p., ordinanza 9 giugno 2021); ma anche Tribunale di Roma (decreto 29 aprile 2021). Sul fronte della giurisprudenza di legittimità, giova premettere che la questione relativa alle restrizioni nell'accesso ai tabulati telefonici si è posta anche prima della sentenza della CGUE del 2021, già a partire dalla sentenza *Digital Rights*, tuttavia, in questa sede, preme dar conto dei soli arresti successivi alla pronuncia *H.K.* Tra questi, in particolare, Cass., sez. II, 7 settembre 2021, n. 33116, in cui si afferma che l'attività di interpretazione sul significato e sui limiti delle disposizioni europee effettuata dalla Corte di giustizia può avere un'efficacia diretta nell'ordinamento statale solo nei casi in cui non rimangano problemi concreti derivanti dalla discrezionalità lasciata agli operatori, dato che in tali situazioni vi sarebbe il rischio di addivenire ad un'applicazione difforme della normativa. Per la dottrina, si veda la posizione di L. Filippi, *La Grande Camera della Corte di giustizia U.E. boccia la disciplina italiana sui tabulati*, in "Penale Diritto e Procedura", 8 marzo 2021, laddove, dopo avere descritto l'effetto dirompente provocato dalla sentenza della Corte di giustizia, si afferma, letteralmente, che «le sentenze della Corte di giustizia U.E. non sono immediatamente operanti nell'ordinamento interno, giacché esse incidono soltanto sugli atti dell'Unione, a norma dell'art. 267 T.F.U.E». Sul tema anche F. Vecchio, *L'ingloriosa fine della direttiva Data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in "Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna", 2014, n. 4, pp. 212-220. E ancora, C. Parodi, *Tabulati telefonici: la Suprema Corte si esprime dopo le indicazioni della CGUE*, in "il penalista.it", 5 agosto 2021.

[25]Un differente orientamento ritiene invero che il pubblico ministero soddisfi il requisito richiesto. Al riguardo, per la giurisprudenza, cfr. Trib. Milano, Sez.VII pen., ord. 22 aprile 2021, su questa pronuncia si veda V. Tondi, *La disciplina italiana in materia di data retention a seguito della sentenza della Corte di giustizia UE*, in "Sistema penale", 7 maggio 2021. La questione, peraltro, è da tempo oggetto di attenzione anche da parte della dottrina, tra cui, *ex plurimis*, A. Camon, *Le intercettazioni nel processo penale*, Giuffrè, 1996, p. 109; nonché S. Scagliarini, *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni pro e alcuni contra*, cit., p. 882, in cui l'Autore, nel riferirsi alla definizione di autorità giudiziaria inclusa nell'art. 15 della Costituzione,

che appunto offre copertura alla tutela della segretezza anche dei dati di traffico, sostiene che «la stringente disciplina dell'art. 15 Cost., a nostro avviso più severa e restrittiva di quella comunitaria, sia pienamente soddisfatta dal decreto del Pubblico Ministero». *Contra*, v., a titolo indicativo, M. Viggiano, *«Navigazione» in Internet e acquisizione occulta di dati personali*, in "Il diritto dell'informazione e dell'informatica", 2007, n. 2, p. 380 ss., e R. Miranda, *Gli obblighi del gestore: esigenze di "data protection" o di "data retention"?*, in A. Pace, R. Zaccaria, G. De Minico (a cura di), "Mezzi di comunicazione e riservatezza", Jovene, 2008, p. 230 ss., che critica l'attribuzione di questa funzione al Pubblico Ministero in quanto organo privo della richiesta terzietà.

[26] Sentenza *H.K.* par. 50.

[27] Si veda l'ordinanza ingiunzione del Garante nei confronti di Tim S.p.A., 8 luglio 2021.

[28] Garante per la protezione dei dati personali, *Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, del 10 settembre 2021.

[29] *Ibidem*.

[30] Considerazione espressa in *Relazione su novità normativa*, cit., p. 5, nota 15.

[31] Vedi *supra*, par. 2.

[32] Se l'eliminazione di tale previsione è stata apprezzata da alcuni, in quanto ritenuta singolare per l'asserita introduzione di una convalida retroattiva o addirittura, più gravemente, per aver introdotto la retroattività di una legge penale procedurale (Cfr. G. Pestelli, *D.L. 132/2021: un discutibile e inutile aggravio*, in "il Quotidiano Giuridico", 4 ottobre 2021; C. Gittardi, *Sull'utilizzabilità dei dati di traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in "Giustizia Insieme", 7 ottobre 2021; per altri, la maggior parte a dire il vero, essa rappresentava uno strumento indispensabile, in assenza del quale, si sarebbe verificata una situazione a dir poco caotica ed incerta nelle aule giudiziarie (a tal proposito, per tutti, si veda L. Filippi, *La nuova disciplina dei tabulati: il commento a caldo del prof. Filippi*, in "Penale Diritto e Procedura", 1 ottobre 2021, p. 13).

[33] Cfr. *supra*, primo paragrafo.

[34] Ovvero alla necessità che i dati siano adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati, come previsto dall' art. 5 del Regolamento (UE) 2016/679.

[35] Cfr. G. Leo, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in "Sistema Penale", 31 maggio 2021, che a p. 5, specifica «È noto cioè che i tabulati possono contenere dati molto più interessanti del contenuto delle conversazioni» e ancora, «se l'inquirente deve accertare quanti contatti hanno avuto tra loro due persone determinate, perché deve essere acquisita la lista di tutti i rapporti intrattenuti dall'interessato, qualunque altra persona riguardino? E se serve la geolocalizzazione di un determinato apparecchio mobile, perché si deve conoscere l'identità degli interlocutori telefonici dell'interessato?».

[36] Cfr. A. Malacarne, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in "Sistema Penale", 8 ottobre 2021, in cui l'Autore afferma che «l'esigenza di non limitare l'alveo dei destinatari dell'apprensione dei dati esteriori esclusivamente a coloro che risultano indagati o imputati si giustifichi nell'ottica di consentire l'acquisizione degli stessi anche nei procedimenti contro ignoti».

[37] L. Filippi, *La nuova disciplina dei tabulati: il commento a caldo del prof. Filippi*, cit., p. 11.

* * *

Data retention and online privacy: towards regulation compliant with EU law?

Abstract: Law Decree n.132/2021, then converted into law with amendments, draws a line under the criticised discipline on the "Retention of traffic data for other purposes" in order to comply with European law on the protection of personal data, as well as with the CJEU's rulings on this matter. The new law has regulated the procedural aspects, providing for additional conditions for the acquisition of mobile and computer data traffic. With the present contribution we will discuss the considerable goals already achieved by the lawmaker, as well as those that, loudly, still require to be achieved. The discussion will take place with an eye toward the fair balance of rights and interests at stake, through a reinterpretation of the means of collecting the evidence in question, in the light of the new physiognomy it has assumed in the era of digitalization.

Keywords: Processing of personal data in the electronic communications sector – Data retention – Use of data in criminal proceedings as evidence

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0056
Articolo sottoposto a peer review

Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma

Giuseppe De Ruvo

L'articolo intende mostrare lo stretto legame che intercorre tra raccolta dati e sicurezza nazionale. L'obiettivo è quello di mostrare come la raccolta dati non sia solo importante per le operazioni commerciali e di profilazione delle grandi aziende digitali, perché essa è fondamentale anche per lo sviluppo dell'intelligenza artificiale in campo bellico. In questo senso, l'articolo mostra come l'intervento dello Stato – particolarmente negli USA – nel mercato dei dati abbia come principale obiettivo non quello di garantire la protezione dei dati dell'individuo, ma quello di instaurare un rapporto con le aziende in modo che i dati raccolti possano essere utilizzati per lo sviluppo dell'IA, in una prospettiva strategica e non meramente commerciale. In questo senso, primaria per gli USA è la protezione dei dati domestici per mezzo di limitazioni di mercato ad aziende cinesi, attraverso il *Committee on Foreign Investments in the US* (CFIUS) e lo *International Emergency Economic Powers Act* (IEEPA). Questa impostazione a somma zero dello spazio digitale rende estremamente difficile arrivare ad una data governance globale. In conclusione, analizzeremo il caso TikTok come esempio paradigmatico, dal momento che gli USA hanno consapevolmente deciso di utilizzare lo IEEPA in funzione anti-cinese, sebbene essi avrebbero potuto usarlo per generare un effetto domino in grado di innescare un circolo virtuoso che avrebbe potuto aprire la strada ad un effettivo processo di regolamentazione del flusso di dati. La conclusione principale di questo lavoro è che a rendere difficile il raggiungimento di una data governance globale sono le dinamiche geopolitiche, e non solamente l'opposizione delle grandi aziende a politiche di questo genere.

Intelligenza Artificiale – Raccolta dati – Sicurezza nazionale – Stati Uniti – Cina

Sommario: *1. Introduzione: la raccolta dati oltre la privacy – 2. Estrazione dati e sicurezza nazionale negli Stati Uniti: oltre il paradigma commerciale – 3. Sicurezza nazionale e interesse geopolitico: l'istituto del CFIUS – 4. L'algoritmo strategico di Tiktok e il capitalismo politico cinese – 5. L'interpretazione americana del caso TikTok: la guerra digitale a somma zero – 6.* Excursus. *Limiti e virtù della strategia europea: la normativa GDPR e l'effetto Bruxelles – 7. Conclusione. La strettoia americana: proteggere i dati dei cittadini o dominare il mondo?*

G. De Ruvo è laureato in Filosofia teoretica e geopolitica presso l'Università Vita-Salute del San Raffaele di Milano. Attualmente frequenta il master in Filosofia del digitale presso l'Università degli studi di Udine. Ha pubblicato articoli su *Limes – Rivista italiana di geopolitica*.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

1. Introduzione: la raccolta dati oltre la privacy

La ricerca intorno alla raccolta dati ha vissuto un impressionante sviluppo negli ultimi anni, in svariati campi. Da un punto di vista filosofico e sociologico, la letteratura è sostanzialmente unanime nel ritenere che, grazie alle nuove tecnologie digitali, si stia assistendo ad una vera e propria *mediatizzazione integrale del mondo della vita*, cioè del mondo di cui l'individuo fa ordinariamente esperienza[1]. Questo processo, oltre a dar luogo a dinamiche di potere descritte da autori come Couldry[2] e Zuboff[3], genera una vera e propria metamorfosi strutturale della nozione di *medium*: esso passa dall'essere – per l'appunto – il *mezzo* in grado di collegare differenti mondi della vita, *a essere esso stesso il mondo della vita comunemente esperito dai soggetti*. La tecnologia, dunque, passa dall'essere uno strumento per raggiungere un particolare fine all'essere l'ambiente che quotidianamente abitiamo. In questo senso, appare giustificato il neologismo coniato da Luciano Floridi, per il quale non ha più senso parlare, astrattamente, di una vita offline e di una online, poiché la nostra vita è sempre *onlife*: «non ha molto senso chiedersi se qualcuno è online o offline mentre guida seguendo le istruzioni del navigatore»[4]. Proprio per queste ragioni, la raccolta dati è divenuta pervasiva come non mai e, di conseguenza, il dibattito sulla protezione dei dati, sulla privacy e sulla data governance si è a sua volta sviluppato proporzionalmente[5]. Tuttavia, non è nostra intenzione, in questo articolo, entrare nel dibattito circa le diverse policy che sono state intraprese o che potrebbero essere intraprese. Nostro interesse è mostrare come la partita dei dati si giochi soprattutto a livello geopolitico, e come gli interessi geo-strategici delle grandi potenze digitali – oltre ad influenzare il loro approccio giuridico nei confronti di queste tematiche – rendano estremamente difficile arrivare ad una data governance trasparente che possa, dal canto suo, agire come forma di empowerment dei cittadini. Per fare ciò, dovremmo innanzitutto mostrare tre fattori: in primo luogo, lo strettissimo legame che intercorre tra le *big tech* della Silicon Valley e gli apparati governativi americani, illustrando come sia in atto un vero e proprio processo di fusione tra la sfera militare e la sfera civile anche nell'ambito del data mining; in secondo luogo, analizzeremo due istituti giuridici americani, il CFIUS (*Committee on Foreign Investments in the US*) e lo IEEPA (*International Emergency Economic Powers Act*), protagonisti della guerra digitale sino-americana, per mostrare in che termini si configura la sovranità tecnologica e la data governance in questo contesto; in terzo luogo, analizzeremo il caso TikTok, particolarmente istruttivo perché – come mostreremo – gli USA, davanti alla minaccia cinese di TikTok, hanno plasticamente mostrato il loro disinteresse a giungere ad una data governance concertata e condivisa dalla comunità internazionale, considerando anche il mondo digitale come un'arena a somma zero[6], mostrando quindi una continuità con la loro impostazione geopolitica post-guerra fredda. Usare come filo conduttore la politica americana è molto istruttivo, per due ordini di ragioni: in primo luogo, perché le più grandi aziende digitali – ad esclusione di ByteDance, proprietaria di TikTok –, che contribuiscono alla raccolta dati, sono americane e devono, in qualche forma, intrattenere dei rapporti con l'Amministrazione; rapporti che non sono sempre ottimi, ma che sono l'impalcatura decisiva di quello che è stato chiamato "capitalismo politico" americano[7]; in secondo luogo, è decisivo studiare *ora* il caso americano, perché gli USA stanno completando – in questi anni – una transizione decisiva. Nel 1982 – in pieno reaganismo e al crepuscolo dell'URSS – il Presidente della *Federal Communications Commission* aveva una linea molto chiara: appaltare la gestione della privacy ad aziende private[8]. Ciò ha contribuito a creare, per le grandi piattaforme del Web, quello che Zuboff ha denominato "habitat neoliberista", nel quale esse potessero muoversi nella raccolta dati senza eccessivi intoppi legislativi[9]. Tuttavia, questa stagione politica sta venendo meno. Eric Schmidt – ex CEO di Google e ad ora uomo centrale nell'amministrazione Biden per quanto riguarda i temi del digitale e dell'innovazione tecnologica[10] –, in un lungo articolo per il New York Times, invoca un intervento del governo «in grado di creare innovazione, di guidare l'impresa privata e rinnovare la leadership americana»[11]. Per Schmidt, il Governo deve intervenire donando alla raccolta dati una direzione strategica, slegandola da mere dinamiche di mercato. Gli USA stanno andando proprio verso questa direzione e, dunque, anche i loro strumenti giuridici stanno venendo utilizzati in tal senso, cercando di perseguire i *loro* obiettivi strategici, piuttosto che lavorare per arrivare ad una data governance globale[12]. La raccolta e l'uso dei dati, come vedremo, non hanno rilevanza solo per il singolo e per la sua sfera di riservatezza, ma pongono delle vere e proprie minacce alla sicurezza nazionale, che non si limitano alle – seppur presenti – attività di *hacking*, poiché, come già notava Rodotà «il caratterizzarsi della nostra organizzazione sociale sempre più come società basata sull'accumulazione e la circolazione delle informazioni comporta la nascita di una vera e propria nuova "risorsa" di base, alla quale si collega lo stabilirsi di nuove situazioni di potere»[13].

I dati come risorse di base, dunque. Ma risorse di che genere? Rispondendo a questa domanda, capiremo anche perché essi sono considerati materia di sicurezza nazionale.

2. Estrazione dati e sicurezza nazionale negli Stati Uniti: oltre il paradigma commerciale

Buona parte della letteratura si concentra soprattutto su come la raccolta dati invada la sfera di riservatezza del singolo, acquisendo informazioni su di esso con un consenso che a volte non è pienamente consapevole[14]. Affrontando il problema in questi termini, le operazioni di sorveglianza e di data mining vengono tuttavia intese da un punto di vista strettamente commerciale, concentrandosi in particolare sui dati estratti dalle grandi piattaforme a scopo pubblicitario[15]: la raccolta dati, infatti, permette alle aziende di identificare e conoscere meglio i consumatori, in modo da poter fornire servizi di advertising personalizzati. Non bisogna sottovalutare la pervasività di questa nuova forma di capitalismo: quello che Zuboff ha chiamato capitalismo della sorveglianza, infatti, non semplicemente genera plusvalore attraverso la raccolta dati, ma riorganizza – nel contesto delle mediatizzazione del mondo della vita – l'esperienza vissuta degli individui, generando tutta una serie di problemi psicologici e politici che, ampiamente discussi[16], noi non tematizzeremo. Non li tematizzeremo perché scopo di questo articolo è mostrare che il motivo principale per cui non si è ancora giunti ad una data governance globale non è solamente l'opposizione delle *big tech* a policy di questo genere, quanto – soprattutto – la rilevanza, per gli Stati Uniti, della raccolta dati per lo sviluppo dell'intelligenza artificiale in campo bellico. Negli ultimi anni, infatti, gli USA si sono scoperti in pericoloso ritardo rispetto alla Cina in questa nuova corsa agli armamenti[17]. Questo ritardo è dovuto a numerosi fattori: in primo luogo, Internet ha conosciuto il suo grande sviluppo nel momento *unipolare* degli USA, dopo la caduta dell'URSS e prima dell'ascesa della Cina: «la coincidenza tra la fine della guerra fredda e l'avvento di Internet è largamente interpretata come il trionfo della società aperta»[18]. Ancora nel 2016, diversi studiosi mostravano – a ragione – come i report governativi toccassero soltanto di sfuggita il problema delle *Lethal Autonomous Weapons* (LAWs), sottolineando soprattutto «gli irrisolti dilemmi etici»[19] ad esse collegati. In secondo luogo, come nota Eric Schmidt nell'articolo precedentemente citato[20], gli USA hanno sottovalutato la capacità cinese di innovare autonomamente, convinti che essi fossero soltanto in grado di copiare le tecnologie a stelle e strisce. Ciò ha portato i decisori americani a non considerare la rete come un asset strategico, ma come una mera protesi commerciale. In questo senso, la raccolta dati che le *big tech* portavano avanti serviva ad aumentare i loro profitti, e non veniva conferita ad essa una rilevanza strategica, se non come forma di *soft power*[21]. La situazione è drasticamente cambiata quando si è scoperta la possibilità di utilizzare l'intelligenza artificiale in campo bellico, con la costruzione di armi estremamente precise ed indipendenti da qualsiasi controllo umano[22]. Come scrive il Generale Fabio Mini, infatti, «in campo militare si sta passando dal controllo sulle forze con il miglior equipaggiamento al controllo della migliore *informazione* e *informatizzazione* che consentono di pianificare in fretta, coordinare ed attaccare con precisione»[23].

Per capire l'importanza dei dati in questo campo, basta intendersi su come funziona – in linea di massima – l'intelligenza artificiale: le nuove tecnologie dell'intelligenza artificiale e del *machine learning*, infatti, non si limitano ad applicare regole precostituite, ma ricavano da sé regole e soluzioni. Il "carburante", però, sono proprio i dati: il sistema riceve dall'esterno una grande quantità di dati grezzi, ma esso è capace di generalizzazione, che naturalmente diventa più precisa aumentando la quantità di dati che vengono immessi nel sistema. Per ottenere il primato nelle tecnologie emergenti dell'intelligenza artificiale – anche in campo bellico – *conditio sine qua non* è possedere una banca dati enorme, per volume e varietà. Non basta, tuttavia, che questi dati siano presenti: essi devono essere anche integrati, ovvero devono essere racchiusi in un cloud, nel quale questi possano interagire[24]. Tuttavia, gli americani – proprio a causa di una protratta percezione unipolare di sé e dello spazio geopolitico – non si erano mai posti il problema di integrare l'enorme mole di dati che possedevano e che le grandi aziende del digitale andavano raccogliendo: il loro obiettivo era semplicemente quello di legare a sé i satelliti cavalcandone il consumismo. È a questa sfida che si è dedicato il *China Strategy Group*, presieduto da Eric Schmidt, che ha prodotto un report fondamentale per capire la direzione che gli USA stanno prendendo. La proposta fondamentale che il report porta avanti è quella di integrare le conoscenze, il know-how e i dati che sono presenti, seppure in maniera diffusa, nelle varie sfere della società. Il settore privato – Schmidt, fondatore di Google, ne è consapevole probabilmente più di chiunque altro – ha certamente dati e know-how superiori rispetto alla comunità dell'intelligence, in particolare nella capacità di estrarre e aggregare i dati. Questo, però,

non significa che la politica di innovazione tecnologica debba essere lasciata nelle mani della Silicon Valley. Al contrario, «c'è bisogno di aggregare [*marshalling*]»[25] questi dati e questo know-how, creando un «National S&T Analysis Center (NSTAC)»[26], gestito dal dipartimento della difesa. Il NSTAC dovrebbe configurarsi come una agenzia pubblica in grado di creare una condivisione di dati, di tecnologie e di know-how tra agenzie federali ed aziende private – attraverso modalità di lavoro *open source* nei settori strategici – in modo da mettere a sistema il patrimonio di dati che, al momento, è diffuso nei vari meandri della burocrazia (pubblica e privata) americana, così da produrre «dei piani di investimento a lungo termine per le autorità federali»[27]. Gli americani, dunque, sono consapevoli del ritardo accumulato nei confronti dei cinesi, i quali, anche per la loro organizzazione statuale[28], da sempre riescono ad integrare un'enorme mole di dati, che estraggono attraverso piattaforme come WeChat, che copre, in un'unica app, le funzionalità dei maggiori social media occidentali[29]. Se, dunque, il ritardo nella raccolta dati americana rispetto a quella cinese mette il Celeste Impero nella condizione di sviluppare in maniera più efficace l'intelligenza artificiale in campo bellico, è evidente che questa diventa, per gli USA, una tematica che tira in ballo la sicurezza nazionale. Anche perché la raccolta dati cinese non sembra volersi fermare in Asia e in Africa, ma sembra aver preso di mira anche il Nuovo ed il Vecchio Continente.

3. Sicurezza nazionale e interesse geopolitico: l'istituto del CFIUS

È sulla base di questa minaccia alla sicurezza nazionale che interviene, sempre più spesso, il *Committee on Foreign Investments in the US* (CFIUS). L'analisi di questo istituto è decisiva per comprendere come, in realtà, a rendere estremamente difficile una data governance globale non siano soltanto le congiunture geopolitiche, ma anche la natura delle istituzioni giuridiche che negli USA intervengono in questo contesto. Il CFIUS nasce negli anni '50, ma diventa centrale nelle dinamiche internazionali negli anni '70 e '80 in un'altra guerra tecnologica: quella tra Giappone e Stati Uniti inerente ai semiconduttori[30]. In quella congiuntura, il CFIUS, ha bloccato l'acquisizione di Fairchild Semiconductor da parte di Fujitsu, non permettendo al Giappone di superare gli USA nella *semiconductor race*. I poteri del CFIUS sono stati rafforzati, nel 1988, dall'Exon-Florio *amendment*, che permette al Presidente, tramite un *executive order*, di bloccare, sulla base di un'indagine del CFIUS, qualsiasi fusione o acquisizione straniera che possa mettere a rischio la sicurezza nazionale[31]. Il CFIUS, dunque, è un istituto che serve a *proteggere* gli interessi geo-economici americani. Come funziona, però, da un punto di vista procedurale? Quando un'azienda straniera decide di fare degli investimenti negli USA, essa è tenuta ad informare il CFIUS. Inizialmente si apre un dibattito informale tra le aziende e il CFIUS. Se la situazione sembra essere rischiosa per la sicurezza nazionale – non significa necessariamente che ci sia dolo, ma soltanto che gli USA vogliono procedere con ulteriori verifiche – si apre la *National security review*. Questa, di solito, viene chiesta congiuntamente dall'azienda e dal CFIUS, ma quest'ultimo può anche richiederla *sua sponte* – tendenza che, in questa congiuntura, sta aumentando nei confronti degli investimenti cinesi[32]. Se gli USA nutrono ancora dei dubbi, possono aprire la *National security investigation*, obbligatoria per ogni infrastruttura critica, che si può concludere con un *executive order* del Presidente, in grado di bloccare qualsiasi operazione commerciale, se sussistono le criticità inerenti alla sicurezza nazionale, senza possibilità di appello da parte della controparte[33]. Il punto problematico, evidentemente, è la nozione di sicurezza nazionale: è possibile inquadrarla normativamente? Come si fa a definire "critica" un'infrastruttura? Proprio in questa direzione sono andati gli sforzi di diversi studiosi, che hanno cercato di delineare il perimetro di intervento del CFIUS, provando a definire positivamente quali asset fossero da considerare delle infrastrutture critiche. Il tentativo più autorevole è stato quello di Theodore Moran che, in uno studio intitolato *Three Threats: An Analytical Framework for the CFIUS Process*, pubblicato nell'agosto del 2009, ha cercato di circoscrivere il campo di intervento del CFIUS a tre tipi di minacce alla sicurezza nazionale: la minaccia energetica, per la quale gli USA rischierebbero di diventare dipendenti da un'altra nazione per quanto riguarda il proprio fabbisogno energetico; la minaccia dovuta ad un possibile furto di know-how in ambito tecnologico; la minaccia inerente alla possibilità di spionaggio industriale[34]. Se lo studio di Moran ha il merito di essere il più completo in assoluto, è evidente che questo framework normativo non è più adatto alla circostanza attuale, perché non tiene conto delle nuove forme di minaccia alla sicurezza nazionale. La sicurezza nazionale, dunque, diventa un concetto di difficile definizione normativa, perché essa non può essere definita *a priori*, ma dipende dalle contingenze geopolitiche e geoeconomiche. Se si pensa al caso di TikTok, è evidente che, se il CFIUS avesse seguito la *policy* descritta da Moran, esso, semplicemente, non sarebbe potuto intervenire: TikTok non

ha sottratto nessun bene energetico agli USA; non ha copiato nessuno e non ha alcuna intenzione di sabotare le aziende americane o di spiarle, dato che i suoi algoritmi sono semplicemente migliori. Eppure, TikTok – come vedremo – è effettivamente una minaccia alla sicurezza nazionale. Poiché il concetto di sicurezza nazionale evolve e si ridefinisce continuamente, sulla base delle nuove tecnologie e dei nuovi obiettivi geostrategici che le potenze cercano di perseguire, non è possibile definirlo una volta per tutte: «una definizione statica è impossibile e non è fornita dalla legge degli Stati Uniti, nemmeno dal *Defense Production Act* su cui si basa l'edificio normativo del CFIUS. [...] la sicurezza nazionale, per un impero, è ciò che esso vuole che sia per mantenersi»[35].

Dal momento che, come abbiamo mostrato nel precedente paragrafo, i dati sono da considerarsi a tutti gli effetti come un asset decisivo per la sicurezza nazionale data la loro rilevanza in campo bellico, le aziende straniere che li raccolgono – per operare negli USA – dovranno passare per un'istruttoria del CFIUS. Ma se il campo d'azione del CFIUS non risponde a principi normativi ben definiti, ma solamente alla nozione di sicurezza nazionale che viene di volta in volta ridefinita dai decisori politici sulla base delle esigenze geopolitiche, ne segue che – in questo contesto – la data governance diventa, per l'appunto, una questione di sicurezza nazionale, nella quale le esigenze geostrategiche delle grandi potenze sono prioritarie rispetto alle esigenze – e ai diritti – dei singoli individui. Gli stessi istituti giuridici di cui gli USA si servono – il CFIUS e, come vedremo, lo IEEPA – non sono in alcun modo disegnati per giungere ad una data governance realmente trasparente nei confronti degli utenti e, anche quando essi potrebbero essere utilizzati in tal senso, le potenze geopolitiche preferiscono farne un uso geo-strategico, riflettendo la loro visione a somma zero dell'arena tecnologica. Il punto fondamentale è il seguente: non sono le dinamiche di mercato o la potenza delle *big tech* ad ostacolare la transizione verso una data governance globale e concertata, ma sono le esigenze geopolitiche delle grandi potenze – in particolare degli USA – legittimate attraverso la nozione di sicurezza nazionale. Analizziamo ora il caso TikTok, nel quale queste pratiche appaiono evidenti.

4. L'algoritmo strategico di Tiktok e il capitalismo politico cinese

TikTok è una vera creatura della Cina contemporanea, fin dalla sua nascita. Esso diventa il colosso che conosciamo con l'acquisto da parte di ByteDance di Musical.ly nel 2017. Musical.ly era un'azienda cinese con sede a San Francisco, e la fusione non è stata casuale: nel 2015, infatti, il Partito Comunista Cinese ha rilasciato *China 2025*, il piano decennale inerente alle nuove tecnologie, nel quale è esplicita la richiesta al settore privato di procedere con fusioni aziendali ed acquisizioni così da creare campioni nazionali in grado di rivaleggiare con le grandi aziende occidentali[36]. Tale piano ha avuto un incredibile successo e alcuni autori cinesi sostengono che – dopo il periodo "manifatturiero" targato Deng Xiaoping – l'economia della Cina di Xi Jinping – non più timoniere, come Mao, ma CEO della Cina[37] – sia oramai centrata e basata soprattutto sulle nuove tecnologie dell'informazione[38]. Il grande giorno della fusione è stato il 2 agosto 2018: Musical.ly sarebbe scomparso per sempre semplicemente aggiornando l'applicazione, e gli utenti si sarebbero ritrovati TikTok al suo posto, creando un colosso da 600 milioni di utenti. Analizzare le funzionalità tecniche di TikTok può essere molto importante per comprendere per quale motivo esso abbia destato tanta preoccupazione negli USA. Intanto, TikTok ha un pubblico giovanissimo, e ciò gli permette di entrare profondamente nel processo di formazione della personalità dei giovani utenti, favorendo la promozione di determinati contenuti[39]. Ma il fattore decisivo è l'algoritmo che ByteDance ha sviluppato perché, come nota Zhang, «nonostante sia pubblicamente considerata come una comunità di intrattenimento, il vero potere che rende TikTok fondamentale è la sua applicazione nell'intelligenza artificiale»[40]. TikTok è un laboratorio fondamentale per lo sviluppo dell'intelligenza artificiale cinese perché il suo algoritmo deve comportarsi in maniera più autonoma rispetto a quello di Instagram o di Facebook. Se su Instagram o Facebook gli utenti danno inizio alla loro azione di profilazione seguendo pagine o persone, su TikTok l'algoritmo deve fare tutto da solo, ovviamente coadiuvato dai *like*, ma senza ricevere dall'utente indicazioni precise. L'algoritmo di TikTok, inoltre, avendo a che fare con un pubblico di giovani, con gusti in rapida evoluzione, deve essere in grado di adattarsi repentinamente, cosa che invece Facebook e Instagram non riescono a fare, anzi, scoraggiano. L'algoritmo di Facebook ed Instagram è un algoritmo conservatore ed adattivo per consumatori, ha l'intenzione di migliorarsi solo per migliorare l'esperienza di consumo dell'utente, e qualsiasi cambiamento improvviso – dell'algoritmo o dell'utente – è aborrito: esso ci incastra «nei nostri gesti muti senza consentirci di modificarli»[41]. L'algoritmo di TikTok, al contrario, è un algoritmo che ha come fine lo sviluppo del *machine learning* e dell'intelligenza artificiale. Il cambiamento significa possibilità di sviluppo e di miglioramento: è un *algoritmo strategico* che deve

imparare costantemente, perché è lui a scegliere cosa l'utente deve vedere senza ricevere da esso indicazioni specifiche. Un tale algoritmo, dunque, gioca ad un livello di complessità maggiore di quello di Instagram e Facebook e quindi, quando raccoglie dati, ne raccoglie di migliori: raccoglie dati che sono già stati processati da meccanismi di *machine learning* e che possono essere immediatamente utilizzati da altre forme di intelligenza artificiale, come quella bellica. Era inevitabile che un'applicazione di questo genere – il cui legame con il Partito Comunista Cinese è evidente – finisse sotto la lente del CFIUS, che infatti ha aperto un'investigazione non appena ByteDance ha acquisito Musical.ly. L'investigazione è stata resa possibile dal fatto che Musical.ly avesse sede a San Francisco, e dunque l'investimento di ByteDance è stato considerato un investimento cinese in territorio americano. Il ragionamento americano, in questo contesto, è stato molto semplice. Dato che ByteDance è un'azienda cinese, essa è soggetta alla giurisdizione e alle pressioni cinesi. Questo non significa necessariamente che ByteDance sia controllata dal Partito Comunista Cinese, ma – come nota Mark Wu – nel sistema economico cinese «lo Stato apre dei canali informali, secondari, con le aziende private»[42], attraverso i quali si configura il "patto" che tiene in piedi il capitalismo politico cinese: il governo non interviene direttamente nelle dinamiche di mercato delle aziende private, che anzi si sviluppano sempre più rapidamente a scapito di quelle pubbliche[43], ma le aziende private – per operare in Cina – devono tenere presente che il loro interesse non può andare contro le linee guida del Partito Comunista Cinese e con gli interessi strategici del Celeste Impero[44]. In sintesi, le aziende private in Cina sono libere di operare e di fare profitto, ma «lo Stato richiede i contributi delle piattaforme per raggiungere obiettivi di governo»[45]. Data la consapevolezza di questa organizzazione politico-economica, per gli USA «ogni capacità cinese su larga scala di collezione ed analisi di dati degli utenti americani resterà sempre un pericolo»[46], e legittimerà l'intervento del CFIUS. Tuttavia, non sarà direttamente il CFIUS a chiedere il *ban* di TikTok, ma esso avverrà tramite IEEPA, e questo fatto, per quanto controverso, ci permetterà di intendere ancora meglio la postura americana nei confronti della data governance.

5. L'interpretazione americana del caso TikTok: la guerra digitale a somma zero

Per comprendere il caso TikTok e l'atteggiamento americano, è opportuno tornare nelle pagine del report curato da Schmidt. Davanti ad uno scenario in cui una tecnologia strategica è coinvolta, gli Stati Uniti devono decidere se intervenire sul mercato in base alla logica esemplificata dalla Figura 1.

Il procedimento è molto semplice: appurato che una piattaforma è strategicamente rilevante, i decisori politici devono capire se è possibile risolvere il problema «attraverso soluzioni tecniche e/o attraverso negoziati con l'azienda o il governo cinese»[47], oppure se ci si trova davanti ad una situazione «estremamente rischiosa, che presenta problemi che non possono essere tollerati o gestiti con successo»[48]. Ora, davanti ad una situazione del genere, il *China Strategy Group* propone uno spettro di policy di intensità crescente. La prima possibilità è quella di negoziare con il governo cinese, cercando di ottenere delle garanzie *soprattutto per quanto riguarda la crittografia e l'uso dei dati personali*. Le tattiche utilizzate per portare i cinesi a negoziare possono essere dei dazi, oppure una *Transaction Scrutinity* operata dal CFIUS. Sulla base delle indagini del CFIUS si può procedere, attraverso lo IEEPA, a «bloccare le transazioni e a congelare [*freeze*] gli asset in risposta ad una minaccia straordinaria»[49]. Di norma, in questi casi si apre una fase legale nella quale gli USA e la compagnia sottoposta a IEEPA cercano di raggiungere un accordo su alcuni punti come il crittaggio, la chiarezza della proprietà o la proprietà intellettuale. Qualora neanche ciò si rivelasse sufficiente, un'opzione per il governo americano è quella di richiedere alle aziende cinesi di adottare specifici requisiti tecnici, in particolare l'inserimento della crittografia *end-to-end*. Un'altra opzione è quella di chiedere alle aziende cinesi di rendere le piattaforme open access per continuare ad operare negli Stati Uniti. L'*extrema ratio* è rappresentata dal *ban*. Lo strumento chiave, in questo contesto, è lo IEEPA. Esso «può essere esercitato per affrontare una particolare e straordinaria minaccia [...] alla sicurezza nazionale, alla politica estera, o all'economia degli Stati Uniti»[50]. Il vantaggio dello IEEPA è la sua versatilità, perché lascia aperta una vasta gamma di opzioni ai decisori, che vanno dal blocco delle operazioni economiche del soggetto sottoposto a IEEPA, al congelamento delle operazioni commerciali per ulteriori verifiche. Lo IEEPA, inoltre, a differenza dell'*executive order* che deriva direttamente da un indagine del CFIUS, essendo fondato normativamente, è più aperto a possibili ricorsi, ed è quello che è avvenuto con TikTok. Rimane, ovviamente, il fatto che esso può essere utilizzato in condizioni di minaccia alla sicurezza nazionale, che come abbiamo visto è un concetto ai limiti dell'arbitrario. Utilizzare lo IEEPA, dunque, non significa necessariamente impedire che l'asset ad esso sottopo-

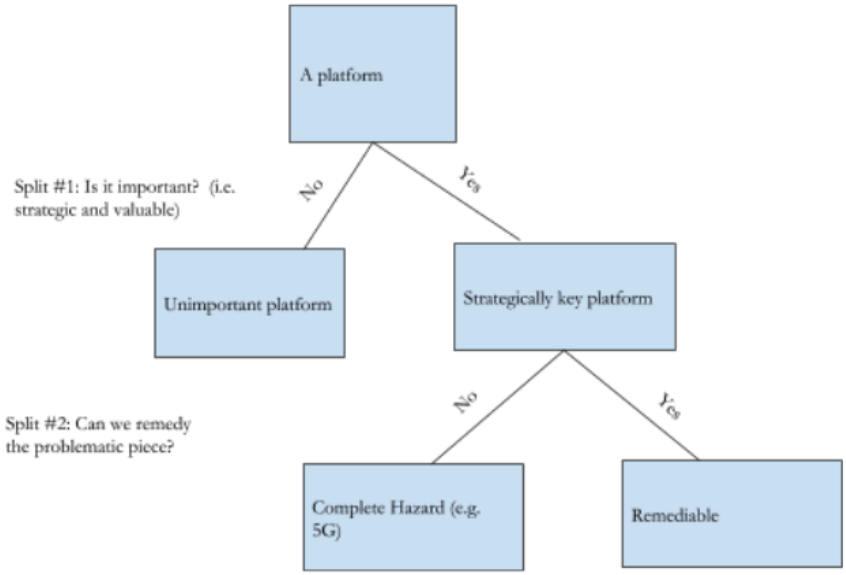

Figura 1: Fonte: China Strategy Group, *Asymmetric Competition: A Strategy for China & Technology*, 2020, p. 10.

sto possa continuare ad operare – nel momento in cui la controparte ricorre contro lo IEEPA, la piattaforma può infatti continuare ad operare fino a sentenza definitiva, ed è quello che è avvenuto con TikTok – ma esso può essere utilizzato come arma di deterrenza per raggiungere determinati obiettivi che lo stesso Eric Schmidt, come abbiamo mostrato, individuava nella possibilità di chiedere alle piattaforme cinesi – ma in generale di qualsiasi nazionalità – di rendere i propri server open access. Ciò significa che, attraverso lo IEEPA, gli USA sarebbero dotati di uno strumento in grado di promuovere una politica di trasparenza per quanto riguarda il flusso di dati. Da un punto di vista normativo, lo IEEPA – come mostrato da Schmidt – può congelare un asset fino a quando esso non rispetta le condizioni che gli USA dettano, e tra queste condizioni vi può essere la richiesta di rendere i server open access per continuare ad operare negli USA. Questa pratica, se applicata al caso TikTok, avrebbe potuto generare un precedente importante, che avrebbe potuto essere utilizzato anche – da altri paesi – nei confronti degli USA, obbligando le grandi potenze a giungere ad un accordo per non vedere – tutte – la propria raccolta dati compromessa. Tuttavia, non è così che gli USA hanno agito e non lo hanno fatto proprio per evitare un effetto domino di questo tipo. Piuttosto che chiedere ai cinesi di rendere i dati raccolti da TikTok open access, gli americani hanno direttamente bannato TikTok, ponendo come condizione che esso avrebbe potuto continuare ad operare *se e solo se fosse stato venduto ad un'azienda americana*. Tradotto: TikTok può continuare ad operare e ad estrarre dati, ma quei dati devono restare in America, perché servono per migliorare l'intelligenza artificiale a stelle e strisce, e non quella cinese. La protezione dei dati dei cittadini non è entrata minimamente nel ragionamento americano. È lo stesso Eric Schmidt, in un libro scritto insieme a Kissinger, a mettere nero su bianco questa intenzione americana: «Washington si è mossa per forzare la vendita di TikTok a un'azienda americana che potesse gestire i dati in patria, evitando che venissero esportati in Cina»[51]. Non è intenzione americana quella di giungere ad una data governance globale: strumenti come il CFIUS non sono disegnati per alcun tipo di multilateralismo, e strumenti come lo IEEPA – che pure potrebbero essere utilizzati in tal senso – vengono sfruttati, al contrario, come arma geoeconomica, nel tentativo di impossessarsi dello spazio economico digitale, piuttosto che per arrivare ad una sua regolamentazione.

6. *Excursus.* Limiti e virtù della strategia europea: la normativa GDPR e l'effetto Bruxelles

Se tra Cina e Stati Uniti la situazione conflittuale sembra rendere impossibile anche semplicemente pensare ad una normativa di protezione dati efficace, l'Unione Europea sembra muoversi in maniera diffe-

rente. La normativa GDPR – entrata ufficialmente in vigore nel 2016 – sembra infatti seguire una duplice direzione: da un lato, la creazione di un mercato comune di dati e di informazioni viene ritenuta strategica; dall'altro lato, viene ritenuta della massima importanza la costruzione di un'infrastruttura legale che possa – al contempo – garantire la *data protection* e stabilire regole chiare che i gestori di dati debbono seguire. La normativa GDPR ha forti radici europee, nella misura in cui trova il suo centro nevralgico nella nozione di accountability, che nel testo italiano è stata tradotta con *responsabilizzazione*. L'idea normativa alla base della GDPR è quella di evitare due estremi: da un lato, non viene considerato adeguato un approccio *top-down*, attraverso il quale l'autorità centrale imporrebbe positivamente una serie di obblighi specifici volti a regolamentare dall'alto le pratiche dei *data holders*; dall'altro lato, la GDPR rifiuta anche un approccio *bottom-up* di autoregolamentazione da parte dei gestori di dati. Il problema può essere espresso in questi termini: in un mondo sempre più mediatizzato, la raccolta dati ha dimensione strategica e quindi non può essere limitata eccessivamente. Tuttavia, la normativa GDPR tiene presente il fatto che «l'analisi dei dati personali è un'attività che può generare dei rischi»[52], e quindi non viene considerato normativamente adeguato lasciare ai *data holders* la possibilità di autoregolarsi. Da questa apparente aporia giuridica – per la quale né l'impostazione *top-down* né l'impostazione *bottom-up* sembrano funzionare – la normativa GDPR riesce ad uscire grazie al concetto di accountability, che non va inteso semplicemente come *responsabilità*, ma – come abbiamo accennato – come *processo di responsabilizzazione*, secondo una tradizione europea che, da Weber a Jonas, caratterizza l'approccio giuridico europeo[53]. La normativa GDPR, infatti, richiede ai soggetti che possiedono dati semplicemente 1) di prevenire i possibili fattori di rischio (attraverso *blockchain*, ad esempio); 2) di introdurre misure preventive (sia *by design* che *by default*) per evitare che si generino effetti indesiderati e, 3), di organizzarsi internamente affinché la sicurezza dei dati sia garantita (chiarezza della proprietà, distribuzione delle responsabilità legali). In questo senso, alcuni studiosi hanno parlato di un approccio *middle-out*, ovvero di una via di mezzo tra l'assoluto *laissez faire* e un interventismo pubblico troppo pesante. Il modello *middle-out* della GDPR, dunque, stabilisce certamente i principi che devono essere seguiti, e definisce anche con chiarezza i risultati che dovrebbero essere raggiunti per essere *accountable*, ma non stabilisce in alcun modo come ciò debba avvenire: «capire come raggiungere tali obiettivi, comunque, rimane prerogativa di chi controlla i dati»[54]. Le aziende che estraggono dati – se vogliono aprirsi al mercato europeo, che rimane fondamentale sia in termini di know-how che di consumo – devono adeguarsi alla normativa GDPR, e rendersi dunque accountable, così da «garantire una protezione preventiva dei dati personali, piuttosto che rimediare in seguito»[55]. La prospettiva europea, dunque, sembra essere effettivamente efficace nella protezione dati, e sembrerebbe anche essere geoeconomicamente strategica. Dato che il mercato dei dati europeo è estremamente ricco (di dati e di consumatori), le grandi aziende del Web non sembrano poterne fare a meno. Sulla base di questa consapevolezza, il GDPR rientra pienamente in quella strategia che è stata denominata *Brussels effect*: le normative europee tendono ad essere assimilate dagli altri attori perché nessuno può rinunciare ad intrattenere buoni rapporti (politici ed economici) con l'UE, e dunque, spesso, esse svolgono il ruolo di apripista verso un modello di *governance globale*[56]. La GDPR, tuttavia, non prevede – e non rientra neppure nelle sue prerogative – alcuna visione strategica per l'Europa, oltre al tentativo di agire come *benchmark* mondiale nella legislazione sulla *data protection*. In breve: la GDPR costituisce un ottimo strumento di tutela per i cittadini, ma – in una fase storica nella quale attorno all'intelligenza artificiale si sta generando una vera e propria corsa agli armamenti – non indica una prospettiva strategica e comunitaria per l'*uso* dei dati – che vengono sostanzialmente lasciati nelle mani dei *data holders* senza particolari restrizioni – scontando evidentemente l'assenza – o l'impossibilità[57] – di una politica estera comunitaria. È per questo che gli USA, nell'affrontare queste tematiche, tendono a non considerare l'UE come un'unica entità, ma a riferirsi ai singoli Stati membri, sfruttando quanto richiamato dal considerando 16 del Regolamento, che permette ai singoli Stati di non attuare la normativa se ad essere in ballo vi è la politica estera o la sicurezza nazionale. Su questa base, Eric Schmidt propone – in funzione anticinese – un'alleanza delle "tecno-democrazie" composta da singoli Stati europei che – riconoscendo la minaccia alla sicurezza nazionale dovuta allo sviluppo cinese – decidano di integrare i dati che vengono raccolti nel loro territorio con l'amministrazione americana, sostanzialmente aggirando la normativa GDPR[58]. Se dunque il tentativo europeo di garantire la *data protection* attraverso il *middle-out approach* rappresentato dalla GDPR sembra essere estremamente efficace dal punto di vista della regolamentazione, della tutela del cittadino e dell'*accountability*, esso – isolatamente – non riesce a rispondere alle sfide geopolitiche che l'aumento della tensione tra Cina e Stati Uniti gene-

ra e, in virtù del considerando 16 sopra citato, rischia di legittimare il *free-riding* di alcuni paesi sulla base della nozione di sicurezza nazionale e dell'interesse geopolitico che, come abbiamo più volte specificato, sono concetti ai limiti dell'arbitrario. L'Unione europea, dunque, necessiterebbe di una politica digitale estera comune che accompagni il GDPR, per evitare di rimanere incastrata nello scontro tra Cina e Stati Uniti, a cui torniamo adesso a volgere lo sguardo.

7. Conclusione. La strettoia americana: proteggere i dati dei cittadini o dominare il mondo?

Prima di diventare una delle voci più influenti dell'intelligence americana, Eric Schmidt era CEO di Google. Davanti alle prime accuse di furto di dati e di violazione della privacy, Schmidt si rivolse direttamente al Congresso americano, nel quale cominciavano ad alzarsi le prime voci contro quello che oggi chiamiamo capitalismo della sorveglianza, ammonendolo: «technology will move faster than governments, so don't legislate before you understand the consequences»[59]. Pronunciata dal CEO di una delle più grandi aziende del mondo, questa affermazione può apparire epifania di liberismo. Ma pronunciata dal direttore del *Defence Innovation Board*, questa frase assume tutt'altro significato. Se gli Stati Uniti procedessero a regolamentare il flusso di dati che le grandi aziende del digitale raccolgono, limitandone l'accesso alle *big tech* o introducendo dei paletti simili a quelli della GDPR, l'innovazione tecnologica americana subirebbe un clamoroso rallentamento che – nella lettura a somma zero americana – non potrebbe che lasciare spazio ai cinesi, pronti ad approfittarne per ottenere l'unico vantaggio bellico ad ora conseguibile. Il monito di Schmidt, dunque, va riletto in questo contesto e assume un senso completamente diverso, coerente con la sua nuova posizione di esperto di sicurezza nazionale: piuttosto che legiferare *contro* la raccolta dati, il governo americano deve lavorare per costruire *insieme* alle grandi aziende del digitale una partnership strategica che permetta agli Stati Uniti di giocare la partita della raccolta dati e dell'intelligenza artificiale con i cinesi ad armi pari, aggregando – sia da un punto di vista quantitativo, sia da un punto di vista infrastrutturale – i dati raccolti dalle *big tech* con quelli raccolti da agenzie federali come la *National Security Agency*[60], attraverso la creazione del NSTAC[61]. Schmidt presiede anche la *National Security Commission on Artificial Intelligence* (NSCAI), che ha recentemente rilasciato un report di oltre 700 pagine, in cui viene delineata la strategia americana sull'intelligenza artificiale. La competizione con la Cina, nota Schmidt, si fa crescente, e il Governo «è lontano dall'essere pronto per l'intelligenza artificiale»[62]. Da ciò segue che lo Stato deve sicuramente intervenire nei confronti delle grandi aziende digitali, ma di certo non per limitarne la raccolta dati: «il bisogno di migliorare la forza di computing e la necessità di grandi quantità di dati per migliorare gli algoritmi sono gli elementi che guidano l'innovazione. Il governo federale deve lavorare insieme alle aziende americane per mantenere la leadership americana e per supportare lo sviluppo di diverse applicazioni dell'intelligenza artificiale che possano portare avanti l'interesse nazionale nel senso più ampio possibile»[63].

La differenza con la GDPR è evidente: gli USA parlano di lavorare con le imprese per portare avanti l'interesse nazionale e qualsiasi riferimento all'*accountability* o alla protezione dei dati dei consumatori è qui rimosso. Da ciò segue, inevitabilmente, che gli strumenti giuridici debbano essere utilizzati secondo una logica strettamente geopolitica. Come nota Kai-Fu Lee, informatico taiwanese formatosi in America che ha guidato il non fortunato tentativo di Google di aprirsi al mercato cinese, «la Cina ha già superato gli Stati Uniti per quanto riguarda la quantità totale di dati che è in grado di trattare e produrre. Questa raccolta dati non è impressionante solo per la quantità, ma grazie allo straordinario ecosistema tecnologico cinese – un universo alternativo di prodotti e funzioni mai visti – questi dati sono fatti su misura per costruire aziende legate all'intelligenza artificiale»[64].

Per competere in questa arena, dunque, la prima cosa da fare è proteggere i propri dati, per evitare che essi finiscano nelle mani del nemico. In una congiuntura del genere, il dibattito sulla *data protection* e sul diritto alla riservatezza non può che passare in secondo piano, non perché meno importante, ma perché la pervasività delle nuove tecnologie e la loro rilevanza in campo bellico fa sì che «la dipendenza digitale in tutti gli aspetti della vita sta trasformando le vulnerabilità personali e commerciali in potenziali debolezze inerenti alla sicurezza nazionale»[65]. Negli Stati Uniti, dunque, l'alternativa non è tra privacy ed assenza di privacy, ma è tra *data protection* e autonomia geopolitica. Ma questa alternativa, negli USA, si traduce immediatamente nella scelta tra il garantire la *data protection* e la perdita della primazia mondiale: «l'intelligenza artificiale sta allargando la finestra di vulnerabilità nella quale gli USA sono già entrati»[66]. È evidente che questa, per un paese come gli USA, è una non scelta, perché perdere la corsa tecnologica contro la Cina significherebbe rischiare di rinunciare al rango imperiale, scadendo a numero due

sullo scacchiere delle potenze. È su questa base che i suoi istituti giuridici e le sue prassi politiche sono sempre rivolte verso la conservazione della sua primazia, mettendo tra parentesi la possibilità – peraltro osteggiata anche dai cinesi, in preda ad un *Nazionalismo Digitale*[67] – di giungere ad una effettiva data governance globale e condivisa, nella quale, al primo posto, vi sia il totale rispetto della sfera di riservatezza del singoli e la protezione dei loro dati attraverso pratiche *accountable*. Gli Stati Uniti, dall'alto della loro «città sulla collina»[68], si sono fino ad ora limitati a controllare il mondo, a spiarlo, vendendo i propri prodotti per sfogare il *surplus commerciale* e per generare *soft power*. Si tratta ora, davanti alla minaccia cinese, di difendere quella città, e gli abitanti – cittadini giustamente preoccupati per l'uso dei loro dati – e grandi aziende digitali dovranno collaborare perché, scrive Schmidt nella lettera che apre il suo report sull'intelligenza artificiale, il nostro «non è il tempo per criticare astrattamente la politica industriale»[69], nemmeno per la sua pervasività nella raccolta dati.

Note

[1]Cfr., almeno, A. Hepp, *Deep mediatization*, Routledge, 2020, 260 p.

[2]N. Couldry, *The costs of connection*, Stanford University Press, 2019, 323 p.

[3]S. Zuboff, *Il capitalismo della sorveglianza* (trad. it. P. Bassotti), LUISS University Press, 2019, 622 p.

[4]L. Floridi, *La quarta rivoluzione* (trad. it. M. Durante), Cortina, 2017, p. 48.

[5] Si veda, al riguardo, l'interessantissimo e recentissimo articolo di N. Hajli, F. Shirazi, M. Tajvidi, N. Huda, *Towards an Understanding of Privacy Management Architecure in Big Data: an Experimental Research*, in "British Journal of Management", 2021, n. 1, p. 548-565, nel quale gli autori mostrano empiricamente come l'infrastruttura dei principali *social* riesca ad acquisire informazioni degli utenti, svelandone le tattiche più recenti. Sul tema del diritto all'accesso ai dati personali, cfr., invece, R. Mahieu, *The right of access to personal data: a genealogy*, in "Technology and Regulation", 2021, n. 1, p. 62-75, nel quale l'autore analizza le diverse scuole di pensiero recuperando, in conclusione, la tesi esposta in S. Rodotà, *Tecnologie e diritti* a cura di G. Alpa, M.R. Marella, G. Marini, G. Resta, il Mulino, 2021, 528 p., secondo la quale il diritto d'accesso ai dati dovrebbe essere legittimato e considerato come una forma di bilanciamento dei poteri nei confronti di chi estrae informazioni, sottolineando dunque la dimensione pubblica e non meramente privatistica del tema della privacy.

[6]G. Rachmann, *Zero Sum World. Power and Prosperity After the Crush*, Atlantic Books, 2011, 352 p. Si veda anche D. Castro, M. Mclaughlin, E. Chivot,*Who is winning the AI race: China, the EU or the United States?*, Center for Data Innovation, 2019, p. 13: «in molti credono che non vi è competizione quando si ha a che fare con l'innovazione. In quest'ottica, ci sarebbero solo vincitori, e non vinti. Ma in realtà, ci saranno vincitori e vinti nella corsa mondiale all'intelligenza artificiale».

[7]A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, La Nave di Teseo, 2020, 509 p. Si veda anche, sugli ambigui rapporti tra *big tech* e Amministrazione americana, L. Mainoldi, *Washington e Silicon Valley non si amano ma spiano il mondo insieme* in "Limes. La rete a stelle e strisce", 2018, n. 10, pp. 53-62.

[8]A.F. Westin, *Home Information Systems: The Privacy Debate*, in "Datamation", 1982, n. 4, p. 112.

[9]S. Zuboff, *op. cit.*, pp. 47-50.

[10]Eric Schmidt, di simpatie dichiaratamente democratiche, presiede ad oggi il DIB (*Defence Innovation Board*) e il NSCAI (*National Security Commission on Artificial Intelligence*).

[11]E. Schmidt, *I Used To Run Google. Silicon Valley could Lose to China*, in "The New York Times", 27 February 2020.

[12]In questo senso, vi è una continuità con l'uso politico del diritto che sembra contraddistinguere la giurisprudenza americana, come notato da M.J. Horwitz, *La trasformazione del diritto americano. 1870-1960* (trad. it. M.R. Ferrarese), il Mulino, 2004, 504 p., con la differenza che ad essere al centro è, ora, la politica internazionale.

[13]S. Rodotà, *Tecnologie e Diritti*, cit., p. 35.

[14]Su questo, rimandiamo all'ottimo lavoro di N.S. Kim, D.A. Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consensus*, in "Missouri Law Review", vol. 80, 2015, n. 3, p. 725-770, che ha il merito di mostrare non solo le tecniche che le *big tech* usano per ottenere il consenso all'estrazione ed all'uso di dati, ma anche come la maggior parte delle persone sia molto più incline a fidarsi e ad accettare queste policy di quanto lo sia a lasciare i propri dati direttamente al Governo.

[15]Si veda il recentissimo lavoro di L. Balestrieri, *Le Piattaforme Mondo. L'egemonia dei nuovi signori dei media*, LUISS University Press, 2021, 200 p., nel quale l'autore mostra – sia quantitativamente che da un punto di vista operazionale – le strategie che le grandi piattaforme del Web seguono per aumentare i loro profitti attraverso il data mining e la cattura dell'attenzione, dando particolare rilievo alla transnazionalità dei nuovi media, che viene sfruttata per ottenere tutta una serie di vantaggi, sia politici che fiscali.

[16]La bibliografia è sterminata, si vedano almeno D. Palano, *Bubble Democracy. La fine del pubblico e la nuova polarizzazione*, Scholè, 2020, 224 p.; C. Sunstein, *#Republic. La democrazia ai tempi dei social media* (trad. it. A. Asioli), il Mulino, 2017, 337 p.; sui problemi psicologici, cfr. P. Wallace, *Psicologia di Internet* (trad. it. P. Ferri e S. Moriggi), Cortina, 2017, 542 p.; interessante anche il contributo di T. Cantelmi, *Tecnoliquidità. La psicologia ai tempi di internet: la mente tecnoliquida*, Edizioni San Paolo, 2013, 234 p.

[17]Si veda, D. Garcia, J. Haner, *The artificial intelligence arms race: trends and world leaders in autonomous weapons development*, in "Global Policy", 2019, n. 3, pp. 331-337.

[18]F. Balestrieri, L. Balestrieri, *Guerra Digitale*, LUISS University Press, 2019, p. 45.

[19]C. Cath, L. Floridi et al., *Artificial Intelligence and the "Good Society": the US, EU and UK approach*, in "Science and Engineering Ethics", 2018, n. 2, p. 511.

[20]Cfr., *supra*, nota 11.

[21]Su questo, decisivo è V. De Grazia, *L'Impero irresistibile. La società dei consumi americana alla conquista del mondo* (trad. it. L. Lamberti, A. Mazza), Einaudi, 2020, 621 p., dove viene mostrato chiaramente come la tendenza americana sia quella di ridurre gli alleati a satelliti attraverso l'imposizione di uno stile di vita consumistico ed economicistico, in grado di sopprimere qualsiasi velleità militarista e di autonomia geostrategica.

[22]Si veda, per una trattazione anche etico-morale, E. Schwarz, *Silicon Valley Goes to War: artificial intelligence, weapons systems and the de-skilled moral agent*, in "Philosophy Today", 2021, n. 3, pp. 549-569.

[23]F. Mini, *Che guerra sarà*, il Mulino, 2017, p. 130.

[24]Per un'introduzione al problema del *machine learning* e al suo funzionamento, cfr. P. Ferragina, F. Luccio, *Il pensiero computazionale. Dagli algoritmi al coding*, il Mulino, 2017, 247 p. Per la sua applicazione nell'IA, cfr. M.A. Boden, *L'Intelligenza Artificiale* (trad. it. D. Marconi), il Mulino, 2019, 188 p.

[25]China Strategy Group, *Asymmetric Competition: A Strategy for China & Technology*, 2020, p. 16 (traduzione mia).

[26]*Ibidem*.

[27]*Ibidem*.

[28]Su questo, si veda l'oramai classico, M. Wu, *The "China Inc." challenge to global trade governance*, in "Harvard International Law Journal", vol. 57, 2016, n. 2, pp. 261-324, in cui l'autore mostra approfonditamente i legami tra Stato, Partito ed aziende private. Traduzione sempre mia.

[29]A. Ghizzoni, G. Cuscito, *In Cina WeChat è Internet*, in "Limes. La rete a stelle e strisce", 2018, n. 10, pp. 161-164.

[30]Su questo si veda il classico testo di E. Vogel, *Japan as Number One. Lessons For America*, Harvard University Press, 2014, 288 p.

[31]Su questo, cfr. Congress of the USA, *AReview Of The CFIUS Process For Implementing The Exon-Florio Amendment*, ULAN Press, 2011, 196 p.

[32]Per un'analisi di questa tendenza, cfr. U. Khanapurkar, *CFIUS 2.0: An Instrument of American Economy Statecraft Targeting China*, in "Journal of current Chinese affairs", 2020, n. 1, p. 1-15.

[33]Per approfondire il funzionamento del CFIUS, si veda USA Treasury Department, *Guidance concerning the National Security Review conducted by CFIUS*, 73 Federal Register 74567, 8/12/2008. Si veda anche, per una lettura geopolitica dell'operato del CFIUS, A. Aresu, M. Negro, *La Geopolitica della Protezione. Investimenti e Sicurezza Nazionale: Gli Stati Uniti, L'Italia e L'UE*, Verso l'Europa, 2020, pp. 25-63.

[34]T.H. Moran, *Three Threats: An Analytical Framework for the CFIUS Process*, Peterson Institute for International Economics, 2009, 65 p.

[35]A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, cit., p. 371.

[36]Si veda H. Ma et al., *Strategic Plan of Made in China 2025 and Its Implementations*, in R. Brunet-Thornton, F. Martinez (eds.), "Analysing the Impacts of Industry 4.0 in Modern Business Environments", IGI Global, 2018, p. 1-23, dove il piano China 2025 viene paragonato alle politiche industriali degli altri attori globali.

[37]K. Brown, *CEO, China. The Rise of Xi Jinping*, I.B. Tauris, 2017, 262 p.

[38]Su questo, si veda S. Li, X. Xu, *Has "Internet Plus" effectively promoted the innovation of small and micro enterprises?*, in "Shandong Social Sciences", 2019, n. 2, p. 151-156.

[39]Su questo, si veda G. De Ruvo, *Geopolitica della bassezza: TikTok e la post-storicizzazione degli adolescenti americani*, in "Limes. La Riscoperta del futuro", 2021, n. 10, pp. 139-144.

[40]Z. Zhang, *Infrastructuralization of Tik Tok: transformation, power relationships, and platformization of video entertainment in China*, in "Media, Culture and Society", vol. 43, 2020, n. 2, p. 6. Traduzione sempre mia.

[41]T. Numerico, *Big data e algoritmi. Prospettive Critiche*, Carocci, 2021, p. 13.

[42]M. Wu, *op. cit.*, p. 265.

[43]Si veda, D. Xu, X. Wu, *From political power to personal wealth: Privatization and Elite opportunity in Post-Reform China* in "Journal of contemporary China", 2021, p. 993-1013.

[44]Ciò è stato plasticamente dimostrato dalla scomparsa di Jack Ma che – a capo di Ant Group e di Alibaba – aveva criticato il sistema bancario cinese. Si veda, G. Cuscito, *Messaggio per Alibaba: la Cina non sarà degli oligarchi digitali*, in "Cina, scontro tra Pechino e Alibaba - Limes", 17 dicembre 2020.

[45]Z. Zhang, *op. cit.*, p. 14

[46]A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, cit., p. 412.

[47]China Strategy Group, *Asymmetric Competition: A Strategy for China & Technology*, 2020, p. 10.

[48]*Ibidem*.

[49]*Ivi*, p. 13.

[50]US Code, *Unusual and extraordinary threat; declaration of national emergency; exercise of Presidential authorities*, title 50, chapter 35, section 1701.

[51]D. Huttenlocher, H.A. Kissinger, E. Schmidt, *The Age of AI and Our Human Future*, John Murray Publishers, 2021, p. 117. Traduzione mia.

[52]U. Pagallo, P. Casanovas, R. Madelin, *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*, in "The Theory and Practice of Legislation", 2019, n. 1, p. 9. Traduzione sempre mia.

[53]Si veda, H. Jonas, *Il principio responsabilità. Un'etica per la civiltà tecnologica* (trad. it. P.P. Portinaro), Einaudi, 2009, 322 p; M. Weber, *Il lavoro intellettuale come professione* (trad. it. M. Cacciari), Mondadori, 2018, 194 p.

[54]U. Pagallo, P. Casanovas, R. Madelin, *op. cit.*, p. 9.

[55]*Ivi*, p. 11.

[56]A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020, 424 p. Questa, tra l'altro, è la strategia che l'UE ha seguito nel negoziare gli accordi di Parigi. Cfr. R. Falkner, *The Paris Agreement and the new logic of international climate politics* in "International Affairs", 2016, n. 5, p. 1107-1125.

[57]Non entriamo nel merito della questione, che ci porterebbe troppo lontano, ma ci limitiamo a rimandare a P. Müller, K. Pomorska, P. Tonra, *The Domestic Challenge to EU Foreign Policy-Making: From Europeanisation to de-Europeanisation?*, in "Journal of European Integration", 2021, n. 5, pp. 519-534, dove gli autori fanno i conti con il principale ostacolo alla creazione di una politica estera comune: la divergenza di interessi geostrategici degli Stati membri.

[58]China Strategy Group, *op. cit.*, p. 25-27.

[59]Citato in BBC News, *Zuckerberg and Schmidt warn on over regulation of web*, 25 May 2011.

[60]Sulle operazioni di sorveglianza della NSA, J. Bamford, *L'orecchio di Dio. Anatomia e Storia della National Security Agency* (trad. it. R. Masini), Fazi Editore, 2004, 700 p.

[61]È su questa visione dell'IA che si sta consumando la rottura – interna all'establishment americano – tra Schmidt e Zuckerberg, nella misura in cui il fondatore di Facebook ritiene che il digitale debba essere usato per scopi meramente commerciali. Schmidt, invece, ritiene che il digitale ha una forte valenza strategica, e per questo motivo è anche critico nei confronti del Metaverso, che il fondatore di Google interpreta come un mondo digitale che potrebbe distrarre gli americani dal loro ruolo storico. Mi permetto di rimandare, su questo, a G. De Ruvo, *Il virus del Metaverso, se l'America fugge dall'inferno della storia* in "Limes. L'altro virus", 2022, n. 1, pp. 41-46.

[62]National Security Commission on Artificial Intelligence, *Final Report*, 2021, p. 2. Traduzione sempre mia.

[63]*Ivi*, p. 4.

[64]Kai-Fu Lee, *AI superpowers*, Houghton Mifflin Harcourt, 2018, p. 23.

[65]National Security Commission on Artificial Intelligence, *op. cit.*, p. 9.

[66]*Ivi*, p. 7.

[67]F. Schneider, *China's digital nationalism*, Oxford University Press, 2018, 320 p.

[68]Questa l'espressione con cui i padri fondatori si rivolgevano a loro stessi appena sbarcati dall'Inghilterra. Tale espressione ha origine in J. Whintrop, *Un modello di carità cristiana* (trad. it. C. Vergaro), Morlacchi, 2015, p. 47.

[69]National Security Commission on Artificial Intelligence, *op. cit.*, p. 4.

* * *

Data mining, artificial intelligence and national security: The geopolitical use of American legal infrastructure as an obstacle for a global data governance. The TikTok case as a paradigm

Abstract: This article aims to show the close link between data mining and national security. The aim is to show how data mining is not only important for big tech's commercial and profiling operations, because it is also critical to develop AI driven warfare. Thus, the article shows how the main goal of the State intervention – particularly in the US – in the data market is not guaranteeing the protection of the individual's data, but is establishing a close relationship with the companies so that the collected data can be used for the development of AI, in a strategic – and not merely commercial – perspective. In this sense, primary for the US is the protection of domestic data through market restrictions to Chinese companies, achieved throughout the intervention of the Committee on Foreign Investments in the US (CFIUS) and the use of the International Emergency Economic Powers Act (IEEPA). The paper claims that this zero-sum approach to the digital space makes the achievement of a global data governance extremely difficult. In conclusion, the paper analyzes the TikTok case as a paradigmatic example, since the US consciously decided to use the IEEPA in an anti-Chinese way, although they could have used it to generate a domino effect capable of triggering a virtuous circle that could have opened the way to an effective process of data regulation. The main conclusion of this paper is that it is because of geopolitical dynamics that the achievement of a global data governance is difficult, and not just because of corporates opposition to such policies.

Keywords: Artificial Intelligence – Data mining – National security – United States – China

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0065
Articolo sottoposto a peer review

The surge of non-fungible tokens and its implications for digital ownership from an Internet governance perspective

Amaury Trujillo

This work explores the recent rise of non-fungible tokens – and blockchain technology in general – which has brought into question traditional perceptions on property rights and decentralized organization in the digital age, with significant implications for the future of Internet Governance. To this end, the article starts with the story and evolution of non-fungible tokens within the context of blockchain technology. Particular attention is given to some of the events that happened in the year 2021 that triggered the surge of public interest in these tokens. Afterward, we touch upon current issues of digital ownership and non-fungible tokens, as well as the potential solution offered by distributed ledger technologies such as blockchain. Then, we comment on the main characteristics of blockchain regulation (primarily in Europe) and decentralized governance. Finally, we inquire into the current efforts and possible effects related to Internet Governance in terms of decentralization, taking into account all of the previous aspects.

Digital ownership – Blockchain – Decentralized autonomous organization – Web3

Summary: *1. Introduction – 2. The surge of non-fungible tokens – 3. Digital ownership – 4. Blockchain regulation and governance – 5. Towards decentralized Internet property – 6. Conclusion*

1. Introduction

A non-fungible token (NFT) is a unique identifier recorded in a distributed ledger (typically a blockchain) that could be used to certify the authenticity and ownership of both tangible and intangible assets. NFT applications have existed for several years now, but recently there has been a sudden increased interest due to several high-profile acquisitions of digital assets in, among others, the domains of arts, collectibles, gaming, and sports. This surge has in turn sparked a frenzy in NFT marketplaces, in which users transfer the ownership of digital objects, usually by means of cryptocurrency transactions, in what some observers call an *NFT rush* reminiscent of a gold fever[1]. Nevertheless, there remains much uncertainty regarding the legal recognition on this so-called *ownership* of digital assets via NFTs, as well as other related legal aspects such as regulation and governance. These issues are further exacerbated by the frenetic development of the underlying blockchain technology.

In essence, blockchain technology is an approach to implement a distributed ledger as a decentralized immutable list of records spread over a peer-to-peer network without the need of a trusted authority. It was first introduced in 2009 by a person or group of persons known by the pseudonym of Satoshi Nakamoto, along with Bitcoin[2] – the first successful decentralized electronic cash system based on cryptography. Since its introduction, blockchain has been perceived as a disruptive technology due to its poten-

A. Trujillo is researcher at the Institute of Informatics and Telematics of the National Research Council of Italy (IIT-CNR).
The paper is part of the Special issue "Internet governance and the challenges of digital transformation" edited by Laura Abba, Adriana Lazzaroni and Marina Pietrangelo.

tial to transform not only financial systems, but also society itself[3]. Internet Governance (IG) is a case in point. The Internet is commonly thought of as decentralized, albeit this is not really the case; it is better described as a sociotechnical system with distributed arrangements – both in terms of technology and governance[4]. Thus, it is not surprising that the decentralized sociotechnical constructs of the blockchain ecosystem, in terms of governance by the infrastructure (achieved via automated protocols) and governance of the infrastructure (managed by its community), have piqued the interest of IG scholars as a potential way to achieve better individual autonomy and collective self-organization for the Internet[5].

Today, distributed ledger technology (DLT) has diversified and many other implementations have sprung to tackle some of the shortcomings of Bitcoin, although blockchain technology continues to be by far the most commonly used approach. Arguably, the most successful of these alternatives is Ethereum, which was released in 2015 and became widely used thanks to the versatility of its smart contracts, i.e., transaction protocols that automatically execute, control, and document an agreement without the need of a trusted intermediator[6]. In fact, in Ethereum NFTs are implemented as smart contract interfaces that follow specific community standards called Ethereum Request for Comments (ERC), namely ERC-721 and ERC-1155[7]. Incidentally, this collaborative standardization system – common to the blockchain ecosystem – is inspired on the Request for Comments (RFC) of the Internet Engineering Task Force (IETF).

This work thus provides an overview of the NFT phenomenon and the regulation and governance of cryptoassets, with the hope of stimulating the debate concerning the implications for an Internet Governance that could go towards building a decentralized digital ownership.

2. The surge of non-fungible tokens

Non-fungible tokens represent units of data stored on a ledger that – unlike fungible tokens such as cryptocurrencies – are not mutually interchangeable, as each token is unique and distinct, and which can be associated with digital or real-world assets. The idea of creating unique tokens to represent assets on a blockchain emerged a few years after the release of Bitcoin, but due to the latter's design as a system of interchange of tokens (i.e., cryptocurrency), the first efforts were often rudimentary and did not gain widespread use[8]. It was thanks to the more generalizable smart contracts of Ethereum that NFTs gained traction. Even today, NFT marketplaces on the Ethereum blockchain, together with many cryptocurrencies, represent the majority of the cryptoasset ecosystem in terms of volume and value of transactions[9].

In particular, two crucial projects marked the dawn of NFTs on Ethereum: CryptoPunks and CryptoKitties. CryptoPunks are a limited edition of uniquely generated character images; the project was launched in 2017 and is the inspiration for ERC-721[10]. CryptoKitties, released later in the same year, is a marketplace for collectibles in the form of unique virtual cats that are algorithmically *bred*[11]. The project was among the first to adopt ERC-721, and it became so popular that it slowed down the Ethereum blockchain with its kitty-related transactions[12]. The project's popularity also reached mainstream media, increasing the public awareness on NFTs, albeit moderately. In fact, safe for a few instances, interest diminished in the following couple of years after the virtual kitty hype had subsided.

In the year 2021, however, there were several high-profile sales of digital assets across a wide range of sectors that significantly increased public interest on NFTs. Probably the sector of digital arts has been the most affected by the rise of NFTs[13], especially with the sale of the piece *Everydays: The first 5000 days* for US $69M by Beeple, pseudonym of digital artist Michael Winkelmann[14]. Relevant NFT sales in more mainstream sectors include a dunk highlight of basketball player LeBron James sold for US$200K within NBA's *Top Shot* marketplace[15], and rapper Eminem's sale of a collection of digital objects related to his musical career for US$1.8M[16]. Interestingly, several significant sales were also made on digital Internet memorabilia, such as the first ever tweet[17], the source code of the initial implementation of the World Wide Web[18], and the *Doge* meme figuring a bewildered Shiba dog[19].

Consequently many artists, businesses, and organizations in the realm of intellectual property started to pay more attention to the potential of NFTs as a source of revenue. Furthermore, the apparent ease with which individuals became rich overnight with NFTs attracted the collective imagination of laypeople; even teenagers with little to no professional experience seemed to be earning significant amounts of money through the sale of NFTs[20]. A prominent example is the case of twelve-year-old Benyamin Ahmed, who made more than £290K with his pixel art collection, called *Weird Whales*; one should not ignore, however, that his father is a professional software developer for financial institutions[21]. In addition, as the year advanced, more educational mate-

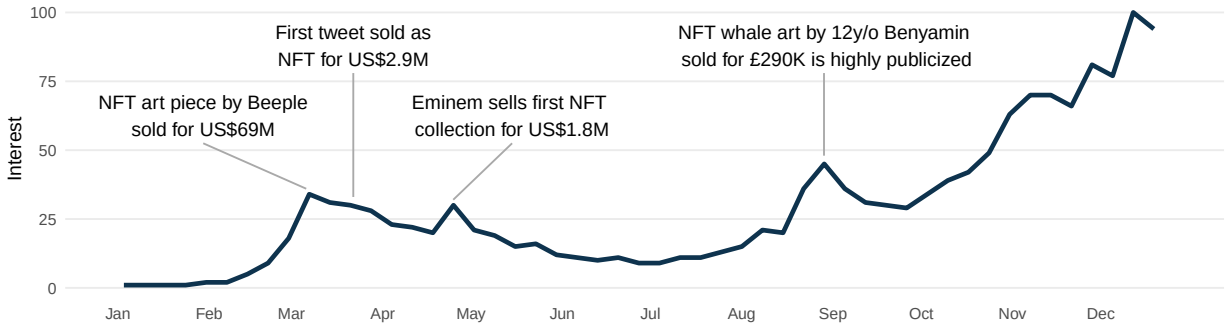

Figure 1: *Global search interest on the term* NFT *for the year 2021, according to Google Trends. Interest over time is scaled on a range of 0 to 100 (peak popularity for the term in the given period)*

rial on the subject, as well as various marketplaces and applications, were made available, further increasing the interest on NFTs by the general public. This growth can be clearly seen in the global trend of Google searches for the term *NFT* for the year 2021, as illustrated in Figure 1.

Not all interest is positive though. There are many detractors of NFTs, more so with how many nascent and established applications are plagued by software bugs, disappointing quality of service, and are fertile ground for abuse[22]. For example, Ubisoft, one of the most important videogame publishers in the world, met widespread backlash regarding the introduction of a NFT marketplace of in-game digital items, which was perceived as a cash grab and restrictive initiative[23]. Similar opinions are prevalent with regards to newcomer start-ups and established corporations that are heftily building marketplaces and other applications to take advantage of the rising interest and investments in NFTs.

Arguably, however, the world of arts is the most divided on the subject, in which despite the promises and eagerness of improved control and riches by and for artists, dissenting voices decry the nascent business practices and perceptions around NFT art[24]. There is for instance the preoccupation about the changing relations between digital and physical art with the legal ramifications of the sale of real-world art pieces as NFTs[25]. Above all, fundamental questions remain unanswered regarding the ownership of NFTs and the assets that they represent, as succinctly expressed by art historian D. Joselit: «The NFT is a social contract that values property over material experience. That contract can be broken»[26].

3. Digital ownership

Many buyers on NFT marketplaces are lured by the very promise of *owning* the assets these represent[27]. Ironically, at the present time the *ownership* of such assets, especially in digital form, is mostly intrinsic to the given DLT platform, and its recognition outside of this platform is not guaranteed[28]. Moreover, there is no general consensus on what is being owned after an NFT transaction: only the token itself, the token and the object it represents, both plus any related copyright, all or none of the above?[29] The answer to this question differs not only on a platform basis, but also case by case. In brief, at the moment of writing we are in a legal *no man's land* with respect to ownership and NFTs.

In very broad terms, ownership can be described as the set of exclusive rights over property, usually classified as tangible (e.g., real estate, chattel) or intangible (e.g., intellectual property, digital objects). In general, property rights are recognized as fundamental in most nations, with some form of property law being inscribed in the constitutional or charter texts of many jurisdictions[30]. The concept of ownership, however, has changed and continues to change over time according to the mores of society, e.g., owning persons as property, that is slavery, was once perfectly legal in most of the world, but nowadays is outlawed in every country; and technological innovations, e.g., digital media now allow perfect copies of works at almost zero cost. This last characteristic of digital objects is of prime importance[31], given that the concepts of rivalry (impossible simultaneous use) and scarcity (limited availability) applied to pre-digital kinds of property are less well-defined, which has caused much debate regarding the rights of buyers, creators, and distributors of digital assets, with the former often losing many expected privileges associated with ownership.

According to Perzanowski and Schultz, most efforts to limit ownership rights of buyers in the digital economy have been undertaken in the name of

reinforcing the intellectual property (IP) rights of creators, with the reasoning that this would provide better economic incentives for the creation of new inventions and works of expression[32]. The two most prominent examples of this phenomenon are the licensing of goods and digital rights management (DRM) technology. There is an increasing shift towards licensing digital content to the detriment of ownership, in which the creators (or most likely the distributors) of the content retain its rights, contrary to the expectation of most buyers. An infamous example involves the e-book reading platform Kindle of Amazon, in which books have been remotely deleted from users' devices, as Amazon states that its content is licensed, not sold, despite deceptive language on its platform such as buttons that show "Buy" or "Purchase"[33]. Concerning DRM, another infamous example is the installation of a piece of software by Sony with special privileges on the computers of buyers of its musical CDs – unbeknownst to them – in order to prevent copying, which became a scandal in terms of consumer security and privacy[34]. It is not wonder then that the NFT promise of true ownership of digital assets is alluring to most people, despite the current uncertainties.

Furthermore, DLT has also given rise to new interpretations on the very concept of property. For instance, a particularly thought-provoking interpretation by J.A.T. Fairfield considers property as pure information (e.g., who owns what, when, how, etc.); in other words, «property is the law of lists and ledgers»[35]. This property-as-information view contrasts with traditional property theory. In particular, it goes against the use of tangibility as a way to classify assets in legal contexts, building on the argument by J.M. Moringiello that such a classification places paramount importance on physicality and ignores general property principles, such as rivalry and scarcity, for which tangibility is frequently used in courts as a faulty proxy[36]. Instead, property law could be viewed as an information system that records transferable, scarce, rival, persistent and sharply delineated objects. For instance, Internet domain names – a core theme of IG – are an often-used example to illustrate the inadequacies of the traditional property language to digital assets: they are not scarce yet they are rivalrous.

This analogy goes well with the perception alluded before of DLT as a sociotechnical construct akin to a worldwide distributed and decentralized information system, in a similar vein as the Internet. And, by the same token, the novel governance approaches in the blockchain ecosystem are influencing and being influenced by current IG practices. Nevertheless, inadequate regulation risks being an obstacle for such digital governance transformation. That is not to say that governments around the world are ignoring the societal ramifications of DLT and cryptoassets in general, quite the contrary.

4. Blockchain regulation and governance

Several national and supranational governments have already begun to delineate or implement regulations on blockchain technology. For instance, the European Commission has started an initiative to create a legal and regulatory framework for blockchain technology, particularly in the context of financial applications[37]. In the United States, most of the regulation has been driven by the Securities and Exchange Commission (SEC), in particular with respect to the issue of deciding if cryptocurrencies are securities or not. In a landmark consideration, SEC chairman Jay Clayton stated at the end of 2017 that cryptocurrencies function as securities, thus these should be regulated as such[38]. This statement gave way to the recognition of cryptocurrencies as legal in the United States, but subject to more stringent regulations in line with other assets considered to be securities. Most other countries around the world implicitly or explicitly allow and tolerate the use of cryptocurrencies. Yet others, such as China, Russia, and Colombia, have taken a much more restrictive approach, explicitly deeming Bitcoin-like cryptocurrencies as illegal. And, at the other end of the spectrum, El Salvador, in a 2021 initiative that many experts consider highly risky, became the first country to recognize Bitcoin as legal tender[39].

Despite the many legal strategies and guidances adapted around the globe, most DLT regulation and government-backed initiatives have focused on fungible assets used as financial instruments. At the moment of writing there are fewer instances in which DLT is being regulated with respect to non-financial applications. For example, blockchain technology is explicitly mentioned as a key area for investment in the recently announced plan of the European Commission for digital transformation, called Path to the Digital Decade[40]. This plan also recognizes the potential of DLT for the future of a digital society, as demonstrated by the European Blockchain Services Infrastructure (EBSI) to deliver decentralized cross-border services for public administrators[41]. Nonetheless, at the moment of writing EBSI is still experimental and it only supports four use cases: identity, educational credentials, document traceability, and trusted data sharing for customs and tax authori-

ties. Tokenization of property via NFT or a similar mechanism is not yet within the scope of the project.

NFTs pose, however, related yet different legal conundrums which remain unresolved. In addition, the technology evolves so rapidly that the emerging regulations are already partially obsolete before they are even enacted. For instance, in September 2020 the EC published the final version of the impact assessment regarding a proposal for a regulation of markets in cryptoassets[42], in which there is no mention of the use of tokens as a means to manage property rights. As a matter of fact, the document recognizes that there is no official categorization of cryptoassets in use inside and outside the EU; moreover, the classification used therein does not take into account non-fungible cryptoassets.

Further complicating regulation of blockchain technology is the use and rapid evolution of a distributed and decentralized self-organization peculiar to the blockchain ecosystem. Such kind of organization is called a decentralized autonomous organization (DAO). In a DAO, a blockchain-based system enables people to coordinate and govern themselves by means of a set of self-executing rules (e.g., smart contracts) deployed on a public blockchain, effectively having a decentralized governance[43]. In this vision, there are two main governance structures: governance by the infrastructure and governance of the infrastructure[44]. The first, governance by the infrastructure, also called "on-chain" governance, refers to hard-coded rules embedded in a technological system (e.g., a blockchain), which includes both endogenous and exogenous rules that come from within or are imposed outside the reference community. The second, governance of the infrastructure, also called "off-chain" governance, refers to all the forces that subsist outside the technological system, but nevertheless influence its development and operations, with rules operating at the social or institutional level. These rules and procedures are not automatically executed, and a third-party authority might be necessary for enforcement or oversight. As with the first structure, there are rules of endogenous (e.g., social norms, customs) and exogenous (e.g., laws) nature. The concepts behind a DAO have also been identified on a more regulation-base perspective as two approaches called *Code of Law* (conventional law produced and enforced by national legal systems) and *Code as Law* (smart contracts on the blockchain)[45]. In either case, DAOs represent a novel approach for governance, which are starting to influence the governing approaches of many organizations, including IG.

5. Towards decentralized Internet property

The Internet Governance Forum (IGF), the main group for policy dialogue on governance of the Internet, has paid particular attention to blockchain technology for the last few years. In this regard, the IGF dynamic coalition on blockchain technology was born[46], and later consolidated as the Coalition of Automated Legal Applications (COALA)[47]. The coalition is comprised of leading academics, lawyers, economists, protocol architects, technologists, and entrepreneurs who work on blockchain-based legal and technical frameworks, standards and applications alongside governance policies that enable innovation and evolution of systems and networks. Indeed, P. De Filippi, one of the leading figures in blockchain governance and a founding member of COALA, «recommends that public and private institutions adopt some of the technological guarantees provided by blockchain technology to increase public confidence and trust. Governments can play a leading role in that regard, using regulation to promote the use of blockchain-based for regulatory compliance, and encourage the adoption of common global standards and shared international blockchain-based infrastructures for public services»[48].

COALA has published many documents regarding the impact of blockchain governance and the impact and regulation of DAOs. In addition, the coalition has also created a group that works on intellectual property, called COALA-IP, with the goal of establishing free, open, and easy-to-use methods of recording attribution and related metadata about works, assigning or licensing rights, mediating disputes, and authenticating claims by others[49]. This is a promising step forward in the autonomous management of IP in a decentralized manner, albeit IP does not comprehend all of property law. Besides, the coalition initiative started before the surge of NFTs. Nevertheless, these emerging solutions within the blockchain ecosystem will have a great influence on the future of property rights on the Internet. In fact, NFTs are already being used in new standards that implement a completely decentralized paradigm to some of the core technologies that both defined the Internet and gave way to IG.

Among these solutions we find two in particular: Ethereum Name Service (ENS) and the Interplanetary File System (IPFS). ENS complements and competes at the same time with the current Domain Name System (DNS). It allows to map the long cryptographic addresses of the accounts and smart contracts on the blockchain to more human-readable

names, and recently a compatibility with DNS was added to map traditional domain names in a decentralized manner within the Ethereum blockchain[50]. Users can buy and manage ENS domains as NFTs, which allows a decentralized ownership of the domains, as opposed to the more hierarchical and centralized nature of DNS. As with digital objects in other domains, NFTs for ENS domains have also been subject to an increased interest, with the unwelcome consequence of domain name squatting[51]. On the other hand, IPFS is a distributed and decentralized peer-to-peer hypermedia protocol[52]. It was created by Juan Benet, who is also a COALA contributor. It is the most common technology to store the asset associated with the NFT, which is embedded as a link address within the token metadata that points to a file on IPFS. Incidentally, ENS domains can point to IPFS addresses, which improves the usability and storage resilience of NFTs. Both are projects that follow a DAO approach for governance, and demonstrate how the current Internet could evolve to integrate a decentralized autonomous property system.

Furthermore, ENS and IPFS are also already functioning examples of the rapidly increasing digital token economy, which is converging toward what many people call Web3, a potential decentralized and token-based iteration of the Web[53]. In this vision, the retrospectively called Web 1.0 refers to an iteration in which most users were consumers of static-only content; Web 2.0 refers to a more participatory or social iteration, characterized by the emphasis in dynamic and user-generated content[54]; and Web3 would thus be an iteration based on DLT available to all users, who could not only consume and generate content, but also execute smart contracts on a peer-to-peer basis. Confusingly enough, the decentralized Web3 is distinct from the similarly named but older Web 3.0, an implementation of the semantic Web envisioned and promoted by Tim Berners-Lee since the beginning of the century[55]. The main idea behind the semantic Web is that data in it is described in a formal language, which can be processed by intelligent agent systems on behalf of humans.

It should be noted, however, that these "numeric versions" are just labels to describe a related set of changes within the Web ecosystem. Indeed, the Web could be described as an ever evolving set of technologies and practices to share information over the Internet. The dynamism touted in Web 2.0 is expected in most websites, but not necessary in many others; and several of the capabilities of the semantic Web are already available via standardized metadata and linked data, albeit its full potential has not been yet realized as originally envisioned. With regards to the decentralized Web3, we are starting to see the integration of token economics such as NFTs into some of the most mainstream social media platforms. A first example concerns Twitter, which now allows to set NFT profile pictures, distinguished by their hexagonal shape; however, these must be bought as ERC-721 and ERC-1155 tokens on marketplaces unrelated to Twitter[56]. A second and more adventurous example regards Reddit, which has started to sell NFT avatars called CryptoSnoos (Reddit's mascot is named Snoo), in collaboration with the OpenSea marketplace[57].

All of the above existing NFT functionalities offer a glimpse of decentralized Internet property. In the present, we can easily imagine a user that buys their CryptoSnoo avatar on Reddit, sets it as profile picture on Twitter, while also connecting their account on both platforms to an ENS domain pointing to their personal webpage hosted on IPFS; all of which gives the user the perception of *owning* their digital self-representation on the Internet. In the future, some scholars and enthusiasts imagine a much more immersive and intertwined digital ownership via NFTs in the so called Metaverse[58], an envisioned ecosystem of virtual reality worlds navigable via avatars[59]. Nevertheless, in order to realize such vision – even if only partially – many sociotechnical issues must be resolved, such as legal recognition and regulation, decentralized organization, and standards and protocols, just to name a few of those treated herein. Consequently, I believe that IG on the subject is of the utmost importance, and I hope that Internet stakeholders beyond COALA and the IGF in general will pay closer attention to its development.

6. Conclusion

Digital ownership is on the verge of a revolution with the arrival and surge of NFTs. However, at the present moment it is more likely that we are living in an NFT economic bubble that might burst in a not so distant future. My hope is that stakeholders on the realm of IG will be able to see beyond these hectic times and pay closer attention to the novel mechanisms and possibilities that a decentralized approach to digital property might entail. Who knows? Perhaps this is the way in which property will work in the much exalted and vilified future Metaverse... or not. In any case, what is certain is that the concept of ownership will continue to evolve with new technologies and changing mores, as NFTs attest, thus IG stakeholders must be prepared and aid in this transformation. In the end, this is but a small

contribution on the discussion regarding the subject, intended to stimulate more scholarly debate on these pressing issues.

Notes

[1]C. Thompson, *The Untold Story of the NFT Boom*, in "The New York Times Magazine", 2021.

[2]Given its profound impact, it should be noted that the original white paper by S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, is surprisingly brief at only nine pages (including code examples and references).

[3]L. Swartz, *Blockchain dreams: Imagining techno-economic alternatives after Bitcoin*, in M. Castells et al., "Another economy is possible: Culture and economy in a time of crisis", Polity, 2017.

[4]A.J. Mathew, *The myth of the decentralised internet*, in "Internet Policy Review", vol. 5, 2016, n. 3.

[5]P. De Filippi, B. Loveluck, *The invisible politics of bitcoin: governance crisis of a decentralized infrastructure*, in "Internet Policy Review", vol. 5, 2016, n. 3.

[6]For a comprehensive description of Ethereum, I recommend the book by A.M. Antonopoulos, G. Wood, *Mastering ethereum: building smart contracts and dapps*, O'reilly Media, 2018.

[7]The first blockchain NFT standard began as the Ethereum Improvement Proposal EIP-721, which was later accepted and specified as ERC-721. Incidentally, in ERC-721 an alternative name for a NFT is *deed*. However, this standard and previous standards were limited to a single token type, thus ERC-1155 was created to manage multiple token types in a single smart contract, be it fungible (ERC-20) or non-fungible tokens.

[8]Many consider *colored coins* to be the spiritual precursors of current NFTs. These are *marked* Bitcoin tokens that represent a real-world value asset. Due to the limitations of the Bitcoin scripting language, colored coins fell in disuse in favor of the more sophisticated NFTs.

[9]Ethereum NFT marketplaces also manifest high cointegration and significant causal short-run connections among themselves. See A. Lennart, *Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations*, 2021.

[10]Larva Labs, *CryptoPunks*.

[11]Dapper Labs, *CryptoKitties*.

[12]J.I. Wong, *The ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain*, Quartz Media, December 2017.

[13]R. McLaughlin, *'I went from having to borrow money to makink $4m in a day': how NFTs are shaking up the art world*, in "The Guardian", 6 November 2021.

[14]M. O'Brien, K. Chan, *How two friends made art history buying a $70M digital work*, Associated Press, 26 March 2021.

[15]C. Curtis, *An NBA Top Shot highlight of an epic LeBron James dunk just sold for $200K*, in "USA Today", February 2021.

[16]R. Daly, *Eminem makes £1.3million from first 'Shady Con' NFT collection*, NME, April 2021.

[17]J. Harper, *Jack Dorsey's first ever tweet sells for $2.9m*, in "BBC News", 23 March 2021.

[18]K. Knibbs, *What Tim Berners-Lee's $5M NFT Sale Means for Web History*, Wired Media Group, 30 June 2021.

[19]K. Rosenblatt, *Iconic 'Doge' meme NFT breaks record, selling for $4 million*, NBC News, 11 June 2021.

[20]S. Kurutz, *Teens Cash In on the NFT Art Boom*, in "The New York Times", August 2021.

[21]C. Moloney, *Boy, 12, makes £290,000 in non-fungible tokens with digital whale art*, in "The Guardian", August 2021.

[22]E. Ravenscraft, *The Metaverse Land Rush Is an Illusion*, Wired Media Group, December 2021.

[23]R. Browne, *Cash grab or innovation? The video game world is divided over NFTs*, CNBC, December 2021.

[24]L. Kluger, *Non-fungible tokens and the future of art*, in "Communications of the ACM", vol. 64, 2021, n. 9, p. 19-20.

[25]H. Lydiate, *Crypto Art Business*, in "Art Monthly", n. 447, 2021, p. 44.

[26]D. Joselit, *NFTs, or The Readymade Reversed*, MIT Presse, October 2021, p. 3-4.

[27]I. Akerman, *'It's like buying a star': Inside the bizarre, billionaires' world of NFTs*, in "Wired", 14 July 2021.

[28]For example, §6.D of the terms of use of CryptoKitties states «CryptoKitties are intangible digital assets that exist only by virtue of the ownership record maintained in the Ethereum network. All smart contracts are conducted and occur on the decentralized ledger within the Ethereum platform. We have no control over and make no guarantees or promises with respect to smart contracts.»

[29]A. Guadamuz, *The treachery of images: non-fungible tokens and copyright*, August 2021.

[30]B. Akkermans, *A comparative overview of European, US and South African constitutional property law*, in "European Property Law Journal", vol. 7, 2018, n. 1, p. 108-143.

[31]J.P. Liu, *Owning digital copies: Copyright law and the incidents of copy ownership*, in "William & Mary Law Review", vol. 42, 2000, n. 4, p. 1245-1366.

[32]A. Perzanowski, J. Schultz, *The end of ownership: Personal property in the digital economy*, MIT Press, 2016, p. 11.

[33]M. Seringhaus, *E-book transactions: Amazon Kindles the copy ownership debate*, in "Yale Journal of Law and Technology", vol. 12, 2009, n. 1, p. 147-207.

[34]E.W. Felten, J.A. Halderman, *Digital rights management, spyware, and security*, in "IEEE Security & Privacy", vol. 4, 2006, n. 1, p. 18-23.

[35]J.A.T. Fairfield, *BitProperty*, in "Southern California Law Review", vol. 88, 2015, n. 4, p. 805-874.

[36]J.M. Moringiello, *False Categories in Commercial Law: The (Ir) relevance of (In) tangibility*, in "Florida State University Law Review", vol. 35, 2007, n. 1, p. 199-165, §III B.

[37]European Commission, *Legal and regulatory framework for blockchain*, 2021.

[38]J. Clayton, *Statement on Cryptocurrencies and Initial Coin Offerings*, 11 December 2017.

[39]S. Pérez, C. Ostroff, *El Salvador Becomes First Country to Adopt Bitcoin as National Currency*, in "The Wall Street Journal", 7 September 2021.

[40]European Commission, *State of the Union: Commission proposes a Path to the Digital Decade to deliver the EU's digital transformation by 2030*, 15 September 2021.

[41]European Commission, *European Blockchain Services Infrastructure (EBSI)*, September 2021.

[42]European Commission, *Commission Staff Working Document Impact Assessment accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937*, September 2020.

[43]S. Hassan, P. De Filippi, *Decentralized Autonomous Organization*, in "Internet Policy Review", vol. 10, 2021, n. 2, p. 1-10.

[44]P. De Filippi, G. McMullen, *Governance of blockchain systems: Governance of and by Distributed Infrastructure*, Blockchain Research Institute and COALA, 2018.

[45]K. Yeung, *Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law*, in "The Modern Law Review", vol. 82, 2019, n. 2, p. 207-239.

[46] Internet Governance Forum, *Dynamic Coalition on Blockchain Technologies*.

[47] COALA, *Coalition of Automated Legal Applications*.

[48] P. De Filippi, *Blockchain Technology as an Instrument for Global Governance*, SciencesPo, 2021.

[49] COALA, *COALA Intellectual Property group*.

[50] ENS, *Ethereum Name Service*.

[51] K.T. Dugan, *There's a New Crypto Land Grab Going On*, in "New York Magazine", November 2021.

[52] IPFS, Interplanetary File System.

[53] For a layperson overview on the subject, see S. Voshmgir, *Token Economy: How the Web3 reinvents the Internet*, Token Kitchen, 2020.

[54] The term Web 2.0 was widely popularized by Tim O'Reilly and his eponymous publishing company in the second half of the 2000s, as a way to refer to emerging Web practices in the years following the dot-com bubble.

[55] T. Berners-Lee, J. Hendler, O. Lassila, *The semantic web*, in "Scientific american", vol. 284, 2001, n. 5, p. 34-43.

[56] At the moment of writing is possible set an NFT profile picture only from the iOS Twitter app, but the hexagonal profile picture is visible across all of the platforms.

[57] For more information see Reddit's CryptoSnoos.

[58] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, W. Cai, *Metaverse for social good: A university campus prototype*, Proceedings of the 29th ACM International Conference on Multimedia, 2021, p. 153-161.

[59] J.D.N. Dionisio, W.G. Burns, G. Richard, *3D virtual worlds and the metaverse: Current status and future possibilities*, in "ACM Computing Surveys (CSUR)", vol. 45, 2013, n. 3, p. 1-38.

* * *

La crescita degli NFT ("gettoni non fungibili") e le implicazioni per i diritti della proprietà digitale nel contesto della governance di Internet

Riassunto: Il presente lavoro esplora la recente crescita dei *gettoni non fungibili* (NFT, *non-fungible tokens*) – e della tecnologia blockchain in generale – che hanno messo in discussione la tradizionale percezione dei diritti di proprietà e l'organizzazione decentralizzata nell'era digitale, con rilevanti implicazioni sul futuro della governance di Internet. A tale scopo, il saggio inizia con l'esaminare la storia e l'evoluzione dei NFT nel contesto della tecnologia blockchain. Particolare attenzione è prestata ad alcuni dei più importanti eventi relativi agli NFT, verificatesi nell'anno 2021, che hanno provocato una vera e propria ondata di crescente interesse da parte dell'opinione pubblica e degli utenti. Il saggio prosegue con l'esaminare le questioni più importanti legate alla proprietà digitale e agli NFT, così come le potenziali soluzioni offerte dalle tecnologie dei registri distribuiti quale blockchain. Dopodiché, sono prese in esame le principali caratteristiche dell'attuale normativa sulla tecnologia blockchain (principalmente quella europea) e le nozioni di governance decentralizzata. Infine, sono esaminate le iniziative in corso e i possibili effetti della decentralizzazione sul futuro della governance di Internet prendendo in considerazione tutti gli aspetti analizzati.

Parole chiave: Proprietà digitale – Blockchain – Organizzazione autonoma decentralizzata – Web3

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0064
Articolo sottoposto a peer review

Moderazione automatizzata e discriminazione algoritmica: il caso dell'*hate speech*

Pietro Dunn

La necessità per gli intermediari digitali di moderare i contenuti pubblicati e diffusi in rete dagli utenti si è fatta negli anni sempre più pressante. A fronte della crescita vertiginosa del flusso informazionale digitale, peraltro, si è reso oggigiorno essenziale il ricorso a strumenti di moderazione algoritmica per la rilevazione dei contenuti da rimuovere. Anche la rilevazione dei discorsi d'odio (*hate speech*) si fonda attualmente su un utilizzo massiccio di sistemi di intelligenza artificiale e *machine-learning*: la letteratura, tuttavia, ha rilevato come tali sistemi siano sovente viziati da *bias* discriminatori che rendono particolarmente elevato il rischio di falsi positivi ai danni delle minoranze. Il presente contributo pone in luce come nel sistema costituzionale europeo il contrasto ai contenuti d'odio sia giustificato dall'esigenza di perseguire un'uguaglianza sostanziale di tutte le componenti sociali e come, pertanto, un'applicazione discriminatoria del divieto di *hate speech* sia in sé incoerente con il sistema di valori dell'Unione europea. Se, dunque, l'intelligenza artificiale rappresenta uno strumento essenziale e ineludibile per garantire un più sicuro e tollerante ecosistema digitale, un elevato margine di errore, in termini di falsi positivi, non risulta essere pienamente accettabile. Occorre, pertanto, un ripensamento delle strategie legislative nell'ottica di offrire più adeguate garanzie, sostanziali e procedurali, a tutela della libertà di espressione e del diritto di non discriminazione dei gruppi marginalizzati.

Moderazione automatica – *Hate speech* – Discriminazione algoritmica – Uguaglianza sostanziale – Libertà di espressione

Sommario: *1. Introduzione: il ruolo odierno della moderazione – 2. Moderazione algoritmica dei contenuti e rilevazione dei discorsi d'odio – 3. Margini di errore e* bias *discriminatori – 4. La moderazione dell'*hate speech *in un'ottica di uguaglianza sostanziale – 5. Conclusioni*

1. Introduzione: il ruolo odierno della moderazione

Le tecnologie digitali, e Internet in particolare, hanno permesso la diffusione di nuovi ed eccezionali strumenti per il godimento di diritti e libertà fondamentali. Nella ormai celebre sentenza *Reno v. ACLU* (1997)[1], la Corte Suprema degli Stati Uniti già segnalava e celebrava il ruolo della rete quale facilitatrice del "libero mercato delle idee", in piena sintonia con la storica interpretazione del Primo Emendamento resa dal giudice Holmes in *Abrams v. United States*[2]. Allo stesso tempo, il ciberspazio ha tuttavia dato adito a nuove sfide e nuovi pericoli[3], tant'è che,

P. Dunn è dottorando di ricerca in Law, Science and Technology presso l'Alma Mater Studiorum – Università di Bologna (CIRSFID-AI) e presso l'Università del Lussemburgo (FDEF).

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

nel vecchio continente, la Corte Europea dei Diritti dell'Uomo (Corte EDU) ha ripetutamente posto in luce gli accresciuti rischi legati alla società dell'informazione, concludendo che ciò possa giustificare un intervento più marcato degli Stati contraenti sulla libertà di espressione in rete[4].

Per fare ordine della caotica massa di informazioni caricate quotidianamente in Internet, nonché per ridurre la quantità di "mali informazionali" (*information bads*[5]), gli intermediari digitali hanno ben presto sviluppato strategie di moderazione dei contenuti sempre più complesse e raffinate[6]. Come posto in luce da Gillespie, nonostante gli intermediari abbiano a lungo cercato di presentarsi come fornitori di servizi (per lo più servizi di hosting) meramente neutrali, l'ideale di una piattaforma priva di alcun controllo rappresenta un'utopia[7]. Tutte le piattaforme moderano: anzi, la moderazione sarebbe da intendersi precipuamente quale prodotto stesso della piattaforma, in quanto rappresenterebbe in ultima istanza ciò che garantisce all'utente consumatore un'esperienza più o meno positiva della rete[8]. Essa è cioè parte integrante del pacchetto offerto dai social media[9].

D'altro canto, è proprio sulla moderazione privata operata dagli intermediari digitali che è andato crescendo il *focus* delle scelte legislative e politiche degli ultimi anni. Soprattutto a partire dalla seconda metà degli anni 2010, si è invero assistito a un sempre maggiore ricorso a tecniche di regolazione della libertà di espressione "di nuova scuola" (*new-school speech regulation*[10]). L'elemento caratteristico di queste nuove forme di regolazione è la scelta di intervenire non tanto attraverso l'imposizione di restrizioni e sanzioni che investano la libertà di espressione dei singoli individui quanto, piuttosto, attraverso la diretta regolazione delle infrastrutture digitali, attraverso l'elaborazione cioè di forme di responsabilità sussidiaria a carico dell'intermediario per la presenza e diffusione di contenuti illeciti generati da terzi[11]. L'Unione europea, tra gli altri, sembra avere intrapreso tale strada negli ultimi anni[12].

La diffusione di tali nuovi strategie di governance, unita a un'accresciuta sensibilità del pubblico, hanno spinto gli intermediari digitali a farsi maggiormente carico del loro ruolo di moderatori. Per far fronte, tuttavia, alla crescita esponenziale del traffico quotidiano di dati e informazioni in rete, l'utilizzo di sistemi di intelligenza artificiale (IA) ha acquisito un maggior rilievo anche in questo settore[13]. Il ricorso a strumenti automatici di decisione per la gestione dei contenuti in rete solleva peraltro una serie di perplessità con riferimento alla protezione e garanzia di diritti umani e valori costituzionali, ivi inclusi la libertà di espressione e informazione e il principio di non discriminazione. Ciò, soprattutto, appare evidente con riferimento alla moderazione dei discorsi d'odio (*hate speech*)[14].

Il presente contributo fornisce uno sguardo sul crescente ruolo dei sistemi di IA e *machine-learning* nell'ambito della rilevazione dei contenuti d'odio (paragrafo 2) e sull'impatto discriminatorio che tali strumenti possono avere sulla libertà di espressione dei gruppi minoritari e/o marginalizzati (paragrafo 3). Il paragrafo 4 argomenta come un'interpretazione del contrasto al fenomeno dell'*hate speech* in una prospettiva di uguaglianza sostanziale richieda un ripensamento altresì delle strategie legislative e di policy sul piano europeo.

2. Moderazione algoritmica dei contenuti e rilevazione dei discorsi d'odio

Secondo Grimmelmann[15], la moderazione dei contenuti rappresenta l'insieme di quei meccanismi di governance che strutturano la partecipazione a una comunità online, al fine di favorire la cooperazione tra gli utenti e prevenire la commissione di abusi. In senso lato, essa comprende due diversi aspetti. Il primo si riferisce alla rimozione dei contenuti contrari alle condizioni d'uso del servizio, nonché all'imposizione di sanzioni (ad esempio, la sospensione o cancellazione del profilo) a carico di chi li abbia postati: in tal senso, si può parlare di moderazione "in senso stretto" o di *hard moderation*[16].

Il secondo aspetto, invece, si riferisce all'organizzazione, distribuzione e disseminazione dei contenuti stessi, attraverso una loro gerarchizzazione atta a migliorare l'esperienza degli utenti. A questi sono offerti, infatti, i contenuti che più possano loro interessare: si parla, con riferimento a tale attività, di "cura dei contenuti" (*content curation*[17] o *soft moderation*[18]). La cura dei contenuti, che si basa generalmente sull'uso di sistemi automatizzati, quali i sistemi di raccomandazione, mirano a massimizzare l'engagement degli utenti[19] e, di conseguenza, i profitti del prestatore di servizi: la letteratura ha rilevato come ciò possa andare a discapito di importanti valori democratici, quali la protezione del pluralismo mediatico e di pensiero, alimentando da un lato la creazione di camere dell'eco e la polarizzazione del dibattito democratico e impattando dall'altro lato la capacità di diffusione dei contenuti prodotti da gruppi minoritari[20]. Nonostante tale significativo impatto della cura dei contenuti sull'ecosistema informazionale digitale, il *focus* del presente contributo

sarà posto in modo particolare sulla moderazione dei contenuti "in senso stretto".

Da un punto di vista pratico, le tecniche di moderazione possono adottare strategie differenti[21]. Una prima distinzione può essere fatta, sulla base del criterio temporale, tra moderazione *ex ante* e moderazione *ex post*, a seconda che il controllo venga esercitato prima o dopo la pubblicazione del contenuto. A sua volta, la moderazione ex post può essere proattiva, laddove l'intermediario si occupi attivamente di individuare i contenuti da rimuovere, o reattiva, quando invece si limiti a ricevere e valutare segnalazioni altrui (ad esempio, da parte di altri utenti del servizio).

Sotto un diverso profilo, la moderazione può essere operata da esseri umani (moderazione umana o manuale), da sistemi di IA (moderazione automatica o algoritmica) oppure attraverso una combinazione dei due (moderazione ibrida). In quest'ultimo caso, la funzione dei sistemi di IA è principalmente quella di operare una scrematura preventiva dei contenuti pubblicati dagli utenti e di rimettere al moderatore umano soltanto i casi più ambigui, istituendo tra l'altro un ordine di priorità rispetto all'ordine di revisione[22]. I sistemi ibridi hanno acquisito negli ultimi anni un rilievo sempre maggiore, soprattutto per le possibilità che gli strumenti di IA offrono agli intermediari di effettuare controlli su larghissima scala. Al tempo stesso, il ricorso all'algoritmo consente di ridurre l'esposizione dei moderatori umani a contenuti potenzialmente dannosi per il loro benessere psicofisico[23].

La ricerca relativa allo sviluppo, perfezionamento e aggiornamento dei sistemi automatizzati di moderazione si è dimostrata particolarmente feconda. Attualmente, gli intermediari digitali godono di una vasta gamma di strumenti algoritmici a loro disposizione, che possono essere variamente combinati a seconda della tipologia di *information bad* che si voglia filtrare e sulla base del formato (testuale, visuale, audiovisuale etc.) che si voglia analizzare[24]. Particolarmente diffusi e utilizzati sono, attualmente, i sistemi di *machine-learning* basati su reti neurali[25]: con riferimento a tali tecnologie, un terreno di ricerca particolarmente fertile risulta essere quello del *natural language processing* (NLP), ovverosia quella branca dell'informatica che si occupa di sviluppare le capacità delle macchine di analizzare contenuti testuali, con il fine specifico di trarre conclusioni in merito al significato del testo stesso[26].

L'utilizzo di sistemi automatizzati di moderazione è andato aumentando drasticamente negli ultimi anni e ha fatto uno straordinario balzo avanti a seguito dello scoppio della pandemia di COVID-19. Se infatti, da un lato, piattaforme e intermediari digitali sono entrati in uno "stato di emergenza"[27] durante la crisi sanitaria, a causa soprattutto dell'aumento preoccupante nella diffusione di *hate speech*[28] e fake news[29], dall'altro lato, le piattaforme hanno nei primi mesi dovuto sviluppare adeguati sistemi di IA per far fronte alla riduzione di manodopera umana disponibile derivante dalla necessità di porre in atto le adeguate misure di contenimento del contagio[30].

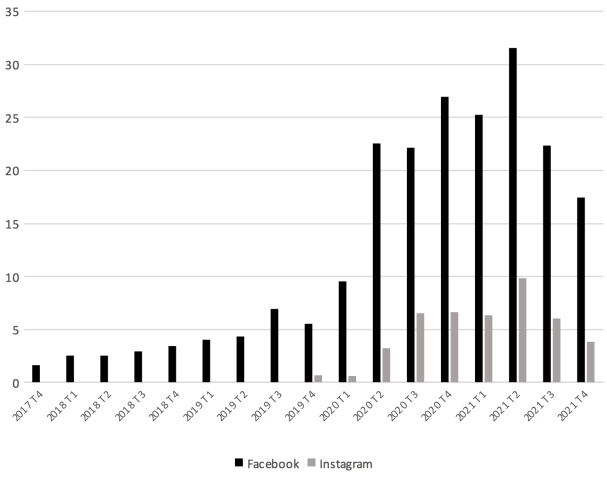

Figura 1: *Totale dei contenuti sanzionati da Instagram e Facebook come contenuti d'odio (in milioni)*

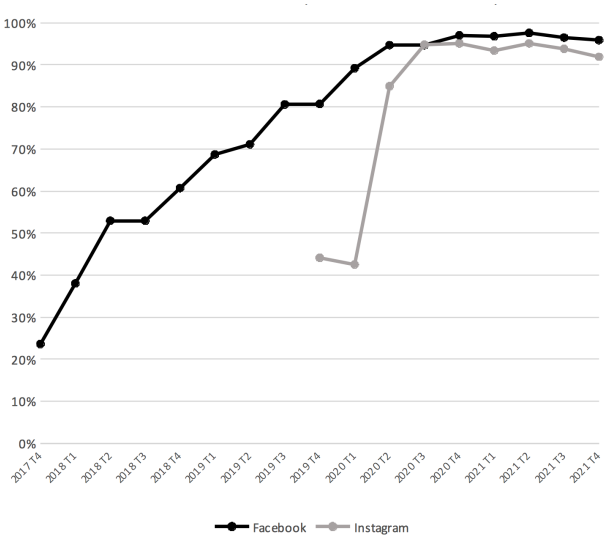

Figura 2: *Percentuale di contenuti d'odio rilevati tramite sistemi automatizzati sul totale dei contenuti d'odio*

I dati pubblicati da Facebook e Instagram nei loro report periodici sull'applicazione degli standard della comunità[31] confermano tali trend. Ciò emerge con particolare vigore con riferimento alla moderazione dei discorsi d'odio, sempre più automatizzata.

La Figura 1 mostra, in particolare, il numero di contenuti sanzionati, in quanto riconosciuti quali fattispecie di *hate speech* dalle piattaforme, nel periodo intercorrente tra l'ultimo trimestre del 2017 e il quarto trimestre del 2021, mentre la Figura 2 mostra, in percentuale, quanti di quei contenuti sono stati rilevati attraverso il ricorso a sistemi di intelligenza artificiale[32]. In tal senso, il numero di contenuti sanzionati da Facebook è aumentato vertiginosamente negli anni: un incremento particolarmente evidente si è avuto a seguito dello scoppio della pandemia, con un salto da 9,5 milioni di contenuti sanzionati nel primo trimestre del 2020 a 22,5 milioni nel trimestre successivo. In realtà, gli ultimi due trimestri del 2021 segnalano un'inversione di tendenza in tal senso, con una drastica riduzione dei numeri che, tuttavia, continuano tutt'ora a essere notevolmente più elevati rispetto all'epoca pre-pandemica[33].

Nel frattempo, un costante aumento si è avuto nell'utilizzo di sistemi di IA per la rilevazione di contenuti d'odio: infatti, se nell'ultimo trimestre del 2017 solo il 23,6% dei post non conformi al divieto di *hate speech* era rilevato proattivamente dagli algoritmi di Facebook, il dato è andato aumentando nel corso del tempo. Attualmente, i contenuti sanzionati dal social network in quanto ritenuti istiganti all'odio sono rilevati tramite sistemi automatizzati per il 96-97% circa. L'attuale CTO di Meta, Mike Schroepfer, ha celebrato questi risultati, sottolineando come l'utilizzo dei sistemi automatizzati di moderazione contribuisca a garantire un ecosistema digitale sicuro[34]. Del resto, secondo i dati pubblicati dalla stessa azienda, si è in effetti assistito a una diminuzione dallo 0,10-0,11% allo 0,03%[35] circa nel grado di "diffusione" di contenuti d'odio (ovverosia la percentuale stimata di visualizzazione di *hate speech* su tutti i contenuti visualizzati dagli utenti[36]).

Tuttavia, se è vero che l'avanzamento tecnologico nel settore rappresenta un fattore importante ed essenziale nella prospettiva di costruire un ciberspazio libero da intolleranze e violenze, è pur vero che le informazioni rese dal gruppo di Facebook rivelano un solo lato della medaglia. Come sottolineato in *Wired*, non è chiaro fino a che punto gli algoritmi di rilevazione dei discorsi d'odio siano andati effettivamente perfezionandosi[37]. Si tenga conto, in particolare, che i dati riportati sono meramente quantitativi: poco ci dicono sulla qualità delle scelte prese dai sistemi di IA o sulla percentuale di errori di rilevazione[38]. Tale ambiguità e opacità rispetto alla qualità e correttezza delle decisioni prese dall'algoritmo risultano essere particolarmente preoccupanti laddove si consideri il rischio di output discriminatori.

3. Margini di errore e *bias* discriminatori

Invero, i sistemi automatizzati di classificazione si basano su fondamenti statistico-probabilistici che, in quanto tali, rendono sempre inevitabile un più o meno elevato margine di errore. Gli errori, in particolare, possono tradursi in falsi negativi o in falsi positivi: se i primi minano l'efficacia di un sistema automatizzato di moderazione, i secondi possono invece essere dannosi per l'esercizio della libertà di espressione online degli utenti. Peraltro, le due tipologie di errore sono in generale inversamente proporzionali[39]: laddove, cioè, si implementi un sistema più "permissivo", vi sarà un rischio minore di falsi positivi a fronte di un maggior numero di contenuti illeciti, o contrari alle condizioni di utilizzo, rimasti impuniti; mentre un sistema più "severo" sarà, all'opposto, più difficilmente eludibile ma più probabilmente esposto al rischio di falsi positivi. In tal senso, il riferito incremento di contenuti sanzionati in quanto ricondotti alla sfera dell'*hate speech* da parte di sistemi di IA ha comportato (e comporta) un verosimile e proporzionale incremento nel numero di falsi positivi.

Se ciò è vero, l'implementazione di sistemi automatizzati di moderazione si traduce in sostanza in un bilanciamento tra due, talora contrastanti, esigenze: da un lato, la necessità di ridurre la diffusione di "mali informazionali"; dall'altro lato, l'esigenza di tutelare la libertà di espressione e il pluralismo di pensiero. Bilanciamento, peraltro, operato sempre più direttamente dalle piattaforme e dagli intermediari digitali. Se, dunque, la scelta di utilizzare tali sistemi richiede l'applicazione di un principio di proporzionalità che tenga conto di tali esigenze, il problema di fondo consiste nell'individuazione della soglia entro la quale il margine di errore (nel senso di falso positivo) sia da ritenersi "accettabile" a fronte del vantaggio sociale determinato dalla riduzione del grado di inquinamento dell'ecosistema informazionale digitale[40]. L'individuazione di tale soglia, tuttavia, può variare a seconda della tipologia di *information bad* che si voglia combattere. A tal proposito, con riferimento al fenomeno dei discorsi d'odio, alcuni fattori richiedono di essere tenuti in considerazione.

Un primo elemento di complicazione è determinato dalla nozione stessa di *hate speech*, tutt'altro che condivisa e ben definita[41]. A seconda della giurisdizione di riferimento, le condotte ascrivibili ai discorsi d'odio penalmente rilevanti possono variare notevolmente. Allo stesso modo, le piattaforme e gli intermediari digitali tendono a definire autonomamente il concetto di *hate speech* sanzionabile ai sensi dei loro termini e condizioni d'utilizzo: molto sovente, per di

più, le nozioni adottate da tali attori risultano essere notevolmente più ampie e aperte rispetto alle fattispecie considerate dai sistemi giuridici statali[42]. Il campo di applicazione di tali standard privati rischia in tal senso di risultare estremamente lato e, talora, pericolosamente indefinito.

Un secondo rilevante aspetto è dettato dal fatto che, come rilevato dalla giurisprudenza e dal dibattito internazionale, la possibilità di ascrivere una determinata forma espressiva alla classe dei discorsi d'odio è strettamente dipendente dalla ricostruzione del contesto all'interno della quale essa si inserisce. L'identità dell'autore e dei componenti dell'audience, per esempio, così come elementi contestuali quale il tempo e il luogo in cui un determinato contenuto sia stato pubblicato o condiviso, sono fattori potenzialmente dirimenti per comprendere lo scopo e i possibili effetti che una certa modalità espressiva può avere: tali fattori richiedono sempre un'attenta ricostruzione al fine di evitare eccessive e sproporzionate interferenze a danno della libertà di espressione individuale[43]. Eppure, ciò rappresenta una sfida rilevante per il moderatore algoritmico, in quanto le macchine, nonostante il loro straordinario potere computazionale[44] e la loro efficienza a livello di comprensione simbolico-sintattica, pongono ancora oggi dei problemi per quanto concerne la capacità di comprensione semantica[45]. È infatti difficile, per un sistema automatizzato, rilevare l'ironia o la satira nascoste dietro un particolare contenuto. Tra l'altro, tale compito è complicato notevolmente dalle modalità espressive caratteristiche della comunicazione in rete, le quali mescolano sovente elementi testuali, visivi e audiovisivi: si pensi, per esempio, ai cosiddetti "meme", contenuti multimodali che si caratterizzano per un'alta viralità e per il fatto di richiedere, ai fini della comprensione, una vera e propria "meme literacy" dell'audience[46].

Le difficoltà prodotte da tali sfide sono esse stesse alla base di quello che è il terzo fattore di complicazione. Come evidenziato da ormai consolidata letteratura, il margine di errore connesso all'utilizzo di sistemi automatizzati di rilevazione delle fattispecie di *hate speech* tende a impattare significativamente proprio sulle comunità tradizionalmente marginalizzate e discriminate[47]. Sempre più studi sono attualmente dediti alla ricerca di tecniche di *debiasing* dei moderatori automatici[48], ma il problema è ancora lungi dall'essere risolto.

Così, per esempio, si è da più parti rilevato come i contenuti pubblicati da membri della comunità afroamericana[49] o della comunità LGBTQIA+[50] siano maggiormente soggetti a subire sanzioni ingiustificate per violazione del divieto di *hate speech* o "*toxic*" *speech*. Le cause di tali risultati discriminatori sono plurime. Accade, per esempio, che i *dataset* utilizzati per allenare l'algoritmo non siano qualitativamente ottimali, soprattutto perché non rappresentativi del gergo e degli usi comunicativi tipici dei gruppi minoritari. In molti casi, i gruppi marginalizzati sviluppano la tendenza a utilizzare termini ed espressioni in sé stessi insultanti e discriminatori (si pensi alla *n-word*) con la doppia finalità, tuttavia, di riappropriarsi di tali termini svuotandoli della loro carica negativa (è questo il caso della parola *queer*, inizialmente utilizzata quale insulto per le persone LGBTQIA+ e facente oggi parte della sigla stessa) e di aiutare i membri della loro stessa comunità a "farsi la pelle dura"[51]. L'incapacità della macchina di cogliere tali sfumature di intenti e di significato rende così particolarmente elevato il rischio di falsi positivi, tant'è che, tra gli attivisti afro-americani, è rapidamente invalso il ricorso al neologismo "zucked" a indicare le frequenti sanzioni loro imposte dalle piattaforme di Meta ogniqualvolta essi pubblichino contenuti che discutano il tema del razzismo[52].

L'applicazione discriminatoria delle regole di una comunità online da parte dei sistemi di moderazione algoritmica è peraltro dettata altresì dagli stessi utenti. Nel 2016-2017, il genocidio e le persecuzioni a danno della comunità musulmana Rohingya in Myanmar sono stati incentivati, da un lato, dal fallimento da parte di Facebook nel ridurre effettivamente la diffusione di *hate speech* avente ad oggetto la minoranza, e, dall'altro lato, dalla ripetuta censura di contenuti di denuncia pubblicati da attivisti Rohingya: in effetti, come sottolineato da Suzor, in molti casi l'algoritmo della piattaforma teneva conto delle ripetute e numerose segnalazioni effettuate da utenti birmani, facenti parte della maggioranza, rispetto a tali contenuti[53].

Tali effetti si riscontrano, del resto, anche a livello di *content curation*: la letteratura ha sottolineato come l'architettura algoritmica delle piattaforme, incentrata a massimizzare l'engagement degli utenti della rete, tenda a premiare in termini di visibilità i contenuti pubblicati dalle categorie demografiche di maggioranza[54], relegando a spazi di nicchia o imponendo un vero e proprio *shadowban*[55] a carico dei gruppi marginalizzati.

4. La moderazione dell'*hate speech* in un'ottica di uguaglianza sostanziale

A fronte di tali rilievi, occorre chiedersi, anche in un'ottica normativa e di *policy-making*, se il margine di errore caratterizzante gli strumenti di moderazione automatizzata dei discorsi d'odio sia effetti-

vamente accettabile o meno a fronte della necessità di garantire agli utenti un ciberspazio maggiormente tollerante e sicuro. In tal senso, sembra essere ineludibile un riferimento all'ormai risalente dibattito concernente la domanda se sia o meno opportuno combattere il fenomeno dell'*hate speech* attraverso l'imposizione di restrizioni alla libertà di espressione, pur nella consapevolezza che tale dibattito non si è sviluppato negli anni con riferimento alla relazione intercorrente tra individuo e intermediario digitale (rapporto tra soggetti privati) ma, piuttosto, con riferimento a quella intercorrente tra persona fisica e istituzioni dello Stato (rapporto tra un soggetto privato e un soggetto pubblico).

Come è noto, il dibattito sulla punibilità dei discorsi d'odio ha condotto, in prospettiva comparata, a soluzioni ben diverse tra loro[56]. Così, se negli USA vige il primato del Primo Emendamento e della tutela del "libero mercato delle idee"[57], con la conseguenza che una normativa volta a limitare la diffusione di *hate speech* debba essere sottoposta a un severissimo scrutinio (*strict scrutiny*) di legittimità costituzionale, quasi sempre fatale[58], il vecchio continente ha dimostrato una ben maggiore apertura a simili restrizioni. Invero, a differenza del Primo Emendamento, sia l'art. 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) sia l'art. 11 della Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza) ammettono l'imposizione di restrizioni e limitazioni alla libertà d'espressione se previste dalla legge e se necessarie in una società democratica per il perseguimento di un fine legittimo, quale è, tra gli altri, la protezione della reputazione o dei diritti altrui[59].

La scelta di ostacolare, anche per mezzo del diritto, la diffusione dei discorsi d'odio può essere ascritta a una pluralità di ragioni tra loro complementari. In primo luogo, la proibizione e punibilità dell'*hate speech* rappresenta uno strumento per proteggere e tutelare gli individui appartenenti ad una classe discriminata dal perpetuarsi e aggravarsi degli episodi di discriminazione e violenza nei loro confronti. Se, come sottolineato dalla Commissione per l'eliminazione della discriminazione razziale (CERD), il discorso razzista e il discorso d'odio possono porre seri pericoli e rischi a medio-lungo termine[60], la loro limitazione rappresenta uno strumento essenziale per la riduzione di reati e illeciti di matrice discriminatoria: in tal senso, l'*hate speech* costituisce una condotta pericolosa in quanto potenzialmente capace di produrre conseguenze dannose per una società democratica[61].

In secondo luogo, è stato da più parti rilevato come l'atto del discorso d'odio sia in sé dannoso per l'integrità psicofisica dei suoi destinatari, nonché per l'esercizio dei loro diritti e delle loro libertà costituzionali. Secondo Matsuda, esponente della *critical race theory* statunitense, le vittime di *hate speech* e *hate propaganda* soffrono in percentuali più alte di sintomi e disturbi quali: sensazioni di panico; aumento del battito cardiaco; difficoltà respiratorie; incubi; disturbi da stress post-traumatico (PTSD); ipertensione; psicosi; suicidio[62]. In *Beizaras e Levickas c. Lituania*[63], la Corte EDU ha recentemente confermato che l'*hate speech*, relativo, nel caso di specie, all'orientamento sessuale dei ricorrenti, rappresenta in sé e per sé un attacco all'integrità fisica e mentale di coloro che ne sono i destinatari. Le vittime, inoltre, vengono attraverso l'*hate speech* ristrette nelle loro libertà, in quanto l'esigenza di sottrarsi a messaggi d'odio le porta a modificare le proprie abitudini di vita e, in molti casi, a rinunciare a esprimere le loro personali opinioni e idee[64]. In ultima istanza, come magistralmente posto in luce da Waldron[65], al cuore delle normative di contrasto al fenomeno in oggetto vi è la necessità di tutelare l'eguale dignità delle comunità vittime e dei singoli individui che ne fanno parte[66].

In altre parole, la regolazione delle espressioni d'odio è mossa sia dall'esigenza di contenere il rischio di ordine pubblico legato a un incremento dell'attività criminosa di matrice discriminatoria sia, soprattutto, da quella di garantire alle categorie "protette" la possibilità di esercitare liberamente i propri diritti e libertà in una condizione di uguaglianza rispetto al resto della popolazione. In questo senso, l'intervento normativo volto a ridurre la diffusione di *hate speech* rappresenta uno strumento volto ad affermare e concretizzare l'uguaglianza sostanziale, e non solo formale, dei gruppi demografici marginalizzati. Lo scopo dell'imposizione di limitazioni alla libertà di espressione per ridurre la diffusione di odio ha quindi come fine ultimo l'empowerment di quei soggetti che l'*hate speech* mira a colpire. Del resto, come sottolineato da Fredman, il perseguimento dell'uguaglianza sostanziale richiede esso stesso un approccio multidimensionale al fenomeno della discriminazione che implichi anche la garanzia che ai gruppi minoritari o comunque discriminati sia concesso partecipare attivamente alla vita comunitaria, pubblica e politica[67].

Se, dunque, la *ratio* ultima del contrasto ai discorsi d'odio è legata al perseguimento dell'uguaglianza sostanziale, anche nella sua dimensione partecipativa, appare evidente che, nel caso della moderazione automatizzata di *hate speech*, la soglia di accettabilità dell'errore, soprattutto se dettato da *bias* di carattere discriminatorio, debba essere particolarmente elevata. Un'applicazione inconsistente ed iniqua tradisce lo stesso spirito originario della moderazio-

ne dell'*hate speech*, svuotando tale attività del suo significato egualitario e rendendola, anzi, controproducente rispetto agli interessi della collettività. Tra l'altro, il silenziamento di quelle categorie di persone che costituiscono le vittime tipiche dei discorsi d'odio rischia di depotenziare fortemente il ruolo, ritenuto da più parti fondamentale, della controarrazione[68].

Per evitare tale cortocircuito, potenzialmente aggravato dal ricorso a tecniche di *new-school speech regulation*, appare pertanto auspicabile un ripensamento, da parte delle istituzioni europee, delle strategie politiche e legislative di settore. Ciò non tanto nell'ottica di una demonizzazione del moderatore algoritmico, il quale costituisce invece uno strumento essenziale e utilissimo per il contrasto all'*hate speech*[69], quanto piuttosto nella prospettiva, da un lato, di incentivare i programmatori di tali sistemi a tenere in adeguata considerazione le esigenze legate al rispetto dei principi dell'uguaglianza sostanziale[70] e, dall'altro lato, di fornire maggiori tutele individuali, sostanziali e soprattutto procedurali[71], a quegli utenti della rete che siano maggiormente esposti ai rischi della discriminazione algoritmica.

In realtà, la Commissione europea ha dato segno negli ultimi anni di una maggiore consapevolezza dei rischi per la libertà di espressione degli utenti che sono ineludibilmente legati a una più massiccia e generalizzata moderazione dei contenuti da parte degli intermediari digitali. Il Regolamento (UE) 2021/784[72] prevede per esempio all'art. 5 che un fornitore di servizi, il quale sia stato riconosciuto come esposto a contenuti terroristici, debba predisporre misure specifiche volte a contrastarne la diffusione: nell'applicare tali misure, tuttavia, il fornitore dovrà tenere pienamente conto dei diritti e degli interessi legittimi degli utilizzatori (ivi inclusa la libertà di espressione e di informazione) e, nel contempo, agire in maniera diligente e, soprattutto, non discriminatoria. È inoltre disposta, all'art. 10, la predisposizione di meccanismi di reclamo a tutela degli utenti i cui contenuti siano stati rimossi, con l'obbligo per il fornitore di rendere decisioni motivate e fatto salvo l'eventuale ricorso all'autorità amministrativa o giudiziaria dello Stato.

A sua volta, la proposta di regolamento per il *Digital Services Act* (DSA) contiene alcune norme di rilievo in tal senso, richiedendo all'art. 12 che gli intermediari applichino le condizioni generali dei loro servizi in modo «equo, trasparente, coerente, diligente, tempestivo, non arbitrario, non discriminatorio e proporzionato», nonché rispettoso dei diritti e degli interessi legittimi delle parti coinvolte (compresi i diritti fondamentali previsti dalla Carta di Nizza), nonché imponendo, alle piattaforme online, di predisporre sistemi interni di gestione dei reclami da attuarsi «in modo tempestivo, non discriminatorio, diligente e non arbitrario» (art. 17). In quest'ultimo caso, peraltro, si prevede espressamente che sia data la possibilità per gli utenti di contattare un interlocutore umano al momento della presentazione del reclamo e che la nuova decisione non possa essere presa solamente attraverso sistemi automatizzati: a tal fine, è fatto inoltre obbligo ai fornitori di servizi di dotarsi di personale qualificato. Dal testo approvato in prima lettura dal Parlamento europeo il 20 gennaio 2022[73] traspare tra l'altro una ancor maggiore consapevolezza del potenziale impatto del DSA sui diritti degli utenti: gli emendamenti proposti, per esempio, includono numerosi riferimenti al principio di non discriminazione.

Peraltro, si è da più parti rilevato come le soluzioni adottate rappresentino in ultima istanza poco più che petizioni di principio, in quanto sovente non corredate da un apparato applicativo e procedurale ben definito e sufficientemente sviluppato. Non è del tutto chiaro, per esempio, se l'art. 12 del DSA implichi la possibilità di opporre qualsiasi diritto ricompreso nella Carta di Nizza oppure soltanto quella ristretta cerchia di diritti per i quali la Corte di Giustizia dell'UE abbia dichiarato la sussistenza di un'efficacia orizzontale[74]. È stato, in generale, posto in luce come il sistema introdotto dal DSA incentiverebbe un ulteriore incremento nell'utilizzo su vasta scala di sistemi di moderazione automatizzati, senza tuttavia la previsione di adeguati rimedi a tutela dell'individuo[75].

Inoltre, se il DSA, pur nell'apprezzabilissima ottica di armonizzazione e riduzione della frammentarietà del quadro normativo sugli intermediari digitali, mira a introdurre una disciplina quadro generale e orizzontale, tale approccio, se non accompagnato da interventi normativi più specifici, ha tuttavia l'inevitabile effetto di appiattire le peculiarità tipiche connesse alla moderazione di ciascun *information bad*. Così, per quanto concerne la rimozione dei contenuti d'odio, non sembra essere presente, nell'attuale testo della proposta di regolamento, la consapevolezza dei rischi tipici, ai danni del principio di uguaglianza sostanziale, che sono inevitabilmente connessi alla rilevazione automatizzata dell'*hate speech*. Se, da un lato, la proposta di regolamento si preoccupa di tutelare i gruppi marginalizzati da contenuti dannosi quali l'"illecito incitamento all'odio" e i "contenuti discriminatori illegali"[76], non sufficiente attenzione è prestata al collaterale, ed altrettanto dannoso, rischio di un'iniqua rimozione degli stessi.

In una prospettiva normativa, risulta pertanto essenziale tenere in maggiore considerazione le specificità e le finalità tipiche del contrasto ai discorsi

d'odio, ovverosia l'uguaglianza sostanziale dei gruppi tradizionalmente marginalizzati e discriminati. Uno strumento promettente sembra essere stato introdotto, per esempio, dall'emendamento del Parlamento europeo volto a introdurre un paragrafo 1-*bis* all'art. 19. Se nel testo originario della Commissione la figura del "segnalatore attendibile" rilevava soltanto ai fini della premoderazione dei contenuti[77], il nuovo testo richiederebbe alle piattaforme online di adottare le misure, tecniche e organizzative, atte a permettere ai segnalatori attendibili di emettere notifiche di rettifica in caso di errore di moderazione: tali notifiche, volte al ripristino di informazioni e contenuti, dovranno essere trattate e decise in via prioritaria e senza indugio. In altre parole, si darebbe la possibilità a segnalatori attendibili, indipendenti ed esperti in materie quali, per l'appunto, il contrasto al fenomeno dei discorsi d'odio, di corroborare le richieste di correzione delle decisioni prese dalla piattaforma. Peraltro, allo stato attuale non risulta chiaro se, quando e con quali modalità sarà possibile per gli utenti richiedere direttamente un simile intervento del segnalatore attendibile.

5. Conclusioni

Il costante incremento del flusso informativo in rete ha reso sempre più essenziale il ruolo degli intermediari digitali nella moderazione dei contenuti postati dagli utenti, al fine di ridurre la commissione di condotte illecite e la diffusione di materiali dannosi o illeciti in Internet. La necessità di tale attività si evince del resto dal crescente numero di iniziative politiche e legislative da parte delle istituzioni pubbliche, nazionali e sovranazionali, volte a delineare sistemi di *new-school speech regulation*. A fronte, tuttavia, della mole straordinaria di contenuti postati quotidianamente online, il ricorso da parte degli intermediari digitali a forme di moderazione automatizzata si è fatto negli anni massiccio.

Sebbene tali sistemi siano sempre più avanzati e raffinati, il loro utilizzo non è esente da criticità: un certo margine di errore è, di fatto, ineludibile. Ciò risulta essere particolarmente evidente in quei casi ove la rilevazione del "male informazionale" si fondi sulla comprensione semantica del contesto e dell'intenzione dell'autore del contenuto, quale è il caso dei discorsi d'odio. In questi casi, come evidenziato da ampia letteratura, risulta particolarmente elevato il rischio di falsi positivi, soprattutto a carico delle minoranze e dei gruppi marginalizzati o discriminati. Il concreto e significativo rischio che la moderazione automatizzata di *hate speech* si traduca in un silenziamento delle categorie discriminate, piuttosto che in una loro tutela, implica la necessaria pretesa di una più esigente soglia di accettabilità dell'errore. In caso contrario, la moderazione dei contenuti d'odio si svuoterebbe di significato, tradendo la *ratio* di fondo che ne giustifica il contrasto: la promozione del principio di uguaglianza sostanziale.

Sotto il profilo di *policy-making*, risulta pertanto auspicabile da parte del legislatore, nazionale ma soprattutto eurounionale, una maggiore attenzione ai rischi "collaterali" connessi a un quadro normativo che incentivi la moderazione (algoritmica) dei discorsi d'odio senza garantire al contempo un apparato adeguato di tutela delle libertà individuali e del diritto di non discriminazione degli utenti. Tale esigenza appare ancor più pressante nell'attuale contesto post-pandemico e, soprattutto, con riferimento alla discussione in corso relativa all'emanazione del *Digital Services Act*.

Note

[1] *Reno v. American Civil Liberties Union*, 521 US 844 (1997).

[2] *Abrams v. United States*, 250 US 616 (1919). Sul punto, si vedano tra gli altri L.C. Bollinger, *The Tolerant Society: Freedom of Speech and Extremist Speech in America*, Oxford University Press, 1988, 304 p., p. 59-61; M. Rosenfeld, *Hate Speech in Constitutional Jurisprudence: A Comparative Analysis*, in "Cardozo Law Review", vol. 24, 2003, n. 4, p. 1523-1567, spec. p. 1533-1535.

[3] Cfr. D. Lupton, *Digital risk society*, in A. Burgess, A. Alemanno, J.O. Zinn et al. (eds.), "Routledge Handbook of Risk Studies", Routledge, 2016, p. 301-309.

[4] Si vedano, *ex multis*, Corte EDU, *Stoll c. Svizzera*, 10 dicembre 2007, ric. 69698/01; *K.U. c. Finlandia*, 2 dicembre 2008, ric. no. 2872/02; *Pravoye Delo e Shtekel c. Ucraina*, 5 maggio 2011, ric. 33014/05. Cfr. O. Pollicino, *Judicial protection of fundamental rights on the Internet: A road towards digital constitutionalism?*, Hart, 2021, XXIV+235 p.

[5] G. Sartor, A. Loreggia, *The impact of algorithms for online content filtering or moderation. "Upload filters"*, studio richiesto dal Comitato JURI del Parlamento europeo, n. PE 657.101), 2020.

[6] J. Grimmelmann, *The Virtues of Moderation*, in "Yale Journal of Law and Technology", 2015, n. 17, p. 42-109.

[7] T. Gillespie, *Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, 2018, 288 p., a p. 5. Si veda anche, sul punto, N. Helberger, J. Pierson, T. Poell, *Governing online platforms: From contested to cooperative responsibility*, in "The Information Society", vol. 23, 2018, n. 1, p. 1-14.

[8] Così T. Gillespie, *op. cit.*, p. 13: «And moderation is, in many ways, the commodity that platforms offer. Though part of the web, social media platforms promise to rise above it, by offering a better experience of all this information and sociality: curated, organized, archived, and moderated».

[9] R. Wilson, M. Land, *Hate Speech on Social Media: Content Moderation in Context*, in "Connecticut Law Review", vol. 52, 2021, n. 3, p. 1029-1076, spec. p. 1054.

[10] J.M. Balkin, *Old-School/New-School Speech Regulation*, in "Harvard Law Review", vol. 127, 2013, n. 8, p. 2296-2342. Si veda, sulla regolazione degli intermediari digitali, G. Frosio

(ed.), *The Oxford handbook of online intermediary liability*, Oxford University Press, 2020, 782 p.

[11]Si vedano altresì J.M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in "U.C. Davis Law Review", vol. 51, 2017, n. 3, p. 1149-1210; J.M. Balkin, *Free Speech Is a Triangle*, in "Columbia Law Review", vol. 118, 2018, n. 7, p. 2011-2056.

[12]In una prima fase, la Commissione europea faceva per lo più ricorso a strumenti di auto-regolazione dal basso. Tra questi, il rimando è, soprattutto, al *Codice di condotta dell'UE per contrastare l'illecito incitamento all'odio* (2016), nonché al *Codice di buone pratiche sulla disinformazione* (2019). Progressivamente, l'approccio della Commissione è tuttavia mutato nella direzione di una maggiore regolazione "dall'alto", attraverso il ricorso sempre più diffuso a strumenti di *hard law*. Si vedano, in particolare: la Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato (2018) OJ L61/69; la Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (2019) OJ L130/92; e il Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online (2021) OJ L172/79. Si veda, da ultimo, la proposta per il cosiddetto *Digital Services Act*: Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM(2020) 825 final.

[13]Si veda, tra gli altri, R. Gorwa, R. Binns, C. Katzenbach, *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, in "Big Data & Society", vol. 7, 2020, n. 1, p. 1-15.

[14]Tra le numerose definizioni che sono state offerte del termine *hate speech*, si veda in particolare European Commission against Racism and Intolerance (ECRI), *General Policy Recommendation no. 15 on Combating Hate Speech*, 21 March 2016, CRI(2016)15, p. 16: «Hate speech for the purpose of the Recommendation entails the use of one or more particular forms of expression – namely, the advocacy, promotion or incitement of the denigration, hatred or vilification of a person or group of persons, as well any harassment, insult, negative stereotyping, stigmatization or threat of such person or persons and any justification of all these forms of expression – that is based on a non-exhaustive list of personal characteristics or status that includes "race", colour, language, religion or belief, nationality or national or ethnic origin, as well as descent, age, disability, sex, gender, gender identity and sexual orientation».

[15]J. Grimmelmann, *op. cit.*, p. 47.

[16]R. Gorwa, R. Binns, C. Katzenbach, *op. cit.*, p. 3.

[17]E. Llansó et al., *Artificial intelligence, Content Moderation, and Freedom of Expression*, TWG, 26 February 2020, 32 p.

[18]R. Gorwa, R. Binns, C. Katzenbach, *op. cit.*, p. 3.

[19]In questo senso, Wu parla di controllo "positivo" della libertà di espressione. Si veda T. Wu, *Will artificial intelligence eat the law? The rise of hybrid social-ordering systems*, in "Columbia Law Review", vol. 119, 2019, n. 7, p. 2001-2028, a p. 2014.

[20]Si vedano, tra gli altri, E. Llansó et al., *op. cit.*; C.R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, 2017, XIV+316 p.; E. Pariser, *The filter bubble: what the Internet is hiding from you*, Penguin, 2011, 294 p.; N. Helberger et al., *A freedom of expression perspective on AI in the media – with a special focus on editorial decision making on social media platforms and in the news media*, in "European Journal of Law and Technology", vol. 11, 2020, n. 3, p. 1-28; S. Milano et al., *Recommender systems and their ethical challenges*, in "AI & Society", vol. 35, 2020, n. 4, p. 957-967; N.P. Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives*, Cambridge University Press, 2019.

[21]Si veda, in particolare, K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in "Harvard Law Review", vol. 131, 2017, n. 6, p. 1598-1670.

[22]G. De Gregorio, *Democratising online content moderation: A constitutional framework*, in "Computer Law & Security Review", vol. 36, 2020, p. 1-17.

[23]Le condizioni lavorative dei moderatori umani, con particolare riferimento ai danni psichici da essi sovente riportati, sono state trattate in particolare in S.T. Roberts, *Behind the screen: Content moderation in the shadows of social media*, Yale University Press, 2019, 266 p. A p. 25, l'autrice sottolinea come i lavoratori del settore siano generalmente «poorly paid human beings who risk burnout, desensitization, and worse because of the nature of their work». Si veda altresì Cambridge Consultants, *Use of AI in Online Content Moderation*, Ofcom, 2019.

[24]Si vedano, sul punto, Cambridge Consultants, *op. cit.*; R. Gorwa, R. Binns, C. Katzenbach, *op. cit.*; G. Sartor, A. Loreggia, *op. cit.*

[25]Cfr. J. Burrell, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in "Big Data & Society", vol. 3, 2016, n. 1, p. 1-12; F. Pasquale, *The black box society: the secret algorithms that control money and information*, Harvard University Press, 2015, 311 p.

[26]J. Eisenstein, *Introduction to Natural Language Processing*, MIT Press, 2019, 536 p. A p. 1 si definisce il *natural language processing* come «the set of methods for making human language accessible to computers». Si veda anche N. Duarte, E. Llansó, A. Loup, *Mixed messages? The limits of automated social media content analysis*, Center for Democracy & Technology, 2017, p. 9. Per quanto concerne l'applicabilità specifica dell'NLP per la moderazione dell'*hate speech*, si veda A. Schmidt, M. Wiegand, *A Survey on Hate Speech Detection using Natural Language Processing*, in L.W. Ku, C.T. Li (eds.), "Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media", ACL, 2017, p. 1-10. Peraltro, un campo di ricerca particolarmente fertile sembra essere, soprattutto ai fini della rilevazione di contenuti d'odio, quello della *sentiment analysis* (o *opinion mining*). Sull'argomento, si vedano B. Liu, *Sentiment Analysis: Mining Opinions, Sentiments, and Emotions*, II ed., Cambridge University Press, 2020, XVIII+430 p.; F.A. Pozzi et al., *Challenges of Sentiment Analysis in Social Networks: An Overview*, in Id., "Sentiment Analysis in Social Networks", Morgan Kaufmann, 2017, p. 1-11.

[27]E. Douek, *Governing online speech: from "posts-as-trumps" to proportionality and probability*, in "Columbia Law Review", vol. 121, 2021, n. 3, p. 759-834.

[28]S. Agarwal, C.R. Chowdary, *Combating hate speech using an adaptive ensemble learning model with a case study on COVID-19*, in "Expert Systems with Applications", 2021, n. 185, p. 1-9; United Nations, *Countering COVID-19 Hate Speech*, 2020.

[29]G. De Gregorio, O. Pollicino, P. Dunn, *Digitisation and the central role of intermediaries in a post-pandemic world*, in "MediaLaws", 2021; F. Tagliabue, L. Galassi, P. Mariani, *The "Pandemic" of Disinformation in*

COVID-19, in "SN Comprehensive Clinical Medicine", 2020, n. 2, p. 1287-1289.

[30] M. Lim, G. Alrasheed, *Beyond a technical bug: Biased algorithms and moderation are censoring activists on social media*, in "The Conversation", 2021.

[31] Facebook Transparency Center, *Community Standards Enforcement Report – Hate Speech*, Meta, 2022.

[32] I dati concernenti la moderazione dei discorsi d'odio su Instagram sono disponibili solo con riferimento al periodo successivo all'ultimo trimestre del 2019.

[33] Occorre sottolineare, peraltro, che nel momento in cui si scrive non è possibile ancora prevedere quali saranno gli effetti, a livello di moderazione dei contenuti d'odio, dello scoppio del conflitto russo-ucraino nel febbraio 2022.

[34] M. Schroepfer, *Update on Our Progress on AI and Hate Speech Detection*, Meta, 2021.

[35] Facebook Transparency Center, *Community Standards Enforcement Report*, cit.

[36] Per una definizione di "diffusione" si veda Facebook Transparency Center, *Prevalence*, Meta, 2021.

[37] T. Simonite, *Facebook's AI for Hate Speech Improves. How Much Is Unclear*, in "Wired", 2020.

[38] Peraltro, alcuni dati sono disponibili relativamente al numero di contenuti successivamente reintegrati sulle piattaforme. Tuttavia, soprattutto a seguito dello scoppio della pandemia, il ruolo dei reclami proposti dagli utenti sembra essere piuttosto marginale. Nel terzo trimestre del 2021, per esempio, a fronte di 22,3 milioni di contenuti sanzionati su Facebook, solo 1,1 milione di reclami sono stati proposti dagli utenti: di questi solo 90,7 mila sono stati accolti. Questo a fronte dei circa 30,3 mila contenuti reintegrati autonomamente da Facebook. In generale, tali dati appaiono essere poco rappresentativi del reale tasso di errore. Facebook Transparency Center, *Community Standards Enforcement Report*, cit.

[39] G. Sartor, A. Loreggia, *op. cit.*

[40] E. Douek, *op. cit.*

[41] A. Brown, *What Is Hate Speech? Part 2: Family Resemblances*, in "Law and Philosophy", vol. 36, 2017, n. 5, p. 561-613; P. Dunn, *Piattaforme digitali e moderazione dei contenuti d'odio: nodi giuridici e pratici*, in "MediaLaws", 2021.

[42] Si veda, in tal senso, R. Wilson, M. Land, *op. cit.* Per la (ampia) definizione utilizzata dalle piattaforme di Meta, si veda Facebook Transparency Center, *Hate speech*, Meta, 2021.

[43] Si veda, in particolare, il c.d. "Piano d'Azione Rabat" delle Nazioni Unite. Consiglio per i diritti umani delle Nazioni Unite, *Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred* (A/HRC/22/17/Add.4), 2013. Si veda altresì A. Weber, *Manual on hate speech*, Council of Europe Publishing, 2009, VI+98 p.

[44] M. Durante, *Potere computazionale. L'impatto delle ICT su diritto, società, sapere*, Meltemi, 2019, 397 p.

[45] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (trad. it. M. Durante), Raffaello Cortina, 2017, XVIII+294 p., pp. 147-164.

[46] Per una comprensione del fenomeno del *meme* in Internet, si veda G. Marino, *Semiotics of spreadability: A systematic approach to Internet memes and virality*, in "Punctum", vol. 1, 2015, n. 1, p. 43-66, a p. 60.

[47] Per uno studio su come gli algoritmi utilizzati da piattaforme e intermediari digitali abbiano la tendenza a riprodurre e replicare *bias* discriminatori, soprattutto nei confronti delle donne afro-americane, si veda S.U. Noble, *Algorithms of oppression: how search engines reinforce racism*, New York University Press, 2018.

[48] J.H. Park, J. Shin, P. Fung, *Reducing Gender Bias in Abusive Language Detection*, in E. Riloff, D. Chiang, J. Hockenmaier, J. Tsujii (eds.), "Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing", ACL, 2018, p. 2799-2804; X. Zhou, M. Sap, S. Swayamdipta et al. (eds.), *Challenges in Automated Debiasing for Toxic Language Detection*, in P. Merlo, J. Tiedemann, R. Tsarfaty (eds.), "Proceedings of the Sixteenth Conference of the European Chapter of the Association for Computational Linguistics: Main Volume", ACL, 2021, p. 3143-3155.

[49] T. Davidson, D. Warmsley, M. Macy, I. Weber, *Automated Hate Speech Detection and the Problem of Offensive Language*, in "Proceedings of the Eleventh International AAAI Conference on Web and Social Media", vol. 11, 2017, n. 1, p. 512-515; T. Davidson, D. Bhattacharya, I. Weber, *Racial Bias in Hate Speech and Abusive Language Detection Datasets*, in T.S. Roberts, J. Tetreault, V. Prabhakaran, Z. Waseem (eds.), "Proceedings of the Third Workshop on Abusive Language Online", ACL, 2019, p. 25-35; M. Sap, D. Card, S. Gabriel et al., *The Risk of Racial Bias in Hate Speech Detection*, in A. Korhonen, D. Traum, L. Màrquez (eds.), "Proceedings of the Fiftyseventh Annual Meeting of the Association for Computational Linguistics", ACL, 2019, p. 1668-1678.

[50] T. Dias Oliva, D.M. Antonialli, A. Gomes, *Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online*, in "Sexuality & Culture", vol. 25, 2021, n. 2, p. 700-732. Il lavoro analizza come il software *Perspective*, sviluppato da Google per individuare contenuti ascrivibili alla classe del *toxic speech*, impatti rispettivamente i tweet pubblicati da celebri *drag queen* statunitensi e quelli pubblicati da altrettanto noti estremisti di destra. Secondo lo studio, i contenuti prodotti dalle prime sarebbero in molti casi rilevati come altrettanto tossici, e spesso come più tossici, dei secondi. Così, per esempio, il tweet «and I'm ... GAY. #HairsprayLive» della *drag queen* Mimi Imfurst risulterebbe essere tossico al 92,31% (p. 720), mentre il tweet del politico *alt-right* Richard Spencer «@hodgie2000 Of course, homosexuality is a naturally occurring phenomenon. But as another already said, so is cannibalism, addiction, suicide, self-harm, etc. The question is: what is the *cause* of this curious phenomenon, from evolutionary, genetic, social, or psychological perspectives», in cui l'omosessualità è di fatto paragonata al cannibalismo, alle dipendenze, al suicidio e all'autolesionismo, riporterebbe un grado di tossicità pari al solo 13,80% (p. 724).

[51] Con riferimento alla comunità LGBTQIA+, e in particolare alla sotto-comunità *drag*, si veda S. McKinnon, *"Building a thick skin for each other": The use of 'reading' as an interactional practice of mock impoliteness in drag queen backstage talk*, in "Journal of Language and Sexuality", vol. 6, 2017, n. 1, p. 90-127. L'autore, nell'occuparsi della pratica del *reading*, riconduce l'uso di espressioni apparentemente insultanti alla categoria della *mock impoliteness*, da intendersi come l'insieme di quelle «utterances, which could potentially be evaluated as genuine impoliteness outside the appropriate context, are positively evaluated by in-group members who recognize the importance of 'building a thick skin' to face a hostile environment from LGBT and non-LGBT people» (p. 90).

[52] J. Guynn, *Facebook while black: Users call it getting «Zucked», say talking about racism is censored as hate speech*, in "Usa Today", 2019. Tale fenomeno, inoltre, sembra colpire in modo ancora più intenso le donne: si veda in tal senso K.L. Gray, K. Stein, *"We 'said her name' and got zucked": Black Women Calling-out the Carceral Logics of Digital Platforms*, in "Gender & Society", vol. 35, 2021, n. 4, p. 538-545.

[53] N.P. Suzor, *op. cit.*, p. 128-129.

[54] A. Chakraborty, J. Messias, F. Benevenuto et al., *Who Makes Trends? Understanding Demographic Biases in*

Crowdsourced Recommendations, in "Proceedings of the Eleventh International AAAI Conference on Web and Social Media", vol. 11, 2017, n. 1, p. 22-31. Come posto in luce in E. Llansó et al., *op. cit.*, in numerosi casi gli algoritmi di *content curation* tendono, anzi, a premiare contenuti fortemente controversi quali *hate speech* e fake news. Ciò appare essere stato confermato dallo scandalo legato ai cosiddetti "Facebook Papers". The New York Times, *The Facebook Papers and their fallout*, 28 October 2021.

[55] C. Are, *The Shadowban Cycle: An autoethnography of pole dancing, nudity and censorship on Instagram*, in "Feminist Media Studies", 2021, p. 1-18.

[56] M. Rosenfeld, *op. cit.*

[57] J. Weinstein, *An Overview of American Free Speech Doctrine and Its Application to Extreme Speech*, in I. Hare, J. Weinstein (eds.), "Extreme Speech and Democracy", Oxford University Press, 2009, p. 81-91.

[58] L. Kendrick, *Content Discrimination Revisited*, in "Virginia Law Review", vol. 98, 2012, n. 2, p. 231-300, a p. 237.

[59] G. Pitruzzella, O. Pollicino, *Disinformation and hate speech*, Bocconi University Press, 2020, VI+168 p.

[60] Comitato per l'eliminazione della discriminazione razziale (CERD), *General recommendation No. 35: Combating racist hate speech*, CERD/C/GC/35, 2013.

[61] Così, per esempio, Comitato per i diritti umani, *Faurisson c. Francia*, 8 novembre 1996, Comunicazione n. 550/1993: «Since the statements made by the author, read in their full context, were of a nature as to raise or strengthen anti-semitic feelings, the restriction served the respect of the Jewish community to live free from fear of an atmosphere of anti-semitism».

[62] M.J. Matsuda, *Public Response to Racist Speech: Considering the Victim's Story*, in M.J. Matsuda et al. (eds.), "Critical Race Theory, Assaultive Speech, and the First Amendment", Westview, 1993, p. 17-51, a p. 24.

[63] Corte EDU, *Beizaras e Levickas c. Lituania*, ric. no. 41288/15, sent. del 14 gennaio 2020.

[64] Così M.J. Matsuda, *op. cit.*, p. 24-25: «Victims are restricted in their personal freedom. To avoid receiving hate messages, victims have to quit jobs, forgo education, leave their homes, avoid certain public places, curtail their own exercise of speech rights, and otherwise modify their behavior and demeanor. The recipient of hate messages struggles with inner turmoil. One subconscious response is to reject one's own identity as a victim-group member. As writers portraying the African-American experience have noted, the price of disassociating from one's own race is often sanity itself».

[65] Si veda J. Waldron, *The harm in hate speech*, Harvard University Press, 2012, VI+292 p., a p. 105-143.

[66] Così, del resto, Corte EDU, *Féret c. Belgio*, 16 luglio 2009, ric. 15615/07: «La tolérance et le respect de l'égale dignité de tous les êtres humains constituent le fondement d'une société démocratique et pluraliste. Il en résulte qu'en principe on peut juger nécessaire, dans les sociétés démocratiques, de sanctionner, voire de prévenir, toutes les formes d'expression qui propagent, encouragent, promeuvent ou justifient la haine fondée sur l'intolérance [...]».

[67] Così S. Fredman, *Substantive equality revisited*, in "International Journal of Constitutional Law", vol. 14, 2016, n. 3, p. 712-738, a p. 731-732: «The right to equality is concerned with two aspects of participation. The first is political. Given that past discrimination or other social mechanisms have blocked the avenues for political participation by particular minorities, equality laws are needed both to compensate for this absence of political voice and to open up the channels for greater participation in the future. [...] The second aspect of the participative dimension is to address the importance of community in the life of individuals. Rather than the universal, abstract individual of formal equality, substantive equality recognizes that individuals are essentially social. To be fully human includes the ability to participate on equal terms in community and society more generally».

[68] F. Faloppa, *#Odio. Manuale di resistenza alla violenza delle parole*, UTET, 2020, 304 p., a p. 199 definisce la controNarrazione come «una narrazione a breve termine, che nasce come risposta diretta e più immediata a uno specifico discorso, o a una specifica narrazione, d'odio» e aggiunge che essa «ha quindi l'obiettivo di evidenziare le incoerenze della narrazione che si vuole contrastare, tentando così di sfidarla sullo stesso piano, indebolirla portandone a galla i meccanismi, smantellarla e delegittimarla». Sul ruolo della controNarrazione nel contrasto all'*hate speech*, si veda European Commission against racism and intolerance (ECRI), *op. cit.* Si veda inoltre R. Cohen-Almagor, *Countering Hate on the Internet*, in "Annual Review of Law and Ethics", vol. 22, 2014, p. 431-443, a p. 435.

[69] G. Ziccardi, *Online Political Hate Speech in Europe: The Rise of New Extremisms*, Edward Elgar Publishing, 2020, p. 116-121.

[70] Sul punto si veda, in particolare, S. Wachter, B. Mittelstadt, C. Russell, *Bias Preservation in Machine Learning: The Legality of Fairness Metrics under EU Non-Discrimination Law*, in "West Virginia Law Review", vol. 123, 2020, n. 3, p. 735-790. Gli autori sottolineano come una prospettiva di uguaglianza sostanziale, anziché meramente formale, sia più in linea con il panorama normativo e i valori costituzionali caratterizzanti l'Unione europea. A tal fine, propongono il ricorso a quelli che loro definiscono *bias transforming metrics* (i quali tengono conto delle disuguaglianze storiche tra categorie di persone) quali parametri per valutare la *fairness* di un sistema di *machine learning*, anziché ai *bias preserving metrics* (che assumono invece una prospettiva di uguaglianza formale degli individui). «Put simply, developers have a choice between two types of metrics: (1) "bias preserving" metrics that take society as it currently exists as a neutral starting point or "level playing field" from which we can measure inequality and bias in machine learning; and (2) "bias transforming" metrics that acknowledge historical inequalities and start from the assumption that certain groups will have a worse starting point than others. [...] [O]ur choice of fairness metric can ensure machine learning applications do not exacerbate existing inequalities and fully acknowledge the extent and significance of existing inequalities. The choice of variables to condition on for fairness tests, thresholds for illegal disparity, and acceptable arguments to justify disparity are difficult political determinations» (p. 778).

[71] Cfr. G. De Gregorio, *op. cit.*

[72] Regolamento (UE) 2021/784, cit.

[73] Emendamenti del Parlamento europeo, approvati il 20 gennaio 2022, alla proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, P9_TA(2022)0014.

[74] N. Appelman, J. Quintais, R. Fahy, *Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions?*, in "DSA Observatory", 31 May 2021. Sul tema dell'efficacia orizzontale dei diritti fondamentali tutelati dalla Carta di Nizza si veda E. Frantziou, *The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle*, in "Cambridge Yearbook of European Legal Studies", 2020, n. 22, p. 208-232.

[75] J. Barata, *The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations*, in "DSA Observatory", 27 July 2021.

[76] Cfr. considerando 12.

[77]L'art. 19 prevede che, in caso di segnalazioni pervenute da soggetti che, sulla base di criteri oggettivi, siano stati riconosciuti quali "segnalatori attendibili", le piattaforme online dovranno valutare tali segnalazioni in via prioritaria.

* * *

Automated content moderation and algorithmic discrimination: the case of hate speech

Abstract: The need for Internet intermediaries to moderate user-generated content has become more and more pressing. Besides, vis-à-vis the extraordinary increase in the quantity of daily online information, the resort to algorithmic tools for moderation is today essential. This is also true for the detection of hate speech acts, which is currently largely based on the use of AI and machine-learning techniques: however, scholarly literature has highlighted how such systems can often be vitiated by discriminatory biases which produce a high risk of false positives affecting minorities. The present contribution argues that, within the European constitutional framework, the fight against hateful contents finds its rationale in the goal of ensuring that all social groups can truly enjoy a substantive equality, and that, as a consequence, a discriminatory enforcement of hate speech bans is inconsistent with the value system of the EU. Therefore, although AI represents a fundamental and necessary tool to guarantee a safer and more tolerant digital ecosystem, a high rate of false positives is not fully acceptable when it comes to hate speech moderation. It is thus necessary to rethink the relevant political and legislative strategies, with a view to ensure that marginalised groups can enjoy appropriate substantive and procedural guarantees protecting their freedom of expression and their right to non-discrimination.

Keywords: Automated content moderation – Hate speech – Algorithmic discrimination – Substantive equality – Freedom of expression

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0063
Articolo sottoposto a peer review

Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD

Alessandro Ortalda • Stefano Leucci

La proposta di emendamento al Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno ha rinvigorito il dibattito europeo sul tema dell'identità digitale. I vari problemi emersi da questo dibattito rendono necessario un miglior coordinamento della proposta con gli strumenti legislativi preesistenti. Il presente contributo mira ad analizzare i principali punti di frizione tra il quadro normativo legato alle identità elettroniche/digitali e la disciplina europea riguardante la protezione dei dati personali.

Identità elettronica – Identità digitale – eIDAS – RGPD

Sommario: *1. Introduzione – 2. Presentazione del quadro normativo – 2.1. Il governo delle identità digitali – 2.2. La protezione dei dati personali – 3. Identità elettronica e rischi per gli individui – 3.1. Interazioni tra eIDAS e RGDP – 3.2. eIDAS e rischi di discriminazione – 4. Conclusione*

1. Introduzione

Il 23 luglio 2014, il Parlamento europeo ed il Consiglio hanno approvato il "Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno" (anche Regolamento 910/2014 o Regolamento eIDAS)[1]. A circa sette anni di distanza, il 3 giugno 2021, la Commissione europea ha presentato una proposta di emendamento al Regolamento eIDAS (anche eIDAS-2)[2], che introduce una serie di modifiche attualmente in fase di discussione. La proposta ha riportato l'attenzione su un argomento che, a livello europeo, sembrava aver perso visibilità rispetto ad altri aspetti legati al mondo digitale come la protezione dei dati personali e la sicurezza cibernetica.

Il rinnovato interesse per il tema dell'identificazione elettronica transfrontaliera coincide sia con una maggior attenzione a livello globale[3], sia con la strategia di governance digitale dell'Unione. Infatti, la crescita di valore degli asset digitali e dei servizi erogati attraverso Internet rappresenta un interessante ambito di sviluppo economico per l'Europa[4]. Tuttavia, la quasi totale egemonia delle grandi piattaforme extra europee può rappresentare un ostacolo per lo sviluppo di questo inespresso potenziale economico. In questo contesto, la creazione di un Mercato unico digitale europeo che permetta a cittadini e residenti autorizzati di accedere a servizi online in tutta Europa è un passaggio quasi obbligato, di cui l'identificazione elettronica transfrontaliera rappresenta un tassello fondamentale[5], come evidenziato dalla rela-

A. Ortalda è dottorando di ricerca presso la Vrije Universiteit Brussel; si occupa di identità digitale, protezione dei dati personali e cybersecurity. È inoltre responsabile delle attività di formazione presso il Brussels Privacy Hub. S. Leucci è responsabile legale e tecnologico presso il Garante europeo della protezione dei dati; le sue principali responsabilità riguardano la previsione strategica delle nuove tendenze tecnologiche, le questioni finanziarie e l'intelligenza artificiale. È fellow al Nexa Center for Internet & Society del Politecnico di Torino.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

zione che accompagna la proposta di emendamento al regolamento eIDAS.

La modifica di uno strumento normativo comporta per sua stessa natura rischi che, se non adeguatamente indirizzati, possono manifestare impatti negativi per l'Unione e i suoi cittadini. Infatti, la proposta di emendamento del Regolamento eIDAS presenta alcuni aspetti potenzialmente problematici. Talvolta si tratta di problemi derivanti da nuove disposizioni introdotte nella proposta. Talvolta si tratta di problemi già presenti nel Regolamento eIDAS in vigore e rimasti invariati nella proposta di emendamento. Talvolta si tratta di potenziali problemi derivanti da possibili frizioni tra diritti degli individui e strumenti legati all'identificazione elettronica non adeguatamente indirizzati dagli strumenti normativi.

La proposta di emendamento è al vaglio di diversi organismi comunitari che dovranno esprimersi su eventuali modifiche[6]; pertanto, è verosimile ritenere che subirà ulteriori modifiche. Tuttavia, proprio in virtù della sua attuale modificabilità è importante sottolinearne gli aspetti problematici e fornire alle parti coinvolte spunti che possano aiutarle nel processo di miglioramento della proposta.

Specificamente, il presente contributo si propone di analizzare i principali punti di frizione tra il quadro normativo legato alle identità elettroniche/digitali[7] e la disciplina riguardante la protezione dei dati personali prevista dal *Regolamento generale sulla protezione dei dati* (anche RGPD)[8]. Il paragrafo 2 descrive i quadri normativi oggetto dell'analisi, rispettivamente quello delineato dal Regolamento eIDAS e dalla successiva proposta di emendamento e quello delineato dal RGPD. Il paragrafo 3 analizza i punti di frizione tra questi quadri normativi e le eventuali problematiche derivanti da tali punti di frizione, includendovi anche gli eventuali rischi di discriminazione che potrebbero derivare dall'utilizzo di sistemi di identificazione elettronica. Infatti, le nuove tecnologie hanno il potenziale di rivoluzionare i processi di identificazione a patto che mitighino adeguatamente i possibili problemi di discriminazione connessi al loro utilizzo e promuovano buone prassi legate alla protezione dei dati personali[9]. Il paragrafo 4, infine, presenta le conclusioni dell'analisi.

2. Presentazione del quadro normativo

2.1. Il governo delle identità digitali

In Europa, il Regolamento eIDAS rappresenta il principale strumento normativo riguardante il governo delle identità digitali. Il Regolamento eIDAS stabilisce un quadro normativo volto ad agevolare la creazione ed il governo di strumenti e processi comuni tra gli Stati membri dell'Unione europea per il riconoscimento transfrontaliero delle identità elettroniche per l'accesso a servizi digitali, istituendo, *inter alia*[10], le modalità di notifica e riconoscimento dei mezzi e regimi di identificazione elettronica. Per mezzi di identificazione elettronica, il Regolamento eIDAS intende «un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online»[11], mentre quando parla di regimi di identificazione elettronica intende «un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche»[12].

Come indicato più sopra, il Regolamento eIDAS si occupa principalmente di definire l'ecosistema normativo per garantire l'interoperabilità tra i diversi mezzi e regimi di identificazione elettronica adottati nell'Unione. Non definisce dunque le modalità e finalità dei singoli regimi nazionali di identificazione elettronica – prerogativa che rimane dei singoli Stati membri – limitandosi ad indicare gli elementi minimi che tali regimi devono soddisfare per garantire l'interoperabilità con i regimi istituiti da altri Stati membri. Specificamente, il Regolamento eIDAS dispone le condizioni affinché i mezzi di comunicazione adottati dai diversi Stati membri possano venire reciprocamente riconosciuti[13] e dispone le modalità attraverso cui gli Stati membri notificano alla Commissione europea l'esistenza e le caratteristiche dei loro regimi di identificazione elettronica[14]. Si noti come il Regolamento eIDAS applichi le sue disposizioni solamente nel caso in cui «i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica possono essere utilizzati per accedere almeno a un servizio che è fornito da un organismo del settore pubblico»[15], escludendo pertanto i mezzi di identificazione utilizzati esclusivamente nell'ambito di servizi offerti da operatori privati. Il Regolamento eIDAS, altresì, non impone agli Stati membri l'obbligo di notificare un regime di identificazione elettronica, lasciando tale scelta alla discrezione dei singoli Stati membri.

Dalla pubblicazione del Regolamento eIDAS, avvenuta nel luglio del 2014, diversi elementi hanno contribuito a modificare lo scenario europeo ed internazionale, non ultimo l'emergenza del Covid-19. Questi hanno modificato le aspettative di utenti ed operatori di servizi in relazione alle caratteristiche che i regimi di identificazione elettronica devono soddisfare[16]. Inoltre, l'aspirazione di creare uno spazio europeo per le identità elettroniche appare disattesa dai bassi tassi di adozione di strumenti

transfrontalieri di identificazione elettronica[17]. Pertanto, la Commissione europea nel febbraio del 2020 sì è impegnata ad avviare un processo di revisione del Regolamento eIDAS con il duplice obiettivo di stimolare una maggiore adozione di strumenti di identificazione elettronica tra gli Stati membri e riscrivere un quadro normativo più adatto al mutato scenario[18]. Nel giugno 2021, la Commissione europea ha pubblicato una proposta contenente una lista di emendamenti al Regolamento eIDAS, due dei quali di particolare rilevanza.

La proposta di emendamento all'articolo 7 del Regolamento eIDAS modifica il processo di notifica e riconoscimento dei regimi di identificazione elettronica, introducendo l'obbligo per gli Stati membri di notificare un regime di identificazione elettronica entro 12 mesi dall'entrata in vigore del Regolamento. Nella proposta di emendamento, pertanto, la notifica cessa di essere una libera scelta degli Stati membri su base volontaria, diventando un requisito.

Con l'introduzione dell'articolo 6-*bis*, invece, la proposta di emendamento al Regolamento eIDAS introduce i cosiddetti "portafogli europei di identità digitale". Questi vengono definiti come «un prodotto e servizio che consente all'utente di conservare dati di identità, credenziali e attributi collegati alla sua identità, fornirli su richiesta alle parti facenti affidamento sulla certificazione e utilizzarli per l'autenticazione, online e offline, per un servizio, conformemente all'articolo 6-*bis*, nonché per creare firme elettroniche qualificate e sigilli elettronici qualificati»[19]. Inoltre, al fine di «garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso sicuro, affidabile e senza soluzione di continuità a servizi pubblici e privati transfrontalieri, ciascuno Stato membro emette un portafoglio europeo di identità digitale entro 12 mesi dall'entrata in vigore del presente regolamento»[20], rendendo i portafogli europei di identità digitale un elemento obbligatorio e fondamentale nel quadro normativo di eIDAS-2.

La modifica dell'articolo 7 e l'introduzione dell'articolo 6-*bis* denotano la volontà da parte della Commissione europea di intervenire con maggior decisione nel processo di creazione di uno spazio europeo per le identità elettroniche. I due emendamenti appaiono finalizzati rispettivamente a promuovere una maggiore adozione di strumenti di identificazione transfrontaliera tra gli Stati membri e a fornire ai cittadini e residenti autorizzati degli strumenti che garantiscano loro un maggior controllo sui propri dati personali, allontanandosi così dal paradigma dei sistemi di identificazione elettronica centralizzati[21]. A queste considerazioni si aggiunga tuttavia che, l'introduzione di un approccio di notifica obbligatoria in vece del precedente approccio volontario per gli Stati membri potrebbe inasprire ulteriormente i fattori di rischio, in quanto eventuali problematiche connesse al quadro normativo si manifesterebbero ovunque in Europa e non soltanto negli Stati membri che avessero deciso di partecipare allo spazio europeo di identificazione elettronica transfrontaliera. Pertanto, una analisi dei potenziali problemi risulta ancora più importante.

2.2. La protezione dei dati personali

Il principale strumento normativo europeo in materia di protezione dei dati personali è il Regolamento generale per la protezione dei dati personali. Emanato nel 2016 ed entrato in vigore nel 2018, il Regolamento abroga la precedente Direttiva 95/46/CE sulla protezione dei dati personali[22]. Il RGPD si applica ai trattamenti di dati personali che avvengono sul territorio dell'Unione europea, oppure nei casi in cui i trattamenti siano finalizzati ad offrire beni o servizi a cittadini europei, nonché nei casi in cui i trattamenti comportino il monitoraggio del comportamento di questi cittadini sul territorio dell'Unione europea. Il RGPD definisce dati personali «qualsiasi informazione riguardante una persona fisica identificata o identificabile»[23], mentre definisce trattamento «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»[24]. Da queste definizioni si evince già come l'utilizzo di strumenti di identità elettronica soddisfi, in moltissimi casi, i requisiti connessi ai trattamenti di dati personali, attivando pertanto l'applicabilità del RGPD.

La disciplina europea in materia di protezione dei dati personali si basa prevalentemente su principi fondanti[25]. L'applicazione di questi principi può variare, anche considerevolmente, a seconda del contesto. Pertanto, il RGPD è da intendersi come una norma di indirizzo che non può prescindere dalla valutazione caso per caso sulle migliori modalità di implementazione delle sue disposizioni. Per il principio di liceità, ogni trattamento di dati personali deve essere svolto sulla base del consenso del soggetto interessato dal trattamento (nel seguito, l'interessato) o di un'altra base legittima[26]. Connessi al principio di liceità vi sono i principi di correttezza e trasparenza[27]. Il primo prevede che le operazioni di trattamento non

siano eseguite in segreto e gli interessati siano adeguatamente informati dei potenziali rischi, oltreché prevedere che i titolari e responsabili del trattamento dei dati predispongano adeguate misure per conformarsi prontamente, per quanto possibile, alla volontà dell'interessato, specialmente quando il suo consenso costituisce la base giuridica del trattamento dei dati[28]. Il secondo si riferisce all'obbligo di adottare misure appropriate per tenere informati gli interessati riguardo gli utilizzi dei loro dati personali[29].

Il principio di limitazione della finalità[30] obbliga ad effettuare il trattamento di dati personali per una finalità specifica e ben definita e prevede che un trattamento possa essere esteso a scopi ulteriori solo nei casi in cui siano compatibili con la finalità iniziale[31]. Il trattamento dei dati per finalità non definite e/o illimitate è, pertanto, illecito.

Secondo il principio di minimizzazione dei dati[32], devono essere trattati solo i dati adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali vengono raccolti e/o per le quali vengono successivamente trattati. Le categorie di dati scelte per il trattamento devono essere necessarie per conseguire l'obiettivo generale dichiarato delle operazioni di trattamento e la raccolta di dati deve essere limitata alle informazioni pertinenti per le finalità perseguite dal trattamento. Inoltre, secondo il principio di esattezza dei dati[33], devono essere adottate misure necessarie e ragionevoli per garantire che i dati siano esatti e mantenuti aggiornati.

Il principio di limitazione della conservazione[34] impone che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Pertanto, i dati devono essere cancellati o resi anonimi quando tali finalità siano state soddisfatte. A tal fine, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica, per garantire che i dati non siano conservati più a lungo del necessario[35].

Il principio di integrità e riservatezza dei dati[36] richiede che siano messe in atto misure tecniche o organizzative adeguate a proteggere i dati da accesso, uso, modifica, o divulgazione non autorizzati o da perdita, distruzione o danno accidentali. Il RGPD prevede che tali misure vengano attuate tenendo conto «dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche»[37].

Infine, il principio di responsabilizzazione (o, in inglese, *accountability*)[38] fornisce una cornice a tutti i precedenti. Secondo tale principio, l'organizzazione che tratta i dati personali deve essere competente nel trattare i dati in modo adeguato e deve essere in grado di comprovarlo[39]. L'essenza di questo principio è dunque quella di assicurarsi che vengano messe in atto misure che garantiscano il rispetto delle norme sulla protezione dei dati e di conservare le prove necessarie per dimostrarlo agli interessati e alle autorità di controllo. Il principio di responsabilizzazione estende la sua area non solo alla conformità delle attività di trattamento alle norme applicabili, ma anche all'efficacia delle misure[40].

Come anticipato, l'applicazione delle regole derivanti dai principi del RGPD deve essere valutata caso per caso e, pertanto, richiede una interpretazione flessibile. Tale flessibilità deve tenere in considerazione il contesto e i rischi per i diritti e le libertà dei soggetti interessati associati al trattamento. Proprio per indirizzare tali problematiche, il RGDP introduce la valutazione dell'impatto sulla protezione dei dati (DPIA), uno degli strumenti più importanti per la gestione del rischio. Il Gruppo di lavoro articolo 29 descrive la DPIA come «un processo per costruire e dimostrare la conformità»[41]. Tuttavia, qualificarlo come mero strumento di conformità potrebbe diminuirne i benefici in relazione ad una corretta protezione dei dati personali[42]. Questo risulta di particolare importanza in un contesto come quello dell'identità digitale, in cui le applicazioni di tali strumenti possono modificarsi nel tempo fino ad assumere modalità imprevedibili al momento iniziale dello sviluppo, così come discusso nel paragrafo 3.2.

3. Identità elettronica e rischi per gli individui

Recenti analisi hanno evidenziato come i punti di contatto tra il quadro normativo legato all'identificazione elettronica e quello legato alla protezione dei dati personali possano dare luogo a sovrapposizioni o frizioni in grado di rendere meno agevole l'implementazione di misure conformi[43]. Questo paragrafo si pone l'obiettivo di analizzare le principali problematiche derivanti dall'interazione tra il Regolamento eIDAS, compresa la sua proposta di emendamento, ed il RGPD. Risulta infatti chiaro come le norme sull'identificazione elettronica e quelle sulla protezione dei dati siano strettamente connesse tra di loro. Non soltanto in virtù del fatto che molte delle attività associate alla gestione e all'utilizzo di mezzi e regimi di identificazione elettronica possano qualificarsi come trattamenti di dati personali ai sensi del RGPD, ma anche per via dei riferimenti espliciti al RGPD

riportati sia dal Regolamento eIDAS che dalla sua proposta di emendamento.

Nell'impossibilità di procedere ad una trattazione sistematica di tutti i potenziali problemi legati all'applicazione del Regolamento eIDAS e della sua proposta di revisione[44], il presente contributo si focalizza su un sottoinsieme di problematiche, descrivendone le caratteristiche principali: la sovrapposizione tra il regime di responsabilità previsto da eIDAS e quello previsto dal RGPD; l'incompatibilità dell'insieme minimo di dati previsto da eIDAS con il principio della minimizzazione dei dati previsto dal RGPD; l'incompatibilità del requisito di ritirare il portafoglio europeo di identità digitale in caso di violazione o compromissione dello stesso con il principio di disponibilità dei dati previsto dal RGPD. Il paragrafo dedica anche spazio all'analisi di possibili rischi di discriminazione derivanti dall'utilizzo di soluzioni di identificazione elettronica, interrogandosi riguardo alle misure messe in campo da eIDAS per la minimizzazione di tali rischi.

3.1. Interazioni tra eIDAS e RGPD

3.1.1. Sovrapposizione tra il regime di responsabilità di eIDAS e del RGPD

L'articolo 11 del Regolamento eIDAS, non modificato dalla proposta di emendamento, definisce il regime di responsabilità da applicarsi in caso di transazioni elettroniche transfrontaliere. Si tratta di un sistema che punta a garantire la corretta attribuzione delle responsabilità tra le molte parti coinvolte nel contesto delle transazioni elettroniche transfrontaliere. Infatti, queste ultime sono caratterizzate da almeno tra passaggi, ognuno dei quali prevede il coinvolgimento di diverse parti: la creazione di una identità elettronica; la fornitura di mezzi di identificazione elettronica; l'autenticazione dell'utente.

Una identità elettronica viene creata sulla base dei dati di identificazione personale, ovverosia «un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica»[45]. Questo presuppone che, al fine di creare una identità elettronica valida, i dati del soggetto interessato vengano raccolti e registrati in maniera corretta. L'articolo 11.1 del Regolamento eIDAS attribuisce agli Stati membri la responsabilità dei danni causati per dolo o negligenza in fase di creazione dell'identità, in quanto gli Stati membri, al momento della creazione dell'identità elettronica all'interno dei loro regimi di identificazione elettronica, devono garantire «che i dati di identificazione personale che rappresentano unicamente la persona in questione siano attribuiti, conformemente alle specifiche tecniche, norme e procedure [...] al momento in cui è rilasciata l'identificazione elettronica»[46]. Si pensi ad esempio ad un caso in cui i dati anagrafici di un individuo vengano registrati in maniera errata in fase di creazione dell'identità elettronica, causando l'impossibilità dello stesso di accedere a servizi offerti in un altro Stato membro. In tal caso, secondo la disciplina eIDAS, lo Stato membro che ha creato e rilasciato l'identità elettronica viene considerato responsabile del danno arrecato. Si noti come l'articolo 11.1 stabilisca esplicitamente che è lo Stato ad essere responsabile, attribuendogli la responsabilità anche nei casi in cui questo si affidi ad una terza parte per la creazione e rilascio delle identità elettroniche.

La fornitura e accesso ai mezzi di identificazione elettronica è condizione necessaria affinché gli utenti possano usufruire dei servizi di identificazione elettronica. L'articolo 11.2 del Regolamento eIDAS attribuisce la responsabilità per danni connessi ai mezzi di identificazione elettronica alla parte che rilascia suddetti mezzi. Si pensi ad esempio ad un caso in cui l'identità elettronica di un utente venga erroneamente associata ad un altro individuo, impedendo al legittimo proprietario di venire identificato nel corso di una transazione transfrontaliera. Si noti come l'articolo 11.2, a differenza dell'articolo 11.1, attribuisca la responsabilità in maniera generica alla parte coinvolta, senza nominare esplicitamente lo Stato membro. Questo significa che, qualora lo Stato membro abbia direttamente rilasciato i mezzi di identificazione elettronica, qualificandosi pertanto come "parte coinvolta", la responsabilità ricade sullo Stato membro stesso. Differentemente, qualora i mezzi di identificazione siano stati rilasciati da altre parti, la responsabilità potrebbe ricadere su queste ultime, ferme restando le ulteriori responsabilità previste dal sistema giuridico nazionale[47].

Infine, l'autenticazione dell'utente è il passaggio attraverso cui una identità elettronica viene utilizzata per accedere al servizio desiderato. Nel contesto di una autenticazione, il sistema verifica che l'identità elettronica abbia le caratteristiche adeguate o i permessi necessari affinché l'utente possa legittimamente accedere al servizio. L'articolo 11.3 del Regolamento eIDAS attribuisce la responsabilità per danni connessi alla procedura di autenticazione alla parte che gestisce suddetta procedura. Si pensi ad esempio ad un caso in cui un individuo non riesca ad accedere a dei sussidi pubblici a causa della mancata associazione alla sua identità elettronica delle autorizzazioni necessarie. Così come all'articolo 11.2, in questi casi la responsabilità è genericamente attribuita alla

parte responsabile, sia questa lo Stato membro o un fornitore di servizi.

Come si evince dalla descrizione di cui sopra, il Regolamento eIDAS definisce un regime di responsabilità ben preciso, associato a specifici momenti del ciclo di vita e di utilizzo di una identità elettronica. Differentemente, il RGPD prevede un regime di responsabilità caratterizzato da una minor compartimentalizzazione. Il RGPD sancisce che, qualora «più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano [...] responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato»[48]. Il problema deriva dal fatto che la divisione categorica applicata da eIDAS risulta impraticabile nel contesto di un trattamento di dati personali ai sensi del RGPD.

Anche dividendo un trattamento di dati personali in singoli elementi coerenti con i tre passaggi presentati da eIDAS (es., trattamento con finalità di creazione di una identità elettronica; trattamento con finalità di identificazione elettronica; trattamento con finalità di autenticazione elettronica), il regime di responsabilità di eIDAS risulta incompatibile con quello del RGPD qualora più parti siano coinvolte nel trattamento. Si consideri il già citato esempio di danni occorsi durante il processo di autenticazione e derivanti da un errata attribuzione di permessi. In tal caso, la situazione non risulta conforme né con il RGPD, in quanto il trattamento avviene in violazione del principio di esattezza dei dati[49], né con il Regolamento eIDAS. Tuttavia, qualora il trattamento veda il coinvolgimento di più titolari o responsabili del trattamento, l'attribuzione delle responsabilità verrebbe complicata da una difficile interpretazione. Infatti, laddove il RGPD prevede che la responsabilità venga attribuita a tutti i titolari e responsabili coinvolti, chiamati in solido a rispondere dei danni causati, nel Regolamento eIDAS la responsabilità ricade solo sulla «parte che gestisce la procedura di autenticazione»[50]. Non è chiaro se questa debba intendersi come una singola entità, il che renderebbe il regime di responsabilità incompatibile con quello previsto dal RGPD, o preveda la possibilità di attribuire la responsabilità a più entità, allineando i regimi di responsabilità del Regolamento eIDAS e RGPD.

Tuttavia, anche qualora si ammettesse una interpretazione che permetta di allineare le due norme, non è chiaro se, a seguito di una violazione prevista da entrambi gli strumenti normativi, questi si applichino indipendentemente l'uno dall'altro, se le violazioni possano in qualche modo essere assimilate, o se debba essere tenuta in considerazione una sola violazione prevedendo l'applicazione di uno solo dei regimi di responsabilità. Qualora l'interpretazione propenda per quest'ultimo scenario, risulta inoltre incerto quale dei due regimi debba essere applicato. Entrambi gli strumenti sono infatti regolamenti europei e appartengono alla stessa categoria delle fonti del diritto comunitario, rendendo incerto stabilire quale dei due strumenti debba prevalere. La decisione del legislatore di non attribuire esplicitamente al Regolamento eIDAS lo stato di *lex specialis* rispetto al quadro normativo sulla protezione dei dati personali[51] contribuisce a complicare il dilemma interpretativo.

3.1.2. Incompatibilità dell'insieme minimo di dati con il principio della minimizzazione dei dati

Uno dei requisiti minimi richiesti dalla normativa per garantire l'interoperabilità tra i differenti regimi di identificazione elettronica degli Stati membri è quello di associare ad ogni identità elettronica un insieme minimo di dati di identificazione. Questo insieme viene dettagliato nel *Regolamento di esecuzione 2015/1501* della Commissione relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno [nel seguito, Regolamento di esecuzione eIDAS]. Come dettagliato nell'allegato al Regolamento di esecuzione eIDAS, questo insieme minimo di dati include il nome e cognome attuali dell'individuo, la sua data di nascita ed un identificativo univoco. Durante una transazione, questi dati vengono trasmessi tra le parti coinvolte per garantire l'autenticità dell'identità elettronica.

L'esistenza di un insieme minimo e obbligatorio di dati personali da associare alle identità elettroniche si pone direttamente in contrasto con il principio della minimizzazione dei dati sancito dal RGPD[52], che stabilisce che i dati oggetto di un trattamento debbano essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Non è difficile immaginare servizi che richiedano un numero di informazioni più limitato rispetto a quelle dell'insieme minimo di dati (basti pensare a servizi che richiedono solamente la verifica della maggiore età, senza necessità di conoscere l'esatta data di nascita dell'individuo).

Il tema della coerenza di eIDAS con il principio di minimizzazione dei dati è noto da tempo alla comuni-

tà accademica[53]. La stessa Commissione europea nel suo rapporto sulla valutazione degli impatti del Regolamento eIDAS menziona questo problema[54]. La proposta di emendamento al Regolamento eIDAS ha accolto queste osservazioni, introducendo alcune modifiche specifiche. Pur non abolendo l'insieme minimo di dati, la proposta di emendamento chiarisce che il «portafoglio europeo di identità digitale dovrebbe consentire, a livello tecnico, la divulgazione selettiva degli attributi alle parti facenti affidamento sulla certificazione [...], rafforzando in tal modo la praticità e la tutela dei dati personali, compresa la minimizzazione del trattamento di questi ultimi»[55]. Nonostante il Garante europeo della protezione dei dati abbia accolto con favore la scelta della proposta di emendamento[56], la decisione di limitare questo elemento ad un considerando, senza dedicare specifici articoli all'interno della norma, oltre al linguaggio utilizzato, aperto ad una interpretazione che lascia spazio di manovra ("dovrebbe consentire"), indebolisce la salvaguardia dei diritti degli interessati.

3.1.3. Disponibilità dei dati in caso di ritiro del portafoglio europeo di identità digitale

L'articolo 10-*bis* della proposta di emendamento al Regolamento eIDAS regola la sospensione, revoca o ritiro dei portafogli europei di identità digitali in caso di violazione o compromissione che possano pregiudicarne l'affidabilità o l'affidabilità di altri portafogli europei di identità. L'articolo prevede che a seguito di violazione o compromissione, lo Stato membro sospenda l'emissione e revochi la validità del portafoglio. Qualora non venga posto rimedio alla violazione o compromissione entro tre mesi, o qualora la violazione o compromissione risulti di particolare gravità, lo Stato membro ritira il portafoglio e comunica il ritiro agli altri Stati membri. L'articolo 10-*bis* della proposta di emendamento affianca e non sostituisce l'articolo 10 del Regolamento eIDAS, che sancisce simili disposizioni nel contesto di violazioni o compromissioni dei regimi di identificazione elettronica.

Come si evince sia dall'articolo 10-*bis* della proposta di emendamento che dall'articolo 10 del Regolamento eIDAS, sono previste tre misure a contenimento dei rischi. La sospensione dell'emissione del portafoglio o del regime di identificazione, la revoca della validità del portafoglio o del regime di identificazione ed il ritiro del portafoglio o del regime di identificazione. Il significato dei termini sospensione, revoca e ritiro in relazione ad una violazione o compromissione non viene precisato né dal Regolamento eIDAS né dalla proposta di emendamento. Il Regolamento eIDAS fornisce ulteriori elementi, precisando la distinzione tra il termina sospensione e revoca in relazione ai certificati qualificati, indicando che la «sospensione dei certificati qualificati è [...] diversa dalla revoca e comporta la perdita di validità temporanea di un certificato»[57]. Per estensione, è pertanto possibile affermare che quanto definito per i certificati qualificati possa essere applicato anche ai regimi di identificazione elettronica e ai portafogli europei di identità digitale implicando che, almeno per quanto riguarda la sospensione, la misura sia da intendersi come limitata nel tempo.

Il testo della norma non definisce i termini emissione e validità, che sono dunque da intendersi nel loro significato proprio. La Tabella 1 ricostruisce le diverse casistiche previste dal Regolamento eIDAS e dalla proposta di emendamento e propone una chiave interpretativa.

Come si evince dall'articolo 10 del Regolamento eIDAS e dall'articolo 10-*bis* della proposta di emendamento, è possibile identificare quattro casistiche che potrebbero configurare una impossibilità da parte degli utenti di accedere ai propri dati personali: in caso di revoca del regime di identificazione elettronica, di ritiro del regime di identificazione elettronica, di revoca della validità del portafoglio europeo di identità elettronica e di ritiro del portafoglio europeo di identità elettronica. Le due casistiche legate alla sospensione, invece, appaiono potenzialmente esenti in quanto, interrompendo il servizio solo in relazione a futuri utenti per i quali non sia ancora stato avviato alcun trattamento di dati personali, non configurerebbero alcuna violazione delle norme sulla protezione dei dati personali.

Negli altri casi, invece, l'impossibilità di accedere ai propri dati personali potrebbe configurarsi come una violazione del RGPD, che sancisce che debbano essere implementate misure che garantiscano la disponibilità dei sistemi e dei servizi[58]. Ovviamente, la necessità di tenere conto dei rischi per i diritti e le libertà delle persone fisiche non esclude a priori che la revoca o ritiro di suddetti strumenti possa essere compiuta in conformità al quadro normativo. Il titolare del trattamento è chiamato a svolgere una DPIA relativamente ai rischi derivanti dalla violazione o compromissione ed ai rischi derivanti dall'impossibilità per gli utenti di accedere ai proprio dati. Sulla base di tale valutazione dei rischi, il titolare determina le azioni da mettere in atto. Tuttavia, alcuni elementi concorrono a modificare le considerazioni sul rischio del titolare. Il primo concerne la tempestività di azione del titolare. Sia l'articolo 10 del Regolamento eIDAS che l'articolo 10-*bis* della proposta di emendamento prevedono che la revoca di, rispettivamente, regimi di identificazione elettro-

Strumento	*Articolo*	*Casistica*	*Durata*	*Proposta di interpretazione*
Regolamento eIDAS	Articolo 10	Sospensione del regime di identificazione elettronica	Temporanea	Interruzione temporanea nella distribuzione di nuove utenze associate al regime di identificazione elettronica
Regolamento eIDAS	Articolo 10	Revoca del regime di identificazione elettronica	Non specificata dalla norma	Interruzione del funzionamento del regime di identificazione elettronica
Regolamento eIDAS	Articolo 10	Ritiro del regime di identificazione elettronica	Non specificata dalla norma	Rimozione del regime di identificazione elettronica dalle liste notificate agli Stati membri
Proposta di emendamento al Regolamento eIDAS	Articolo 10-*bis*	Sospensione dell'emissione del portafoglio europeo di identità elettronica	Temporanea	Interruzione temporanea nella distribuzione di nuovi portafogli europei di identità elettronica all'utenza
Proposta di emendamento al Regolamento eIDAS	Articolo 10-*bis*	Revoca della validità del portafoglio europeo di identità elettronica	Non specificata dalla norma	Interruzione del funzionamento dei portafogli europei di identità elettronica
Proposta di emendamento al Regolamento eIDAS	Articolo 10-*bis*	Ritiro del portafoglio europeo di identità elettronica	Non specificata dalla norma	Rimozione dei portafogli europei di identità elettronica dalle liste notificate agli Stati membri

Tabella 1: Misure da adottarsi a seguito di violazione o compromissione e relativa proposta di interpretazione

nica e portafogli europei di identità digitale avvenga senza indugio in caso di violazione o compromissione. L'articolo 10-*bis* prevede anche che, in caso di violazione o compromissione di particolare gravità, il ritiro dei portafogli avvenga senza indugio. Questi elementi aggiungono fattori di rischio per i diritti e le libertà delle persone fisiche, in quanto non fornirebbero all'utente il tempo necessario a poter trasferire i suoi dati presso un altro regime o portafoglio. Inoltre, la mancata qualificazione di cosa costituirebbe una violazione o compromissione di particolare gravità ai sensi dell'articolo 10-*bis* della proposta di emendamento impone alle parti coinvolte di dover decidere autonomamente, senza possibilità di consultare organismi di supporto (quali, ad esempio, team nazionali di risposta incidenti informatici, autorità garanti per la privacy, etc.). Infatti, le disposizioni non forniscono alle parti coinvolte un orizzonte temporale sufficiente per svolgere attività di verifica dell'effettiva criticità della violazione o compromissione.

Il secondo elemento da tenere in considerazione durante l'analisi dei rischi è la durata prevista per le misure di mitigazione. Infatti, una misura temporanea pone minori rischi per i diritti e le libertà delle persone fisiche rispetto a una misura permanente. La mancata definizione della durata o, almeno, dell'indicazione se si tratti di misure temporanee o permanenti comporta una ulteriore difficoltà per il titolare del trattamento chiamato a svolgere una analisi dei rischi. Questa complessità è parzialmente indirizzata dalla *Decisione di esecuzione 2015/1984* della Commissione che definisce le circostanze, i formati e le procedure della notifica di cui all'articolo 9, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno [nel seguito, Decisione di esecuzione eIDAS]. Questo prevede che all'atto di notifica di un regime di identificazione elettronica da parte di uno Stato membro, quest'ultimo descriva «le disposizioni per la sospensione o la revoca del regime di identificazione elettronica notificato o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra»[59]. Il Regolamento eIDAS lascia dunque libertà agli Stati membri di dettagliare quanto concerne la sospensione e la revoca dei regimi di identificazione elettronica, creando ulteriore confusione.

La proposta di emendamento del Regolamento eIDAS dovrebbe introdurre modifiche volte a chiarire il quadro normativo in relazione ai punti di cui sopra. In particolare, dovrebbe specificare il significato dei termini utilizzati, precisando gli orizzonti temporali assegnati ad ognuno di questi, dovrebbe fornire ulteriori indicazioni sui parametri da valutare per stabilire la criticità di una violazione o compromissione. Inoltre, dovrebbe uniformare le disposizioni legate alla sospensione, revoca e ritiro dei regimi di identità elettronica e dei portafogli europei di identità digitali, rimuovendo tale decisione dalle prerogative degli Stati membri o, almeno, identificando dei parametri minimi che questi devono rispettare.

Inoltre, sarebbe opportuno che il regime eIDAS prevedesse delle soluzioni di continuità in caso di sospensione, revoca o ritiro. Ad esempio, potrebbe introdurre un regime di trasferimento automatico dei dati di un utente presso un diverso regime o portafoglio. Questo potrebbe prevedere un trasferimento nazionale qualora uno Stato membro abbia notificato più di un regime di identificazione elettronica o più di un portafoglio europeo di identità digitale, o un trasferimento transfrontaliero, qualora non vi siano altre soluzioni presenti sul territorio dello Stato membro. In quest'ultimo caso, eIDAS dovrebbe definire un quadro uniforme per la stipula di accordi tra Stati membri finalizzati specificamente a questa evenienza.

3.2. eIDAS e rischi di discriminazione

I rischi legati alla discriminazione derivano dal ruolo di primaria importanza che i sistemi di identificazione elettronica possono ricoprire nelle vite degli individui. Come dimostrato dalle vicende giudiziarie di paesi extra europei, si tratta di problemi tangibili che possono manifestarsi in relazione a problemi tecnici o procedurali, sistematizzare situazioni di discriminazione precedentemente esistenti, o esacerbare situazioni di discriminazione nei confronti degli individui più vulnerabili[60]. Una discriminazione si materializza concretamente nel momento in cui ad un individuo viene impedito di esercitare un diritto, come ad esempio la negazione di accesso ad un servizio pubblico. La disciplina europea in materia di identificazione elettronica risulta pertanto direttamente impattata da questo tema, in quanto stabilisce la modalità per garantire l'accesso transfrontaliero a servizi elettronici da parte dei cittadini. Inoltre, il problema risulta ancora più importante in virtù della strategia di armonizzazione dei sistemi digitali prevista dal *Regolamento (UE) 2018/1724* del Parlamento europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012 (nel seguito, Regolamento 2018/1724). Infatti, eventuali problematiche che dovessero portare a situazioni di discriminazione potrebbero risultare amplificate a seguito delle disposizioni del Regolamento 2018/1724, aumentando gli impatti per i diritti e le libertà degli individui. Il problema è emerso anche in ambito extra europeo. Il giudizio *Aadhaar* della Corte suprema indiana ha stabilito che l'esclusione di un individuo dai benefici e dai sussidi a cui avrebbe diritto è una violazione della sua dignità e dunque conduce ad una discriminazione[61]. Il giudizio indiano afferma anche che nonostante l'efficienza sia un elemento fondamentale dell'operato della pubblica amministrazione, non può essere considerata come una giustificazione per compromettere la dignità dell'individuo. Dunque, un sistema di identità digitale deve tendere all'inclusività più ampia possibile.

Per quanto riguarda il Regolamento eIDAS e la proposta di revisione, se da un lato il Regolatore europeo si dimostra attento ai problemi che possono affliggere persone soggette da disabilità, introducendo specifiche disposizioni sia nel Regolamento eIDAS[62] che nella proposta di revisione[63], dall'altro entrambi gli strumenti si rivelano carenti nell'istituire misure a salvaguardia degli individui dai rischi di discriminazione. Si consideri, ad esempio, il tema dell'alfabetizzazione digitale. Secondo il *Digital Economy and Society Index* (indicatore sulla economia e società digitale) 2021, il 13% della popolazione europea non possiederebbe alcuna competenza digitale, mente solo il 56% della popolazione possiederebbe livelli base di alfabetizzazione digitale[64]. Per quanto semplici possano venire progettati e realizzati, gli strumenti di identificazione elettronica, richiederanno sempre un certo livello di alfabetizzazione digitale. Anche ammettendo che tutta la fascia di popolazione a bassa alfabetizzazione sia in grado di utilizzare tali strumenti in maniera adeguata, il 13% senza alcuna alfabetizzazione – che corrisponde a più di 58 milioni di persone all'interno dell'Unione[65] – rimarrebbe escluso dalla possibilità di utilizzare tali strumenti. Pertanto, la scelta di non considerare questo punto all'interno del Regolamento eIDAS o della sua proposta di revisione appare problematico, visto il numero di individui potenzialmente impattato.

La normativa dovrebbe prevedere almeno l'esecuzione obbligatoria di una valutazione di impatto. Infatti, seppure sia possibile affermare che le casistiche ricomprese dal perimetro normativo del Regolamento eIDAS e della sua proposta di revisione soddisfino i requisiti minimi per attivare l'obbligo di svolgere una DPIA, rimane comunque un margine di discrezionalità che potrebbe comportare dei rischi residuali per gli individui.

4. Conclusione

Allo stato attuale, il quadro normativo legato all'identificazione elettronica presenta alcune problematiche derivanti dall'interazione con le norme riguardanti la protezione dei dati personali e dalla mancata considerazione di problemi legati alla discriminazione degli individui. Specificamente, il presente contributo analizza quattro di questi problemi. Il primo riguarda la sovrapposizione tra regimi di responsabilità previsti dal Regolamento eIDAS e dalla sua propo-

sta di revisione con quello previsto dal RGPD. Tale sovrapposizione rende più complessa l'identificazione dei ruoli delle parti coinvolte e l'attribuzione delle relative responsabilità. Il secondo deriva dall'incompatibilità tra l'esistenza di un insieme minimo di dati previsto per le identificazioni elettroniche e il principio di minimizzazione dei dati sancito dal RGPD. Il terzo riguarda i potenziali rischi di non conformità con il principio di disponibilità dei dati sancito dal RGPD di alcune azioni mitigative previste dal Regolamento eIDAS e dalla sua proposta di emendamento da attuarsi a seguito di compromissione o violazione degli strumenti di identificazione previsti da tali norme. Il quarto ed ultimo problema riguarda la mancanza di misure per indirizzare eventuali rischi di discriminazione connessi all'implementazione di misure di identificazione elettronica.

Pur presentando tali problemi, il quadro normativo non risulta compromesso. Nessuno dei problemi analizzati appare infatti bloccante e le incertezze interpretative possono essere risolte attraverso una maggior chiarezza del testo della norma. In tal senso il processo di revisione di eIDAS avviato dalla Commissione europea rappresenta l'opportunità per affrontare questi problemi e definire un nuovo quadro normativo più in linea con il RGPD e gli altri strumenti normativi comunitari.

Note

[1] European Commission, *Commission proposes a trusted and secure Digital Identity for all Europeans*, 3 June 2021.

[2] *Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea 2021*, COM(2021) 281 final del 3 giugno 2021.

[3] Si veda, a titolo di esempio, la bozza di risoluzione delle Nazioni Unite sul riconoscimento dei sistemi di identità nelle transazioni transfrontaliere. United Nations, *Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services 2021*, 26 January 2021.

[4] Si veda Oxford Economics, *Digital Services in Europe. An Evidence Review*, 2020.

[5] A questo si aggiungano altri strumenti legislativi attualmente in fase di definizione quali, ad esempio, la legge sui servizi digitali. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE 2020*, COM(2020) 825 final del 27 aprile 2021.

[6] Per informazioni relative all'attuale stato di lavorazione della proposta presso le istituzioni comunitarie si veda European Parliament - Legislative Observatory, *European Digital Identity Framework. 2021/0136(COD)*.

[7] Ai fini del presente contributo, i termini "elettronico" e "digitale" sono considerati sinonimi.

[8] *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*.

[9] A. Beduschi, *Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights*, in "Big Data & Society", July 2019.

[10] Oltre agli strumenti di identità digitale descritti dal presente contributo, il Regolamento eIDAS istituisce e regola svariati istituti utili ai servizi fiduciari elettronici nel Mercato unico digitale europeo.

[11] *Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (910/2014)*, art. 3.2.

[12] *Ivi*, art. 3.4.

[13] *Ivi*, art. 6.

[14] *Ivi*, art. 9.

[15] *Ivi*, art. 7.b.

[16] European Commission, *Commission Staff Working Document. Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) N. 910/2014 as Regards Establishing a Framework for a European Digital Identity*, 3 June 2021.

[17] Il rapporto sugli impatti del Regolamento eIDAS pubblicato dalla Commissione europea lamenta, alla data di pubblicazione, un tasso di adozione del 59%.

[18] European Commission, *Shaping Europe's Digital Future*, February 2020.

[19] COM(2021) 281 final, cit., art. 3.42.

[20] *Ivi*, art. 6-*bis*.1.

[21] Si veda ad esempio C. Allen, *The Path to Self-Sovereign Identity*, in "Life With Alacrity", 25 April 2016.

[22] *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati 1995 (95/46/CE)*.

[23] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, art. 4.1. Si noti che, come espresso dal Gruppo di lavoro articolo 29 per la protezione dei dati, il concetto di dato personale è da intendersi in maniera ampia e dinamica, piuttosto che come un insieme prestabilito di informazioni fisso nel tempo. Si veda Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 04/2007 sul concetto di dati personali*, giugno 2007.

[24] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 4.2.

[25] *Ivi*, art. 5.

[26] Oltre al consenso, il RGPD prevede cinque presupposti legittimi per il trattamento dei dati, e cioè quando il trattamento dei dati personali sia necessario per l'esecuzione di un contratto, per l'esecuzione di un compito connesso all'esercizio di pubblici poteri, per adempiere un obbligo legale, per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, o se necessario per la salvaguardia degli interessi vitali dell'interessato. *Ivi*, art. 6.1.

[27] *Ivi*, art. 5.1.a.

[28] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on Data Protection Law*, 2018, p. 133.

[29] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 12.

[30] *Ivi*, art. 5.1.b.

[31] Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 03/2013 sulla limitazione delle finalità*, 2 aprile 2013.

[32] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 5.1.c.
[33] *Ivi*, art. 5.1.d.
[34] *Ivi*, art. 5.1.e.
[35] CEDU, *S. e Marper c. Regno Unito*, 4 dicembre 2008, 3052/04, 30565/04.
[36] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 5.1.f.
[37] *Ivi*, art. 32.
[38] *Ivi*, art. 5.2.
[39] *Ibidem*.
[40] *Ivi*, considerando 74.
[41] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679*, 4 aprile 2017, p. 13.
[42] Si veda R. Gellert, *Understanding the Notion of Risk in the General Data Protection Regulation*, in "Computer Law & Security Review", vol. 34, 2018, n. 2, p. 279-288. Si veda anche J. Van Rest, R. Sanchez-Reillo, G. Whittaker et al., *Technical and Operational Issues Associated with Early Warning Zones for Critical Infrastructure*, Publications Office of the European Union, 2019, p. 109.
[43] Si veda a titolo di esempio A. Ortalda, N. Tsakalakis, L. Jasmontaite, *The European Commission Proposal Amending the eIDAS Regulation (EU) No 910/2014: A Personal Data Protection Perspective*, Brussels Privacy Hub, 24 December 2021, p. 5.
[44] Si vedano, a titolo di esempio, European Data Protection Supervisor, *Formal Comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity*, 28 July 2021; Comitato europeo delle Regioni, *Opinione: Identità digitale europea (2022/C 61/09)*, 21 ottobre 2021; Comitato economico e sociale, *e-ID (identificazione elettronica) (INT/951-EESC-2021)*, 20 ottobre 2021.
[45] AGID, *Regolamento eIDAS*, art. 3.3.
[46] *Ivi*, art. 7.d.
[47] *Ivi*, artt. 11.4, 11.5.
[48] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 82.4.
[49] *Ivi*, art. 5.d.
[50] AGID, *Regolamento eIDAS*, cit., art. 11.3.
[51] Soluzione che, al contrario, è stata applicata in altri strumenti europei. Si veda *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) 2002 (2002/56/CE)*, art. 1.
[52] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 5.c.
[53] Si veda N. Tsakalakis, S. Stalla-Bourdillon, K. O'hara, *Data Protection by Design for Cross-Border Electronic Identification: Does the EIDAS Interoperability Framework Need to Be Modernised?* in E. Kosta, J. Pierson, D. Slamanig et al. (eds.), "Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data", Springer, 2019.
[54] European Commission, *Commission Staff Working Document. Impact Assessment Report*, cit. «While eIDAS notified eIDs offer a high level of security, it has limitations as regards the principle of data minimisation. For authentication to online public services cross-border, it is compulsory to exchange the full minimum eIDAS data set and there is no possibility for the user to limit the transmitted personal data to the minimum required for a specific transaction».
[55] COM(2021) 281 final, cit., considerando 29.
[56] European Data Protection Supervisor, *Formal Comments of the EDPS*, cit. «The EDPS welcomes that the European Digital Identity Wallet will give the user better and transparent control on what data to share with whom for what purposes. The technical solution envisaged would be able to solve problems of excessive data processing, as it would allow the data subject to actually reveal only those data that are necessary for a specific purpose».
[57] AGID, *Regolamento eIDAS*, cit., considerando 53.
[58] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 32.1.
[59] Commissione europea, *Decisione di esecuzione 2015/1984 della Commissione che definisce le circostanze, i formati e le procedure della notifica di cui all'articolo 9, paragrafo 5, del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, 3 novembre 2015, art. 4.1.3.
[60] Si veda *A Guide to Litigating Identity Systems*, in "Privacy International", 15 September 2020.
[61] Si veda Supreme Court of India, *Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & Connected Matters*, 2018.
[62] AGID, *Regolamento eIDAS*, cit., art. 15.
[63] COM(2021) 281 final, cit., artt. 6-*bis*, 10, 15.
[64] European Commission, *The Digital Economy and Society Index*, 2022.
[65] Cfr. *Fatti e cifre sulla vita nell'Unione europea*.

* * *

Digital identity and protection of personal data: intersections and risks in the eIDAS and GDPR regulations

Abstract: The proposed amendment to the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) has reinvigorated the European debate on the issue of digital identity. The various problems that have emerged from this debate require better coordination of the proposal with pre-existing legislative instruments. This contribution aims to analyze the main points of friction between the regulatory framework related to electronic/digital identities and the European regulation concerning the protection of personal data.

Keywords: Electronic identity – Digital identity – eIDAS – GDPR

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0069
Articolo sottoposto a peer review

Diritto all'oblio e cooperazione internazionale: problemi e prospettive

Jacopo Ciani Sciolla

Data la natura ubiquitaria dei dati personali in rete, la pretesa di oblio esige necessariamente una risposta disancorata dai confini territoriali propri della giurisdizione adita. Complice l'ampia portata applicativa del GDPR, capace di travalicare i confini nazionali e rivolgersi a qualsiasi soggetto, anche residente al di fuori dell'Unione, sono stati emanati i primi ordini di cancellazione o di deindicizzazione aventi portata *cross-border*, ovvero efficacia esterna rispetto ai confini nazionali degli Stati membri. In assenza di strumenti normativi internazionali di armonizzazione del diritto all'oblio, le diverse tradizioni giuridiche nazionali in materia ostacolano la configurazione di una *global enforcement* del diritto. La cooperazione internazionale passa dunque per una armonizzazione sostanziale dell'istituto e dei suoi presupposti applicativi. I recenti arresti della Cassazione offrono spunti di riflessione, per delineare il diverso atteggiarsi del bilanciamento tra tutela dei dati personali e diritto all'informazione e definire la linea di confine tra oblio e diffamazione.

GDPR – Dati personali – Diritto all'oblio – Cancellazione – Deindicizzazione – Efficacia transnazionale dell'ordine giudiziale

Sommario: *1. L'impatto delle nuove tecnologie sui diritti della personalità: il caso del diritto all'oblio – 2. Il problema dell'efficacia transnazionale dell'ordine giudiziale di cancellazione dei dati personali – 2.1. La posizione della Corte di giustizia nel caso* Google c. CNIL *– 2.2. La posizione della Corte di giustizia nel caso* Glawischnig-Piesczek c. Facebook *– 2.3. Casi concreti di emissione di ordini giudiziali di deindicizzazione globale – 2.4. Le novità introdotte in materia dalla proposta di* Digital Service Act *– 2.5. Le reazioni alla posizione espressa dalla Corte di giustizia UE – 3. Verso un riconoscimento internazionale del diritto all'oblio – 4. Fori istituzionali per una governance globale del diritto all'oblio – 5. Assenza di un concetto unitario di diritto all'oblio e problemi classificatori – 6. Quale oblio? – 7. Il contributo della giurisprudenza italiana – 7.1. Rapporto tra diritto all'oblio e diritto all'immagine – 7.2. Condizioni di azionabilità del diritto all'oblio – 7.3. Ipotesi di classificazione del diritto all'oblio in funzione della specificità del diritto all'informazione contrapposto – 7.4. Specificità del bilanciamento con il diritto all'informazione in funzione della tipologia di diritto all'oblio invocata – 7.5. Coordinamento degli strumenti rimediali con l'ipotesi classificatoria*

1. L'impatto delle nuove tecnologie sui diritti della personalità: il caso del diritto all'oblio

Tra le tante questioni che investono la trasformazione digitale della società e la governance di Internet, il presente contributo affronta in particolare il tema dei diritti della personalità in rete e del rapporto tra la loro tutela e la libertà di manifestazione del pensiero. Le riflessioni degli studiosi e della giurisprudenza sul corretto equilibrio tra di essi si sono storicamente appuntate sul rispetto di due diritti cardini della

J. Ciani Sciolla è ricercatore in Filosofia del diritto e informatica giuridica presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Torino. L'autore ringrazia i proff. Ugo Pagallo e Massimo Durante per i commenti e le osservazioni al testo, di cui ha beneficiato la versione definitiva qui presentata.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

personalità: a) il diritto alla riservatezza della sfera privata[1]; b) il diritto al rispetto della propria immagine, della dignità, dell'onore e della reputazione della persona[2].

La trasformazione digitale ha di per sé giocato un ruolo di grande rilievo in questo ambito, comportando un incremento della pervasività e dannosità delle violazioni. I social network e i motori di ricerca hanno infatti amplificato la portata lesiva della diffusione di dati e informazioni in violazione di tali diritti.

Il progressivo mutamento delle tecnologie dell'informazione non ha tuttavia inciso unicamente sotto questo profilo. Può anzi dirsi che esso abbia contribuito a modificare profondamente lo scenario del rapporto tra i diritti in contesa[3].

La possibilità offerta dai motori di ricerca, muovendo dal nominativo di una persona, di accedere alla lista delle informazioni ad essa relative presenti in rete, ivi compresi tutti gli articoli di stampa contenuti negli archivi online di quotidiani e riviste (c.d. "total memory" ed "eternity effect" di Internet)[4], ha fatto luce su un orizzonte completamente nuovo del problema. Più precisamente, si è assistito all'emersione di un'istanza di riconoscimento di un diritto all'oblio, inteso come diritto dell'individuo a ottenere la deindicizzazione e, talvolta, la cancellazione dei propri dati personali da Internet, al fine di assicurare una rappresentazione corretta e attuale della propria identità digitale in rete.

Per quanto le origini dell'istituto siano indubbiamente anteriori[5], la dottrina ha infatti iniziato ad occuparsene massicciamente in coincidenza con la celebre decisione della Corte di giustizia nel caso *Google Spain*[6].

La codificazione dell'istituto nel GDPR, ove alla nozione di "diritto all'oblio" sono ricondotte una congerie del tutto eterogenea di diritti di cancellazione, ha di fatto creato non poca confusione attorno all'istituto[7], con la conseguenza che oggi non esiste una nozione unitaria e condivisa di diritto all'oblio ed è diventato persino arduo individuare le condizioni applicative o gli elementi costitutivi del diritto (che non sono tipizzate nel dettato normativo)[8]. A riprova di ciò, con un recente arresto la Cassazione civile ha definito il tema dei rapporti tra diritto all'oblio e libertà di informazione «assai complesso e non del tutto suscettibile di una "reductio ad unum"»[9].

Tali difficoltà si riverberano sui tentativi, già affacciatisi all'attenzione della Corte di giustizia dell'UE, di ottenere provvedimenti giudiziali aventi efficacia transnazionale, ovvero tali da consentire una piena realizzazione dell'oblio, indipendentemente dalla giurisdizione in cui siano ubicati i server ove sono conservati i dati personali oggetto della pretesa di cancellazione o deindicizzazione (par. 3).

In assenza di strumenti normativi internazionali di armonizzazione del diritto all'oblio, le differenti tradizioni giuridiche nazionali in materia, si pongono infatti come inevitabile ostacolo alla accettazione e configurazione di qualsivoglia pretesa di *global enforcement* del diritto.

In questo scenario, la cooperazione internazionale in materia di esecuzione *cross-border* dei provvedimenti giudiziali in materia di oblio non può prescindere da una armonizzazione sostanziale dell'istituto e dei suoi presupposti applicativi.

Questo rappresenta il tema centrale del presente contributo che è costruito come segue. Il par. 2 descrive il problema dell'efficacia transnazionale degli ordini giudiziali di cancellazione dei dati personali, anche mediante l'analisi delle pronunce *Google c. CNIL* e *Glawischnig-Piesczek c. Facebook*. Il par. 3 analizza l'approccio dei paesi extra-europei nei confronti del diritto all'oblio e gli sforzi della comunità internazionale tesi a dare riconoscimento effettivo a tale diritto. Il par. 4 individua le istituzioni internazionali che potrebbero giocare un ruolo di rilievo nella definizione di standard regolamentari condivisi, in vista di un rilancio della cooperazione internazionale in materia di *enforcement* del diritto all'oblio. Il par. 5 si sofferma sulla assenza di una nozione unitaria di diritto all'oblio e dà conto dei diversi sforzi classificatori e tassonomici profusi in dottrina. Rileva tuttavia come tali tentativi non abbiano apportato un sostanziale contributo alla definizione coerente e certa dei presupposti applicativi del diritto. Il par. 6 restringe l'area dell'analisi ad una nozione di oblio c.d. in senso stretto, mentre il par. 7 prova a fornire un contributo originale al dibattito. In particolare, prende le mosse da alcuni recenti arresti delle corti nazionali per iniziare a ragionare nella direzione di una definizione chiara di diritto all'oblio ed una classificazione precisa delle sue diverse forme di manifestazione, quali presupposti indefettibili per comprendere l'atteggiarsi del bilanciamento tra tutela dei dati personali e diritto all'informazione e individuare l'esatta linea di demarcazione tra diritto all'oblio e altri illeciti che attentano allo stesso bene giuridico: l'identità digitale del singolo.

2. Il problema dell'efficacia transnazionale dell'ordine giudiziale di cancellazione dei dati personali

Sin qui, anche in ragione del dibattito sorto attorno al caso *Google Spain* ed alla riforma del diritto alla

tutela dei dati personali portata dal GDPR, la letteratura si è occupata del diritto all'oblio come di un istituto di natura prettamente eurounitaria.

Data la natura ubiquitaria dei dati personali diffusi in rete, la pretesa di oblio esige però fisiologicamente una risposta disancorata dai confini territoriali propri della giurisdizione adita. Complice l'ampia portata applicativa del GDPR, capace di travalicare i confini nazionali degli Stati membri e rivolgersi a qualsiasi titolare o responsabile del trattamento, anche residente al di fuori dell'Unione[10], si è ben presto sentita l'esigenza di domandare in giudizio un ordine di cancellazione (o di deindicizzazione) dei dati personali avente portata *cross-border*, ovvero efficacia esterna rispetto ai confini nazionali degli Stati membri[11].

2.1. La posizione della Corte di giustizia nel caso *Google c. CNIL*

L'ammissibilità di un siffatto provvedimento è stata vagliata dalla Corte di giustizia UE su interpello del Conseil d'État francese, investito da Google dell'appello avverso una sanzione irrogata dalla Commissione nazionale per l'informatica e le libertà (CNIL), per essersi il motore di ricerca limitato a rimuovere i soli risultati ottenuti con ricerche effettuate a partire dagli Stati membri dell'UE, ad esclusione di quelle effettuate da domini extra-europei[12].

L'Avvocato generale Szpunar aveva proposto alla Corte di aderire alla tesi della differenziazione a seconda della collocazione geografica dell'utente, escludendo dall'obbligo di deindicizzazione i risultati ottenuti attraverso nomi di dominio relativi a paesi extra-europei, sul presupposto che il diritto all'oblio avrebbe fondamento giuridico ancorato al solo ordinamento europeo[13]. Di conseguenza, anche l'interesse concorrente della collettività ad essere informata dovrebbe considerarsi operante nei limiti dell'area europea. Una estensione a livello mondiale dell'ordine di deindicizzazione, viceversa, metterebbe in difficoltà le stesse Autorità dell'Unione che di fatto «non sarebbero in grado di definire e determinare un diritto a ricevere informazioni e, ancor meno, di bilanciarlo con gli altri diritti fondamentali alla protezione dei dati e alla vita privata»[14].

L'Avvocato generale denunciava dunque l'assenza di una governance globale del diritto all'oblio[15], quale presupposto necessario per l'efficacia transnazionale del diritto.

La Corte di giustizia ha deciso di allinearsi a tali conclusioni stabilendo che l'art. 12, lett. b) e 14, par. 1, lett. a) Dir. 95/46/CE e l'art. 17, par. 1 GDPR «devono essere interpretati nel senso che il gestore di un motore di ricerca, quando accoglie una domanda di deindicizzazione in applicazione delle suddette disposizioni, è tenuto ad effettuare tale deindicizzazione non in tutte le versioni del suo motore di ricerca, ma nelle versioni di tale motore corrispondenti a tutti gli Stati membri». Alla base del ragionamento della Corte vi è la considerazione che il diritto alla protezione dei dati personali «non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»[16]. Tale bilanciamento può variare in maniera anche sensibile da paese a paese[17] e gli strumenti di cooperazione interna previsti dagli artt. 56 e 60-66 GDPR a favore delle autorità di controllo nazionali, al fine di pervenire a soluzioni comuni in termini di bilanciamento tra tutela dei dati personali ed interesse della collettività ad essere informata, non coinvolgono paesi extra UE. Ne consegue che, allo stato attuale, non può darsi un obbligo a carico dei provider di procedere ad una deindicizzazione in tutte le versioni dei loro motori.

Conscia che limitazioni parziali di accesso alle informazioni mediante tecniche di geo-blocking basate sul riconoscimento dell'indirizzo IP possono essere agevolmente eluse[18], la Corte aggiunge però che il diritto dell'Unione «pur se [...] non impone [una deindicizzazione totale], neppure lo vieta». La Corte riconosce alle autorità di controllo o giudiziarie nazionali la competenza a richiedere ai motori di ricerca, nel rispetto delle normative interne, l'eliminazione dei link su tutti i domini a disposizione.

2.2. La posizione della Corte di giustizia nel caso *Glawischnig-Piesczek c. Facebook*

Problema analogo è stato affrontato a distanza di pochi giorni dalla Terza Sezione della stessa Corte, nel caso *Glawischnig-Piesczek c. Facebook Ireland Limited*, relativo alla pubblicazione sulla pagina personale di un utente del social network di un messaggio lesivo del diritto all'onore[19]. Alla Corte è stato chiesto se «l'art. 15 par. 1 della dir. 2000/31/CE, in materia di commercio elettronico che, pur in assenza di un dovere di sorveglianza, obbliga il prestatore di servizi di hosting (in tal caso Facebook) a rimuovere le informazioni illecite, di cui è venuto a conoscenza, sia ostativo alla efficacia mondiale della relativa ingiunzione». L'avvertita esigenza di offrire un'efficace e adeguata protezione ai diritti fondamentali della persona umana, pregiudicati in rete, portava la Corte ad affermare che «stante la dimensione mondiale dei servizi (cons. 52) elettronici», spetta al legislatore garantire la coerenza tra le norme dell'Unione europea e le norme di diritto internazionale, mentre il prestatore di servizi di hosting puo essere destina-

tario di un ordine diretto a rimuovere le informazioni oggetto dell'ingiunzione a livello mondiale.

2.3. Casi concreti di emissione di ordini giudiziali di deindicizzazione globale

Tale possibilità è stata percorsa dal Garante italiano, ancor prima che la Corte di giustizia si pronunciasse sul punto. L'autorità ha infatti ordinato a Google di «rimuovere ... gli URL ... fra i risultati di ricerca ottenuti digitando il nome e cognome del ricorrente, sia nelle versioni europee che extraeuropee, estendendo tale attività anche agli URL già deindicizzati nelle versioni europee di Google»[20]. Anche il Tribunale di Torino, in un caso di rimozione di contenuti per violazione di diritti di proprietà intellettuale, ha ritenuto che l'hosting provider dovesse rimuovere il contenuto illecito completamente dai propri sistemi (e da quelli dei fornitori con cui intrattenga accordi per la memorizzazione e la conservazione di contenuti), non potendosi limitare a oscurarlo dall'Italia, mediante tecniche di *geoblocking*, sul presupposto che «essi sono comunque visibili dall'estero ovvero dallo stesso territorio italiano con accorgimenti di facile approntamento (simulando cioè una connessione dall'estero)»[21].

2.4. Le novità introdotte in materia dalla proposta di *Digital Service Act*

Sul piano normativo, la problematica è ora affrontata dalla proposta di *Digital Service Act*[22] che all'art. 8 par. 1 lett. b) rubricato "Ordini di contrastare i contenuti illegali", prevede, tra le condizioni da soddisfare, che «l'ambito di applicazione territoriale dell'ordine, in base alle norme del diritto dell'Unione e nazionale applicabili, compresa la Carta, e, se del caso, ai principi generali del diritto internazionale, non va[da] al di là di quanto strettamente necessario per conseguire il suo obiettivo». La norma impone dunque all'autorità emanante di attenersi ai principi di legalità (l'ordine deve poggiare sulla base del diritto dell'Unione o nazionale applicabile che consente l'emissione dell'ordine) e di proporzionalità della misura. Il cons. 31 prende espressamente in considerazione la possibilità che l'ordine giudiziale «possa avere effetto oltre il territorio dello Stato membro dell'autorità in questione», ma non chiarisce se l'effetto extra-territoriale possa avere portata extra-UE. Nella prima direzione, parrebbe doversi leggere l'invito alle autorità emananti l'ordine a «valutare se le informazioni in questione possano costituire contenuti illegali in altri Stati membri interessati», con apparente esclusione, dunque, di una portata extra-UE dell'ordine. In senso contrario, lascerebbe invece intendere il successivo invito a tenere conto, ai fini di tale valutazione, «delle pertinenti norme del diritto dell'Unione o del diritto internazionale e degli interessi della cortesia internazionale». Infatti, se si considera che l'esecuzione di ordini giudiziali all'interno del mercato unico è regolato dal diritto dell'UE e precisamente dal Reg. n. 1215/2012[23], il riferimento al diritto internazionale e alla cortesia internazionale non potrebbe che leggersi nel senso di ammettere la possibilità di emanare ordini con portata territoriale extra-europea[24].

2.5. Le reazioni alla posizione espressa dalla Corte di giustizia UE

Le decisioni della Corte di giustizia (e il tema della tensione tra accessibilità globale della rete e principio di sovranità nazionale) hanno già ampiamente interessato il dibattito dottrinale[25] e sono state accolte per lo più con preoccupazione a livello internazionale. Si veda, a titolo esemplificativo, il comunicato formulato dal *Global Network Initiative*, l'organizzazione non-governativa fondata in occasione del sessantesimo anniversario della Dichiarazione universale dei diritti dell'uomo con l'obiettivo, tra gli altri, di salvaguardare la privacy degli individui in rete. L'organizzazione, che annovera tra i propri fondatori anche Google, Yahoo e Microsoft, ha accusato la Corte di aver fallito «to duly grapple with the possible impact of global injunctions on well-established and traditionally respected concepts related to sovereignty, conflict of law, and international comity» e ha invitato «supervisory/regulatory and judicial authorities around the world to refrain from asserting global jurisdiction on the Internet and imposing global removal orders». Per converso, ha raccomandato ai vari stakeholders di «work diligently to establish global standards, based on international law, that ensure the ongoing protection and promotion of freedom of expression and privacy online»[26].

Questo è l'invito che il presente lavoro intende coltivare. In assenza di strumenti normativi internazionali di armonizzazione del diritto all'oblio, le differenti tradizioni giuridiche nazionali in materia di diritto all'oblio e di bilanciamento tra questo nuovo diritto e i diritti c.d. di vecchia generazione sopra enunciati, si pongono come inevitabile ostacolo alla configurazione di una possibilità di efficacia globale degli ordini di cancellazione dei contenuti in rete. Occorre dunque, da un lato, verificare la sussistenza o creare *ex novo* basi comuni per intavolare un dialogo di cooperazione verso un riconoscimento internazionale ampio e condiviso del diritto all'oblio e dei relativi provvedimenti applicativi, dall'altro, in-

dividuare i fori istituzionali competenti e appropriati per farlo germogliare.

3. Verso un riconoscimento internazionale del diritto all'oblio

In dottrina sono stati condotti diversi studi di stampo comparatistico, finalizzati a fare il punto sul riconoscimento e sull'applicazione pratica del diritto all'oblio al di fuori dei confini europei. Garstka e Erdos hanno analizzato gli strumenti adottati in seno a diverse organizzazioni internazionali[27] e hanno riscontrato come tutte forniscano un supporto strutturale per un diritto all'oblio globale. Werro ha condotto uno studio comparatistico in quindici differenti giurisdizioni sulla base di un questionario comune, finalizzato a mettere in risalto elementi di contatto e di discontinuità[28].

Dall'esame dei quadri normativi sulla protezione dei dati personali di tutti i paesi del G20, è emerso che quindici su diciannove incorporano nella legislazione strumenti di opposizione alla disseminazione dei dati personali in rete a cagione della loro inaccuratezza[29], mentre quattordici anche per altre ragioni di illegittimità del trattamento.

Al di là degli strumenti di *soft law* adottati a livello pan-europeo dal Gruppo di lavoro ex art. 29[30] prima e dall'EDPB poi[31], anche le autorità di sorveglianza di diversi paesi extra-UE, tra cui Messico, Argentina, ma ancor più Australia, Canada, Russia e Turchia hanno offerto contributi interpretativi e linee guida[32].

Per quanto altri studi abbiano segnalato che al riconoscimento normativo del diritto all'oblio non corrisponda necessariamente una effettiva applicazione e permangono ancora sostanziali distanze rispetto all'alto livello di tutela europeo[33], il dato a colpire maggiormente è che l'oblio non viene più a configurarsi come un diritto unicamente europeo, ma comune alla maggioranza degli Stati membri del G20[34]. Tale convergenza si spiega non solo alla luce del c.d. "Effetto Bruxelles", ovvero la crescente capacità dell'Unione europea di dettare unilateralmente standard di regolazione per il mercato globale[35], ma anche con l'esigenza per gli Stati extra-europei di garantire un adeguato livello di protezione dei dati personali, al fine di abilitare il flusso di dati in entrata dall'Europa[36]. L'adeguatezza del livello di protezione garantito da un paese terzo, infatti, è valutata con riguardo (tra le altre circostanze) anche alle «norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi». Il mancato riconoscimento di un diritto all'oblio può pertanto determinare gli Stati membri ad adottare misure «per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione».

4. Fori istituzionali per una governance globale del diritto all'oblio

Ci si è altresì interrogati su quale potrebbe essere il foro ideale per favorire la cooperazione internazionale in materia di *enforcement* del diritto all'oblio. Erdos ha suggerito il Comitato consultivo sulla Convenzione 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale[37]. Tale organo riunisce, tra gli altri attori statali e non, anche otto paesi del G20 come membri e altri sette come osservatori e negli ultimi anni ha già preso parte alla redazione di linee guida in materia di protezione dei dati personali[38]. La circostanza che il diritto all'oblio trovi cittadinanza all'interno della Convenzione, porrebbe il Comitato in una posizione privilegiata per facilitare il raggiungimento di posizioni comuni.

Un altro foro potenzialmente candidato a condurre la cooperazione in materia è la *Global Privacy Assembly* (ex ICDPPC - *International Conference of data protection and privacy commissioners*) che riunisce la maggior parte delle autorità nazionali di sorveglianza in materia di protezione dei dati personali[39] e ha già emanato almeno due risoluzioni che toccano i problemi del diritto all'oblio[40]. Allo stato, tuttavia, difetta in tale contesto uno strumento normativo, anche solo di *soft law*, che costituisca la base comune per una discussione in materia.

L'efficacia del dialogo internazionale in materia presuppone però necessariamente una convergenza circa i requisiti sostanziali del diritto da eseguire.

5. Assenza di un concetto unitario di diritto all'oblio e problemi classificatori

Al di là delle critiche circa l'ingannevolezza del termine in sé e per sé[41], si è sottolineato come difetti allo stato attuale una nozione unitaria di diritto all'oblio. Non a caso, diversi autori hanno proposto una vera e propria tassonomia, utile a distinguere tra diritti aventi presupposti applicativi sostanzialmente differenti.

Rustad e Kulevska hanno suggerito di distinguere a seconda della provenienza dell'informazione

a) dal soggetto interessato, che la ha caricata direttamente in rete, salva la successiva ricondivisione da parte di terzi;
b) direttamente da soggetti terzi[42].

Secondo gli autori, il diritto all'oblio dovrebbe essere riconosciuto solo nel caso *sub* a) e ciò contribuirebbe a rendere compatibile l'istituto con il diritto statunitense che tradizionalmente osteggia qualsiasi limitazione della libertà di informazione protetta dal Primo Emendamento (c.d. *free speech*)[43]. La proposta finirebbe però per svuotare di gran parte del suo significato la tutela offerta dall'ordinamento europeo. Tale distinzione non pare perciò utile ad evidenziare differenti presupposti di tutela.

De Terwangne, basandosi sul diritto europeo ed in particolare sulla tradizione giuridica francese, ha individuato tre diverse fasi del diritto all'oblio:

a) *the right to oblivion of the judicial past*, che le corti transalpine riconoscono sin dal 1965[44];
b) *the right to oblivion established by data protection legislation* esteso a qualunque tipologia di dato personale (non più solo ai dati giudiziari) e collegato al principio di *purpose limitation*;
c) un *digital right to oblivion that amounts to personal data having an expiration date or being applicable in the specific context of social networks*[45]. Si tratterebbe di un diritto di cancellazione automatica dei dati in rete allo spirare di un determinato lasso temporale, con il pregio di dare oggettività e certezza del diritto e addossare l'onere di cancellazione direttamente ai provider come obbligo di *privacy by default*.

La proposta, tuttavia, finirebbe per elevare l'oblio a diritto assoluto, sancendone la prevalenza *ex lege* sulla libertà di espressione[46].

Sempre lo stesso autore ha distinto altresì, a seconda del rimedio offerto dall'ordinamento, tra:

a) *right to erase data*;
b) *right to anonymization* (cancellazione dei soli dati identificativi);
c) *right to erase the electronic links towards personal data*;
d) *right to restrict dissemination* (sui social network ad esempio)[47].

Prendendo spunto dalla classificazione proposta da De Terwangne e adattandola ad un contesto transnazionale, Voss ha individuato cinque diverse tipologie di oblio, che rispecchierebbero la varietà di approccio delle diverse giurisdizioni. Le prime due racchiudono il c.d. "oblio analogico", ovvero riferibile ancora alle forme di comunicazione tradizionale, a partire dalla stampa:

1. *Right to rehabilitation* ovvero il diritto alla cancellazione dei dati giudiziari, come forma di riabilitazione del condannato, decorso un certo periodo di tempo dalla condanna ed in presenza di buona condotta[48].
2. *Right to deletion/erasure* corrispondente al diritto alla cancellazione dei dati personali.

Seguono poi tre categorie che rispecchiano invece le esigenze proprie dell'"oblio in ambiente digitale":

3. *Right to delisting/delinking/de-indexing*, che integra l'estensione del diritto alla cancellazione ai motori di ricerca sancito dalla sentenza *Google Spain*.
4. *Right to obscurity*, che implica l'adozione di misure che rendano i dati personali più difficili da essere trovati[49]. Rientrano potenzialmente in tale categoria quelle misure, concesse anche da alcune corti nazionali, che consentono di mantenere l'informazione in rete, ma ne vietano l'indicizzazione da parte dei motori di ricerca.
5. *Right to digital oblivion of data collected by information society services* che l'autore identifica con il diritto alla cancellazione previsto dall'art. 17 lett. f) GDPR, concernente i dati personali del minore trattati per l'offerta diretta di servizi della società dell'informazione, che il legislatore ammette senza necessità di condizioni particolari.

Queste classificazioni nascono dall'osservazione empirica delle fattispecie in cui può essere invocato l'oblio e dei rimedi offerti dai legislatori o dalle corti, mentre non spiegano perché e a quali condizioni dovrebbe operare l'una piuttosto che l'altra fattispecie. Esse risultano pertanto sostanzialmente inutili ai fini della cooperazione internazionale in materia di esecuzione del diritto all'oblio che necessita – viceversa – di riconoscersi in basi giuridiche comuni per poter conferire validità alle decisioni emanate in diverse giurisdizioni e portarle ad esecuzione.

6. Quale oblio?

Per evitare di cadere nello stesso equivoco, occorre chiarire preliminarmente e sin d'ora che il presente contributo si riferirà esclusivamente ad un diritto all'oblio c.d. "in senso stretto", ovvero elaborato dal formante giurisprudenziale. Tale diritto, come si avrà modo di dire più approfonditamente di qui in avanti, consente di domandare la cancellazione di dati personali il cui trattamento non sia conforme alle disposizioni normative «in particolare a causa del carattere incompleto o inesatto dei dati»[50]. Tale condizione rende il trattamento incompatibile con le finalità per le quali i dati vengono rilevati e/o trattati, così generalmente ricadendo sotto il dettato dell'art. 17 par. 1 lett. a) GDPR, che impone al titolare del trattamento l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se «non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati».

Non si prenderanno in considerazione, invece, quelle fattispecie di oblio "in senso ampio" che non implichino alcun giudizio circa la qualità e accuratezza del dato trattato, ovvero circa la meritevolezza della finalità del trattamento. Sono dunque escluse dal raggio di indagine del presente contributo le ipotesi di oblio che consentono la cancellazione dei dati in forza:

i) di un'altra ragione di illiceità del trattamento diversa da quella sopra enunciata (art. 17 par. 1 lett. d), ivi compresa il venir meno di una qualsiasi base giuridica del trattamento *ex* art. 6 GDPR (art. 17 par. 1 lett. b), incluso l'interesse legittimo (art. 17 par. 1 lett. d);
ii) dell'esercizio di un diritto meramente potestativo del soggetto interessato (come nel caso di revoca del consenso *ex* art. 17 par. 1 lett. b o di trattamento di dati di minori *ex* art. 17 par. 1 lett. f);
iii) di un obbligo di legge gravante sul titolare del trattamento diverso da quello stabilito all'art. 17 GDPR (art. 17 par. 1 lett. e).

7. Il contributo della giurisprudenza italiana

Pur avendo ristretto sensibilmente il campo di indagine, le ipotesi di diritto all'oblio "in senso stretto", riconducibili all'art. 17 par. 1 lett. a), sono comunque molteplici. In Italia, uno sforzo classificatorio utile ad associare a ciascuna categoria individuata un determinato regime giuridico differenziale rispetto alle altre, in funzione del mutare della variabile associata al criterio classificatorio adottato, è stato compiuto dalla sentenza della Cassazione a Sezioni Unite, 22 luglio 2019, n. 19681, che ha provato a fare chiarezza sui presupposti applicativi del diritto all'oblio nel nostro paese[51].

La pronuncia trae origine dal rilievo formulato dalla Sezione Terza della Cassazione di una certa confusione circa i presupposti applicativi del diritto all'oblio, che portava a rimettere alle Sezioni Unite «l'individuazione di univoci criteri di riferimento che consentano agli operatori del diritto (ed ai consociati) di conoscere preventivamente i presupposti in presenza dei quali un soggetto ha diritto di chiedere che una notizia, a sé relativa, pur legittimamente diffusa in passato, non resti esposta a tempo indeterminato alla possibilità di nuova divulgazione»[52].

Le sentenza ha formulato il principio di diritto secondo cui «il diritto dell'interessato al mantenimento dell'anonimato sulla sua identità personale è prevalente, a meno che non sussista un rinnovato interesse pubblico ai fatti ovvero il protagonista abbia ricoperto o ricopra una funzione che lo renda pubblicamente noto». Ha però contestualmente avvertito che tale principio è dettato con riferimento e limitatamente ad un'ipotesi particolare di diritto all'oblio: quella di rievocazione di una notizia storica, priva di interesse attuale di cronaca.

Per tale ragione, la pronuncia è stata criticata[53] per essersi limitata a risolvere il particolare ed il contingente, piuttosto che a soddisfare le aspettative di chi contava su di un intervento chiarificatore, di portata generale. Si è rilevato, in particolare, come la Suprema Corte non abbia chiarito se e come tale principio di diritto possa essere trasposto o adattato anche alle altre fattispecie di diritto all'oblio, che la pronuncia individua in *obiter dictum* (e di cui a breve diremo).

La pronuncia solleverebbe, dunque, più interrogativi che non risposte. Nell'individuare nell'utilità sociale dell'informazione il criterio di bilanciamento con il contrapposto diritto di informare, il diritto all'oblio verrebbe a confondersi con l'illecito diffamatorio, che da tempo individua nell'interesse pubblico della notizia la chiave del bilanciamento tra diritto di cronaca e diritto all'onore e alla reputazione[54].

A mio avviso, la pronuncia ha – se non altro – avuto il merito di evidenziare un diritto all'oblio a più facce, ponendo il tema del diverso atteggiarsi del bilanciamento con la libertà di informazione, a seconda della fattispecie concreta che si ponga all'attenzione dell'interprete.

La sentenza inoltre offre un importante spunto di riflessione in merito alla delimitazione dei confini tra oblio e diffamazione.

Di entrambi gli aspetti, che i legislatori nazionali non potranno sottrarsi dal considerare nella ricerca di un consenso internazionale sui presupposti applicativi del diritto all'oblio, proverò a dare conto nei paragrafi che seguono.

7.1. Rapporto tra diritto all'oblio e diritto all'immagine

Nel caso all'attenzione della Corte di legittimità, l'attore aveva lamentato che la ripubblicazione di una notizia avesse generato un pregiudizio di tipo reputazionale. Le stesse corti territoriali, nel rigettare la pretesa di diritto all'oblio, avevano finito per concentrarsi sugli indici tipici della diffamazione (*in primis*, l'utilità sociale dell'informazione[55] e la continenza espressiva[56]), tanto da lasciar dubitare che si trattasse effettivamente di una fattispecie di oblio.

Le Sezioni Unite non hanno revocato in dubbio il corretto inquadramento giuridico della fattispecie da parte delle corti territoriali. La pronuncia offre dunque alcuni spunti utile per riflettere sul rappor-

to (*rectius* sulla demarcazione) tra oblio e diffamazione, se si considera che giurisprudenza e dottrina sono concordi nel ritenere che si tratti di illeciti ben distinti[57].

7.1.1. La comunanza di bene giuridico protetto

La confusione tra le due fattispecie nasce dalla parziale comunanza di bene giuridico protetto[58]. In entrambi i casi si tratta dell'identità personale nella sua proiezione sociale[59]. É ricorrente l'idea che tale bene giuridico venga in considerazione nelle due fattispecie in due dimensioni differenti:

a) nel diritto all'oblio, quella del diritto alla riservatezza ed al controllo dei propri dati personali e all'autodeterminazione informativa, intesa come diritto del singolo di decidere se ed entro quali limiti rendere noti fatti legati alla propria vita personale;
b) nella diffamazione, quella del diritto alla salvaguardia dell'onore, della reputazione e della dignità della persona.

La Cassazione ha tuttavia confutato tale assunto. Mentre senz'altro l'oblio ha a che fare con l'interesse *sub* a), ciò che traspare dalla giurisprudenza di legittimità è l'idea che anche il diritto all'oblio, come la diffamazione, presupponga, in realtà, una lesione della reputazione[60]. Il diritto all'oblio, dunque, verrebbe a configurarsi come un illecito pluri-offensivo, aggredendo non solo la riservatezza e l'autodeterminazione informazionale, ma anche la reputazione.

7.1.2. La natura della lesione al bene giuridico protetto ed il test da applicarsi per disambiguare le rispettive fattispecie di illecito

Il *discrimen* tra le due fattispecie di illecito sarebbe dato, dunque, non tanto dal bene giuridico protetto (che in buona parte coincide), ma dalla natura della lesione, che si presenta ontologicamente diversa nelle due ipotesi di illecito. Infatti, nel diritto all'oblio l'evento lesivo si consuma necessariamente:

a) per effetto di un trattamento illecito di dati personali;
b) che sia avvenuto decorso un certo periodo di tempo dalla prima pubblicazione del contenuto che ospita tali dati.

L'eventuale diffamazione, invece, richiede una lesione della reputazione, sussistente già al momento della prima pubblicazione.

Il test da effettuare è dunque duplice.

In primo luogo, le due fattispecie si distinguono, in linea di massima, perché solo il diritto all'oblio richiede necessariamente che il contenuto lesivo ponga in essere un trattamento di dati personali. Viceversa, la diffamazione può venire in essere anche in assenza di tale trattamento, a condizione però che il soggetto interessato sia comunque identificabile[61]. Si tratta di una distinzione sottilissima e il più delle volte assente: di regola, infatti, entrambe le fattispecie si troveranno accomunate dalla sussistenza di un trattamento di dati personali. La riconoscibilità della persona offesa, necessaria ai fini della sussistenza di una diffamazione, sovente, discenderà proprio dalla divulgazione di dati personali (che, per definizione, consentono proprio l'identificabilità del soggetto leso) e solo raramente sarà possibile anche in assenza di questi. É dunque ben possibile che una fattispecie di diffamazione e di diritto all'oblio possano venire ad innestarsi sul medesimo contenuto, a condizione che questo presenti un trattamento di dati personali. Al fine di distinguere le due fattispecie non basta più allora la sussistenza di una ipotesi di trattamento di dati personali, occorrendo un *quid pluris*.

In secondo luogo, occorre distinguere a seconda che il pregiudizio alla reputazione derivi: a) dal contenuto della notizia, inveritiero o non accurato o contenente dati personali che avrebbero dovuto essere omessi; b) dalla sua forma esteriore o espressiva, incontinente, ovvero volgare, oltraggiosa, gratuitamente aggressiva. Mentre l'ipotesi *sub* a) è ascrivibile in astratto sia ad una fattispecie di diritto all'oblio, sia di diffamazione, l'ipotesi *sub* b) è necessariamente riconducibile solo all'illecito diffamatorio.

In terzo luogo, e con riferimento alla fattispecie *sub* a), in cui i due illeciti trovano ancora terreno di sovrapposizione, il *discrimen* va ravvisato nella rilevanza del decorrere del tempo. Nel diritto all'oblio, il fatto illecito verrebbe necessariamente in essere solo decorso del tempo dalla prima pubblicazione della notizia. Mentre una notizia inveritiera sin dalla sua prima divulgazione (dunque *ex tunc*) integrerebbe una ipotesi di diffamazione, il diritto all'oblio viene in essere quando la stessa notizia, originariamente lecita, acquisti efficacia lesiva della reputazione dell'individuo in un secondo momento, ovvero all'atto della sua ripubblicazione (dunque *ex nunc*)[62]. Il decorso del tempo rappresenta dunque senz'altro un elemento costitutivo del diritto all'oblio[63], nel senso che in mancanza non verrebbero in essere i presupposti di diritto per ottenere la cancellazione dei propri dati personali.

7.1.3. La rilevanza dell'interesse pubblico della notizia

Oblio e diffamazione sono poi accomunati dal venire entrambi ad interferire con il diritto concorrente del terzo ad informarsi. Questo incrocio, unitamente alla

identità del bene giuridico tutelato (la reputazione) spiega la rilevanza comune dell'interesse pubblico della notizia. Essendo il diritto all'oblio e il diritto alla reputazione due facce della stessa medaglia (il diritto all'identità personale), il loro bilanciamento con il diritto all'informazione non può prescindere dalla valutazione dell'utilità dell'informazione. L'interesse pubblico all'informazione è dunque parte integrante del bilanciamento tra questi diritti, con la conseguenza che non è nella presenza o nell'assenza di esso che può rintracciarsi il *discrimen* tra oblio e diffamazione.

Ciò spiega perché le Sezioni Unite abbiano enunciato un principio di diritto in materia di diritto all'oblio che ben potrebbe trovare applicazione ad una fattispecie di diffamazione, così esponendosi alla critica di ingenerare confusione tra le due fattispecie. Queste, seppur accomunate dall'essere entrambe strumenti di tutela dell'identità personale latamente intesa, devono necessariamente rimanere distinte, poggiando su presupposti applicativi differenti.

7.2. Condizioni di azionabilità del diritto all'oblio

Chiarita la linea di demarcazione tra diffamazione e diritto all'oblio, occorre ora chiarire meglio quali siano i presupposti costitutivi particolari del diritto all'oblio.

Vengono in soccorso, a riguardo, più risalenti pronunce della stessa Cassazione[64].

Il diritto all'oblio "in senso stretto" (v. par. 6) integra un trattamento illecito di dati personali derivante dalla violazione del principio di finalità del trattamento (o limitazione della finalità), che, ai sensi dell'art. 5 par. 1 lett. b) GDPR, costituisce un vero e proprio limite intrinseco del trattamento lecito dei dati personali[65]. Tale violazione si estrinseca nel venir meno di «una stretta correlazione temporale tra l'identificabilità del titolare dei dati e la finalità del relativo trattamento». L'identificabilità del soggetto titolare dei dati è «normativamente astretta dai rigorosi limiti temporali per i quali è giustificata ("per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati": D.Lgs. n. 196 del 2003, art. 11, comma 1, lett. e))». Se del dato è consentita la conservazione per finalità anche diversa da quella che ne ha originariamente giustificato il trattamento (ad esempio il passaggio da un archivio ad un altro), nonché la memorizzazione (anche) nella rete di Internet (es. pubblicazione online degli archivi storici dei giornali), tali nuove finalità devono essere compatibili con quella originaria. In caso contrario il nuovo trattamento necessita di nuova base giuridica. Per stabilire la compatibilità della nuova finalità occorre tenere conto, tra l'altro, «della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali oppure se siano trattati dati relativi a condanne penali e a reati», «delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati», nonché «dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione»[66].

Il Gruppo di lavoro ex art. 29, nell'interpretare tali fattori, ha precisato che «devono essere presi in considerazione anche gli impatti emotivi, come l'irritazione, la paura e l'angoscia che possono derivare da una persona interessata che perde il controllo sulle informazioni personali o si rende conto che sono state compromesse». Un impatto rilevante in senso lato può derivare, tra le altre cose, «se i dati sono comunicati al pubblico o altrimenti resi accessibili a un numero elevato di persone»: circostanza che tipicamente si verifica in ipotesi di ripubblicazione in rete di una notizia originariamente diffusa su mezzi analogici e della sua memorizzazione nei risultati di un motore di ricerca.

La compatibilità è espressamente presa in considerazione dal legislatore in ipotesi di nuovo trattamento per finalità di archiviazione. L'art. 89 GDPR richiede che il trattamento a fini di archiviazione nel pubblico interesse, sia «soggetto a garanzie adeguate per i diritti e le libertà dell'interessato», che assicurino «che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati». In particolare, tali misure implicano, quando possibile, anche di non consentire più di identificare l'interessato. Infatti, osserva il Garante europeo, gli storici sono «spesso più interessati ai fatti che all'identità precisa delle persone interessate (e per questi casi possono essere spesso appropriati dati anonimi o pseudonimizzati)». Solo nei casi in cui la notizia si concentri su «individui specifici, come personaggi storici», può risultare giustificato l'utilizzo di dati identificativi.

Il trattamento non è compatibile con le nuove finalità ed è soggetto a diritto all'oblio quando i dati ripubblicati non siano più esatti e aggiornati, pertinenti e completi in relazione alle finalità del trattamento. In difetto dei predetti requisiti, deve ritenersi insussistente l'interesse pubblico all'informazione che integrava la finalità iniziale del trattamento. Se, infatti, la finalità del trattamento iniziale dei dati personali è informare e portare a conoscenza la notizia, il trattamento successivo, che – per essere giustificato – deve poggiare su una analoga finalità di persistente interesse pubblico alla conoscenza della

notizia, non può prescindere dalla sua contestualizzazione «in relazione ai successivi sviluppi della medesima». Lo spostamento della notizia in archivio, con memorizzazione anche nella rete Internet, in altre parole, «deve essere realizzato con modalità tali da consentire alla medesima di continuare a mantenere i suindicati caratteri di verità ed esattezza, e conseguentemente di liceità e correttezza, mediante il relativo aggiornamento e contestualizzazione». Solo in tal modo essa risulterà non violativa del diritto all'identità personale del titolare del dato oggetto di trattamento, nonché dello stesso diritto del cittadino utente a ricevere una informazione completa e corretta. In caso contrario, infatti, verrebbero inevitabilmente meno sia l'interesse pubblico alla notizia, sia lo scopo del trattamento.

Alla luce di tale ricostruzione, il requisito costitutivo del diritto all'oblio "in senso stretto" è l'illiceità del trattamento per violazione del principio di finalità del trattamento, a causa del mutamento di tale finalità, decorso un certo lasso di tempo dal trattamento originario.

7.3. Ipotesi di classificazione del diritto all'oblio in funzione della specificità del diritto all'informazione contrapposto

Nel quadro appena tratteggiato, l'interesse pubblico all'informazione rileva in quanto finalità del trattamento, la cui persistenza è l'oggetto precipuo di valutazione, nel bilanciamento tra diritto alla riservatezza e diritto all'informazione. Questo può atteggiarsi in modo differente a seconda della fattispecie concreta di diritto all'oblio che viene in essere.

Nella specie, le Sezioni Unite, 22 luglio 2019, n. 19681 hanno ritenuto di distinguere "tre differenti situazioni" di diritto all'oblio[67]:

a) Il "caso classico" della "ripubblicazione" a mezzo giornalistico «di quanto già a suo tempo diffuso senza contestazioni», rimanendo «perciò escluso ogni collegamento con i problemi posti dalla moderna tecnologia e dall'uso della rete internet». Tale fattispecie, presenta al suo interno due ulteriori varianti:
   a.1 il caso in cui, in relazione ad un evento del passato, intervengano elementi nuovi tali per cui la notizia ritorni di attualità, di modo che si decida di diffonderla nel momento presente e che ciò rappresenti ancora una manifestazione del diritto di cronaca[68];
   a.2 il caso in cui la notizia venga ripubblicata senza che siano intervenuti fatti nuovi idonei a rendere la notizia attuale, con la conseguenza che l'interesse pubblico alla sua diffusione resta ancorato al *dies a quo* della sua prima diffusione. In assenza di interesse pubblico, tornare a diffondere una notizia del passato, anche se di sicura importanza in allora, costituisce esplicazione di un'attività storiografica, che gode conseguentemente di diverse garanzie costituzionali rispetto al diritto di cronaca.
b) L'ipotesi di "reperibilità di notizie in rete" non già perché nuovamente ripubblicate ovvero citate in un diverso articolo di stampa pubblicato su un numero corrente, ma solo in ragione della permanenza della medesima nella memoria della rete Internet e, a monte, nell'archivio del titolare del sito sorgente.
c) Le ipotesi di pubblicazione del nome dell'interessato nell'elenco dei risultati reperibili su un determinato motore di ricerca.

Alcuni autori hanno rilevato che, soprattutto l'ultima fattispecie, integrerebbe un autonomo e distinto diritto «segnatamente il diritto alla disassociazione del proprio nome da un dato risultato di ricerca ... diverso dal diritto ad essere dimenticato, che coinvolge e richiede una valutazione di contrapposti interessi» differenti. Nel caso del diritto alla dissociazione, infatti, al soggetto interessato non si contrapporrebbe l'interesse del divulgatore della notizia, bensì quello del motore di ricerca che renda la notizia pubblicata sul web maggiormente e piu agevolmente fruibile.

Alla luce di quanto detto in precedenza, deve concludersi, al contrario, che i requisiti costitutivi della tutela dovrebbero essere individuati in maniera unitaria nelle tre fattispecie.

Passibile di differenziazione è invece il test con cui tale diritto è posto in bilanciamento con i diritti concorrenti di terzi, i quali effettivamente, costituendo il criterio discretivo della classificazione, risultano differenti in ciascuna ipotesi di diritto all'oblio presa in considerazione.

In sostanza, tutte le ipotesi di oblio individuate *sub* a), b) e c) implicano un bilanciamento tra diritto alla tutela del dato personale e diritto all'informazione, nella sua duplice dimensione attiva e passiva di diritto di informare e di essere informati[69]. Quest'ultimo, tuttavia, viene ad essere declinato differentemente in ciascuna delle tre ipotesi.

Nella ipotesi *sub* a), esso si configura come diritto di cronaca o come diritto alla rievocazione storica (storiografica) di un fatto. Precisamente, nella fattispecie *sub* a.1), in cui sussiste un interesse pubblico attuale alla rievocazione di un evento del passato, si è in presenza di una manifestazione del diritto di cronaca. Al contrario, nell'ipotesi *sub* a.2), «in assenza di questi elementi, tornare a diffondere una notizia

del passato, anche se di sicura importanza in allora, costituisce esplicazione di un'attività storiografica».

Nelle ipotesi *sub* b) e c), l'interesse contrapposto si identifica con il diritto alla conoscenza di una notizia storica per effetto, nella ipotesi *sub* b), della consultazione di un archivio, che costituisce invero la fonte dell'informazione (c.d. siti sorgente), nell'ipotesi *sub* c), della consultazione della memoria della rete Internet tramite motore di ricerca, che è invece «un mero intermediario telematico, che offre un sistema automatico di reperimento di dati e informazioni attraverso parole chiave, un mero database che indicizza i testi sulla rete e offre agli utenti un accesso per la relativa consultazione».

Le differenze tra le suddette ipotesi sono significative, perché al mutare delle caratteristiche del mezzo di accesso all'informazione, muta anche l'atteggiarsi del bilanciamento tra diritto all'oblio e diritto di essere informati.

7.4. Specificità del bilanciamento con il diritto all'informazione in funzione della tipologia di diritto all'oblio invocata

Come detto, dunque, le tre ipotesi di diritto all'oblio presentano presupposti analoghi. Differiscono però nella valutazione dell'ultimo presupposto che è quello concernente la presenza di eventuali cause di giustificazione. Tutte le ipotesi di diritto all'oblio, infatti, prevedono la possibilità che il trattamento dei dati personali sia lecito perché effettuato nell'esercizio del prevalente diritto all'informazione, così come di volta in volta declinato secondo lo schema che precede.

Il punto sta nel fatto che tale causa di giustificazione ha portata più o meno ampia proprio a seconda della specificità del diritto che si invoca e ciò in quanto muta il bilanciamento che l'organo giudicante è chiamato a porre in essere tra i contrapposti diritti costituzionali all'identità personale e all'informazione.

Occorre dunque analizzare quali siano le variabili: come – in altre parole – si atteggi diffomemente tale bilanciamento in ciascuna ipotesi particolare di diritto all'oblio.

L'ipotesi *sub* a.1) è quella in cui l'esercizio del diritto all'oblio implica il bilanciamento tradizionale tra diritto alla riservatezza e diritto di cronaca. Si tratta dell'ipotesi in assoluto più sfavorevole al soggetto interessato esercente il diritto all'oblio. L'interesse pubblico ancora attuale alla rievocazione della notizia contenente i dati personali premia, infatti, in termini di prevalenza, il diritto di cronaca. Questo in particolare giustifica il riferimento ai dati identificativi della persona, essenziali ai fini di una piena informazione e comprensione della notizia di cronaca.

L'ipotesi *sub* a.2) è quella presa in considerazione dalle Sezioni Unite e prevede il bilanciamento tra diritto alla riservatezza e diritto di rievocazione storica. Tale bilanciamento è più favorevole al diritto all'oblio, che non nel caso che precede. Ciò in quanto, le stesse Sezioni Unite riconoscono che il diritto alla rievocazione storica «non puo godere della stessa garanzia costituzionale che è prevista per il diritto di cronaca». Conseguentemente, la compressione del diritto alla riservatezza sarà inferiore rispetto al caso in cui sussista un interesse attuale alla pubblicazione della notizia contenente i dati personali. Ne deriva, in particolare, che la rievocazione «deve svolgersi in forma anonima, perché nessuna particolare utilità puo trarre chi fruisce di quell'informazione dalla circostanza che siano individuati in modo preciso coloro i quali tali atti hanno compiuto»[70]. Il diritto all'oblio prevarrà dunque ogniqualvolta siano trattati i dati identificativi della persona, a meno che non sussista comunque un «interesse alla conoscenza dell'identità della singola persona che quel fatto ha compiuto», nonostante la finalità meramente rievocativa[71]. Tale interesse sussisterà, in particolare, allorché il fatto rievocato «riguardi personaggi che hanno rivestito o rivestono tuttora un ruolo pubblico, ovvero fatti che per il loro stesso concreto svolgersi implichino il richiamo necessario ai nomi dei protagonisti»[72]. In altre parole, il diritto di rievocazione storica, per prevalere sul diritto all'oblio, richiede che non vi sia l'identificazione personale del soggetto interessato, ovvero che questa non sia «irrilevante, per i destinatari dell'informazione, una volta che il tempo sia trascorso e i fatti, anche se gravi, si siano sbiaditi nella memoria collettiva».

L'ipotesi *sub* b) prevede che l'informazione sia rintracciabile mediante archivio o banca dati. Qui il bilanciamento di interessi si atteggia differentemente rispetto all'opzione *sub* c), in ragione delle differenti caratteristiche del mezzo su cui è reperibile l'informazione. L'archivio «si caratterizza per essere ordinato secondo criteri determinati, con informazioni intercorrelate volte ad agevolarne l'accesso e a consentirne la consultazione, la rete internet costituisce in realtà un ente ove le informazioni non sono archiviate ma solo memorizzate ... Nella rete internet le informazioni non sono in realtà organizzate e strutturate, ma risultano isolate, poste tutte al medesimo livello ("appiattite"), senza una valutazione del relativo peso, e prive di contestualizzazione, prive di collegamento con altre informazioni pubblicate (come segnalato anche in dottrina, lo stesso *pagerank* indica quando una pagina è collegata da link, non a quali informazioni essa debba essere correlata, né fornisce alcun dato sulla qualità dell'informazione)».

Conseguentemente, la memorizzazione in archivio facilita la ricerca della informazione corretta rispetto alla rete che pone «l'esigenza di attribuzione della fonte dell'informazione ad un soggetto, della relativa affidabilità, della qualità e della correttezza dell'informazione»[73]. Il bilanciamento di interessi sarà dunque più favorevole all'oblio nell'ipotesi di informazione reperibile in rete, mentre viceversa, quando le informazioni siano contenute in archivio la pretesa di oblio sarà meno giustificata.

L'ipotesi *sub* c) è stata fatta oggetto delle argomentazioni svolte dalla Corte di giustizia nel caso *Google Spain* e dei principi contenuti nelle Linee Guida interpretative del Gruppo ex art. 29. Si tratta, inoltre, dell'ipotesi probabilmente più sviscerata in letteratura. La Corte ha evidenziato come le libertà fondamentali della persona interessata – segnatamente il suo diritto al rispetto della sua vita privata con riguardo al trattamento dei dati personali, «prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi». Nel conciso riferimento all'individuazione dei parametri per la rimozione dei risultati della ricerca[74], la Corte indica gli elementi del tempo e del ruolo ricoperto dall'interessato nella vita pubblica. Nel bilanciamento dei contrapposti interessi, la Corte chiarisce come, a prescindere dall'esistenza di un pregiudizio per l'interessato, la tutela sia fortemente sbilanciata in favore del diritto alla protezione dei dati personali. Unico limite per l'accoglibilità della richiesta di oblio è rappresentato dalle caratteristiche dei dati o degli interessati ai quali i dati si riferiscono (con particolare riguardo al carattere pubblico dell'interessato)[75].

La giurisprudenza nazionale ha svolto alcune precisazioni, funzionali ad inquadrare correttamente i termini del predetto bilanciamento. Ha precisato, in particolare, che i motori di ricerca, pur svolgendo un ruolo decisivo nella diffusione globale dei dati[76] e contribuendo a rendere piu effettivo il diritto all'informazione, «forniscono informazioni diverse ed assai piu invasive rispetto a quelle fornite dai siti sorgente»[77]. La maggiore incidenza ed invasività delle informazioni veicolate dal motore di ricerca giustifica la maggiore protezione accordata all'interessato e alla sua identità personale, rispetto all'interesse degli utenti ad acquisire elementi informativi che non sono piu quelli originari.

7.5. Coordinamento degli strumenti rimediali con l'ipotesi classificatoria

Dato questo quadro, risulta più agevole collocare gli strumenti rimediali offerti dall'ordinamento.

Occorre distinguere due ipotesi.

i) Nel caso in cui il nuovo trattamento non sia compatibile con la finalità originaria e sia venuto meno *tout court* l'interesse pubblico alla ripubblicazione, i dati personali dovranno essere necessariamente soggetti ad ordine di cancellazione, a meno che non si faccia luogo allo spostamento della notizia di cronaca di cui trattasi in area non indicizzabile dai motori di ricerca, mediante rimozione dei relativi tag. Con riferimento ai motori di ricerca, invece, il rimedio ipotizzabile è il delisting del risultato di ricerca.

ii) Viceversa, qualora sussista l'interesse pubblico alla ripubblicazione e dunque il nuovo trattamento sia astrattamente compatibile con quello originario, ma sia stato posto in essere senza provvedere al necessario adeguamento della notizia, il titolare dell'archivio o del sito web potrà conseguire *ex post* le indicate finalità. All'interessato va dunque riconosciuto il diritto di ottenere l'integrazione ovvero l'aggiornamento della notizia a lui relativa[78], mediante inserimento di notizie successive o nuove rispetto a quelle esistenti al momento iniziale del trattamento, quali la segnalazione (nel corpo o a margine) della sussistenza di un seguito e di uno sviluppo della notizia, con funzione di ripristino dell'ordine del sistema informativo alterato dalla notizia parziale, in maniera del tutto analoga a quanto avviene mediante la rettifica in ipotesi di diffamazione (ad ulteriore evidenza della affinità tra le fattispecie sopra discussa). Tale rimedio, presenta il pregio di garantire altresì «la totale sovrapponibilità, altrimenti irrimediabilmente compromessa, fra l'archivio cartaceo e quello informatico del medesimo giornale, funzionale al diritto della collettività ad essere informata correttamente sulle relative vicende»[79]. Sempre in parallelo, con riferimento ai motori di ricerca, è ammessa la modifica dell'abstract (o *description line*) sottostante al link, qualora possa risultare fuorviante, in quanto non in linea con la narrazione dei fatti riportati nell'articolo[80].

Il rimedio da adottare è dunque strettamente correlato al bilanciamento tra diritti poiché tanto più è forte il diritto all'oblio, tanto maggiore sarà l'inge-

renza, in termini di rimedio ammissibile, nella libertà di informazione dei terzi.

In questi termini, si è pronunciata di recente la Corte europea dei diritti dell'uomo che, nel ritenere legittimo l'operato della giurisdizione nazionale, ha valutato favorevolmente, tra l'altro, che non fosse stato imposto al ricorrente di rimuovere definitivamente l'articolo da Internet, ma solo di deindicizzarne i tag[81]. Ciò verosimilmente porterà i giudici a favorire, ove possibile, rimedi meno invasivi della cancellazione, in omaggio al principio di proporzionalità, così giustificando l'affermazione di chi vede oggi il diritto all'oblio sempre più come il «diritto a non essere trovati facilmente», piuttosto che come il diritto ad essere dimenticati[82]. Tale tendenza è già ravvisabile dall'esame della giurisprudenza di legittimità[83].

In attesa di verificare, con approccio comparatistico, quanto la configurazione del diritto all'oblio e la sua classificazione in tre distinte fattispecie, osservabile dalla nostra giurisprudenza e qui sistematizzata, sia compatibile con i principi attestatisi in altre giurisdizioni, la tendenza verso rimedi "correttivi" (piuttosto che "soppressivi") dovrebbe facilitare un punto di incontro tra l'applicazione del diritto all'oblio nell'Unione e negli Stati Uniti. Ciò – in definitiva – credo possa rappresentare anche un significativo passo in avanti verso una governance globale del diritto all'oblio.

Note

[1]Il primo pronunciamento di una corte sul bilanciamento tra diritto alla riservatezza e diritto di cronaca si fa tradizionalmente risalire al celebre caso *Soraya Esfandiari*. Cfr. Cass. civ., sez. I, 27 maggio 1975, n. 2129, sul quale si rinvia a M. Cuniberti, *Riservatezza e identità personale*, in M. Cuniberti, E. Lamarque, B. Tonoletti, G.E. Vigevani, M.P. Viviani Schlein (a cura di), "Percorsi di diritto dell'informazione", Giappichelli, 2011, p. 116 ss.; P. Caretti, A. Cardone, *Diritto alla riservatezza e diritto all'informazione: premesse normative e sviluppi giurisprudenziali*, in "Diritti umani e diritto internazionale", 2010, n. 1, p. 91 ss. e G. Gardini, *Le regole dell'informazione. Dal cartaceo al bit*, Giappichelli, 2014, p. 314.

[2]Con particolare riferimento alla dignità, i limiti sono stati riassunti in due sentenze che costituiscono ancora oggi imprescindibile punto di riferimento: le sentenze n. 8959 del 30 giugno 1984 delle Sezioni Unite Penali, e n. 5259 del 18 ottobre 1984 della Prima Sezione Civile della Cassazione. Nel trovare il giusto bilanciamento tra questi diritti e l'attività giornalistica e di informazione, la giurisprudenza ha fissato diversi limiti al diritto alla libera manifestazione del pensiero, riassumibili come segue: - il diritto alla riservatezza richiede il rispetto del principio di essenzialità dell'informazione e l'adozione di accorgimenti atti a non svelare, neppure indirettamente, l'identità personale dei soggetti; - con particolare riferimento alla dignità, l'esercizio del diritto di cronaca è legittimo quando concorrono le seguenti tre condizioni: a) utilità sociale dell'informazione; b) verità dei fatti esposti; c) forma "civile" dell'esposizione dei fatti e della loro valutazione (c.d. continenza espressiva). Non tutti i limiti rilevano sempre in egual misura, potendo invece operare in misura variabile a seconda che si eserciti un diritto, piuttosto che un altro (ad es. diritto di cronaca, piuttosto che di critica, di parodia, di rievocazione storica). Una variabilità nella operatività di questi criteri si osserva anche a seconda della tipologia di informazioni che l'attività informativa coinvolga (ad es., informazioni giudiziarie o relative a soggetti minori) o del mezzo attraverso cui essa si esplichi. Si tratta dunque di un bilanciamento dinamico.

[3]C. de Terwangne, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*, in "Revista de Internet, Derecho y Politica", 2012, n. 13, pp. 109, 110.

[4]S. Walz, *Relationship between the freedom of the press and the right to informational privacy in the emerging Information Society*, in "19th International Data Protection Commissars Conference" (Brussels, 17-19 September 1997). Sulle caratteristiche della memoria di Internet, si veda S. Bonavita, *Le ragioni dell'oblio*, in "Ciberspazio e Diritto", 2017, n. 1, p. 104. Sul rapporto tra valore della memoria e diritto individuale sopra di essa v. A. Ghezzi, Â. Guimarães Pereira, L. Vesnić-Alujević, *The Ethics of Memory in a Digital Age. Interrogating the Right to be Forgotten*, Palgrave Macmillan, 2014. Per un inquadramento filosofico della duplice natura del passato v. U. Pagallo, M. Durante, *Legal Memories and the Right to Be Forgotten*, in L. Floridi (ed.), "Protection of Information and the Right to Privacy - A New Equilibrium?" Law, Governance and Technology Series, vol. 17, Springer, 2014, p. 17-30.

[5]L'istituto era già previsto dall'art 12(b) Dir. 95/46 e dalla Convenzione 108/1981, art. 8.c. A far gridare alla novità, è stata l'aggiunta in parentesi tonda, nella rubrica dell'articolo, del termine "Diritto all'oblio" accanto a "Diritto alla cancellazione", peraltro giudicata "impropria" in dottrina, «considerato che si tratta di istituti distinti», posti in rapporto di presupposto-conseguenza l'uno rispetto all'altro. Cfr. L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016, p. 264. L'unica novità di carattere sostanziale è l'aggiunta di un obbligo specifico imposto a coloro che hanno reso pubblici i dati personali di cui è richiesta la cancellazione di adottare misure ragionevoli, comprese misure tecniche, per informare i responsabili del trattamento che l'interessato ha chiesto la cancellazione di qualsiasi collegamento a copia o replica di tali dati personali.

[6]CGUE, 13 maggio 2014, *Google Spain SL e Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) e Mario Costeja Gonzalez*, C-131/12, EU:C:2014:317, p. 91. La sentenza è commentata da S. Peron, *Il diritto all'oblio nell'era dell'informazione on-line*, in "Responsabilità civile e previdenza", 2014, n. 4, pp. 1177-1191, e da L. Bugiolacchi, *Mancata rimozione della indicizzazione di spazi web a richiesta dell'interessato: la nuova frontiera della r.c. dei motori di ricerca*, in "Responsabilità civile e previdenza", 2014, n. 5, pp. 1530-1540. Si vedano, altresì, i contributi pubblicati in "Il diritto dell'informazione e dell'informatica", 2014, n. 4/5, interamente dedicato alla pronuncia in questione. Tutti i saggi sono ora raccolti in G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, RomaTrE-Press, 2015. Si vedano anche A. Bund, *The Curious Case of the Right to Be Forgotten*, in "Computer Law & Security Review", 2015, n. 31, p. 336-350; D. Lindsay, *The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the* Costeja *Ruling*, in "Journal of Media Law", vol. 6, 2014, n. 2, p. 159-179; L. Siry, *Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten*, in "Kentucky Law Journal", vol. 103, 2014, n. 3, p. 311-344; R.H. Weber, *On the Search for an Adequate*

Scope of the Right to Be Forgotten, in "Journal of Intellectual Property, Information Technology and Electronic Commerce Law", vol. 6, 2015, n. 1, p. 2-10; C. Castets-Renard, *Google et l'obligation de dereferencer les liens vers les donnees personnelles ou comment se faire oublier du monde numerique*, in "Revue Lamy Droit de l'immateriel", 2014, n. 106, pp. 68-75; S. Martinelli, voce *Google Spain*, in G. Ziccardi, P. Perri, "Dizionario Legal Tech", Giuffrè Francis Lefebvre, 2020, p. 476.

[7]D. Erdos, *The 'right to be forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps*, in "Journal of Media Law", vol. 13, 2021, n. 1, p. 1-35, a p. 6: «Seen from a highly formalistic vantage point, it could therefore be argued that this right is only recognised by countries subject to the GDPR and that it has whatever meaning is ascribed to it within that instrument».

[8]L. Bolognini, E. Pelino, C. Bistolfi, *op. cit.*, p. 263; F. Di Ciommo, *Il diritto all'oblio (oblito) nel regolamento Ue 2016/679 sul trattamento dei dati personali*, in "Il Foro italiano", 2017, n. 9, pp. 306-314; G. Garofalo, *Identità digitale e diritto all'oblio: questioni aperte all'indomani dell'approvazione del GDPR*, in "Il diritto di famiglia e delle persone", 2021, n. 3, pp. 1505-1518.

[9]Cass. civ. sez. III, 20 aprile 2021, n. 10347, commentata da G. Citarella, *Archivio on-line di quotidiano e diritto all'oblio*, in "Responsabilità civile e previdenza", 2021, n. 6, p. 1936. Di analogo avviso A. Alù, *Esiste il diritto all'oblio su Internet? La complessa evoluzione di tale figura tra giurisprudenza e legge*, in "Il diritto di famiglia e delle persone", 2020, n. 1, pp. 313-328, che giudica la figura del diritto all'oblio «particolarmente problematica nella sua concreta ricostruzione applicativa, anche in virtu delle rilevanti oscillazioni interpretative che si registrano sul piano giurisprudenziale».

[10]Quando ponga in essere un trattamento di dati personali di persone fisiche che si trovano nell'Unione. V. art. 3 e considerando 22-24 GDPR. In dottrina, P. de Hert, M. Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, in "International Data Privacy Law", vol. 6, 2016, n. 3, p. 230-243; M.C. Meneghetti, *The different shapes of extraterritoriality in EU data protection law and its international justifications*, in "Diritto del commercio internazionale", 2019, n. 4, pp. 695-716; D.J.B. Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation*, in "International Data Privacy Law", vol. 5, 2015, n. 4, p. 226-234.

[11]A. Solow-Niederman, F.J. Careaga Franco, N. Jansen Reventlow, V. Krishnamurthy, *Here, There, or Everywhere? Assessing the Geographic Scope of Content Takedown Orders*, Working Paper, Cyberlaw Clinic, Harvard Law School, 2017, analizzano un set di casi implicanti ordini di rimozione di contenuti online e rilevano come nella maggior parte dei casi essi abbiano ancora portata meramente locale.

[12]CGUE, 24 settembre 2019, *Google LLC v Commission nationale de l'informatique et des libertés* (CNIL), C-507/17. Sulla vertenza in oggetto si veda S. Martinelli, *Diritto all'oblio e motori di ricerca. Memoria e privacy nell'era digitale*, Giuffrè, 2017, p. 313 ss.; G. Milizia, *Google deve deindicizzare i dati sensibili degli interessati da tutte le sue "versioni europee"*, in "Diritto e giustizia", 25 settembre 2019.

[13]Conclusioni presentate il 10 gennaio 2019, pp. 59 e 62.

[14]*Ivi*, p. 60.

[15]Sul concetto di governance applicabile al diritto all'oblio si veda soprattutto la dottrina tedesca che parla di un «governance model of a kinetic sculpture in the form of a "fundamental rights mobile" (*Grundrechts-Mobile*)» per evidenziare una struttura di governance flessibile ed egualitaria, che attribuisce alle corti nazionali, transnazionali ed internazionali autonomo spazio di interpretazione delle norme a tutela dei diritti umani, in contrapposizione al tradizionale modello piramidale che simboleggia una struttura di poteri e competenze ben definita. V. J. Polakiewicz, *Europe's multi-layered human rights protection system: challenges, opportunities and risks*, Lecture at Waseda University Tokyo, 14 March 2016; O.J. Gstrein, *Right to be forgotten: european data imperialism, national privilege, or universal human right?*, in "Review of European Administrative Law", vol. 13, 2020, n. 1, p. 125-152.

[16]Sul bilanciamento tra diritti fondamentali vedi M. Durante, *Dealing with Legal Conflicts in the Information Society. An Informational Understanding of Balancing Competing Rights*, in "Philosophy & Technology", vol. 26, 2013, n. 4, p. 437-457.

[17]Critica sul punto M. Samonte, *Google v. CNIL: The territorial scope of the right to be forgotten under EU law*, in "European Papers", vol. 4, 2019, n. 3, p. 839-851, secondo cui «Member States may adopt a different approach [...] which could negatively impact the harmonisation of EU data protection law».

[18]Tra le soluzioni più diffuse è sufficiente menzionare l'utilizzo di servizi di Web Proxy e di programmi VPN che agiscono andando a camuffare l'indirizzo IP del computer che effettua l'interrogazione del server, tramutandolo in uno straniero, estraneo al blocco territoriale impartito dall'autorità. A riprova, lo stesso Gruppo di lavoro ex art. 29, chiamato ad interpretare da un punto di vista applicativo il nuovo obbligo di deindicizzazione fissato dalla sentenza *Google Spain*, si era affrettato ad evidenziare tale criticità, suggerendo sin da allora una deindicizzazione estesa a tutti i domini rilevanti, compreso quello con suffisso ".com". Cfr. Gruppo di lavoro ex art. 29 per la protezione dei dati personali, *Guidelines on the implementation of the Court of Justice of the Europe Union Judgement on "Google Spain and Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez" C-131/12*, 26 November 2016, p. 3 e 9.

[19]CGUE, 3 ottobre 2019, *Glawischnig-Piesczek c. Facebook Ireland Limited*, C-18/08, ECLI:EU:C:2019:821. Sulle due decisioni enunciate in narrativa si veda M. Astone, *Il diritto all'oblio on line alla prova dei limiti territoriali*, in "Europa e diritto privato", 2020, n. 1, pp. 223-235; G. De Gregorio, *Google v. CNIL and Glawischnig-Piesczek v. Facebook: content and data in the algorithmic society*, in "Medialaws", 2020, n. 1, pp. 249-261; F. Fabbrini, E. Celeste, *The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders*, in "German Law Journal", vol. 21, 2020, n. S1, p. 55-65.

[20]Garante per la protezione dei dati personali, *Provvedimento del 21 dicembre 2017, n. 557*, con nota di F. Frigerio, *Deindicizzazione globale degli URL su Google: sì del Garante Privacy, in attesa della Corte di Giustizia*, in "Medialaws", 2018, n. 2, pp. 381-386.

[21]Trib. Torino, sez. I civ., 7 aprile 2017, n. 1928, con nota di F. Frigerio, *Il Tribunale di Torino interviene sulla responsabilità degli Internet Service Provider*, in "Medialaws", 2017, n. 1, pp. 169-172.

[22]*Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, COM/2020/825 final.

[23]Regolamento n. 1215/2012 del Parlamento europeo e del Consiglio del 12 dicembre 2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, GU L 351, 20 dicembre 2012, pp. 1-32.

[24]In questo senso paiono propendere G. Frosio, O. Bulayenko, *Study on dynamic blocking injunctions in the European Union. IPR Enforcement case-law collection*, EUIPO, 2021, pp. 56-57. Sul concetto di cortesia internazionale, per

cui un ordine giudiziale è ammesso solo se una misura dello stesso tipo è disponibile per la stessa fattispecie in una situazione nazionale comparabile nello Stato di emissione, si veda P.K. Bookman, *Litigation Isolationism*, in "Stanford Law Review", vol. 67, 2015, p. 1081, 1096, che la definisce «a sort of intercourt diplomacy».

[25]C.T. Bavitz, *The Right to be Forgotten and Internet Governance: Challenges and Opportunities*, in "Latin American Law Review", 2019, n. 2, p. 1-21; G.F. Frosio, *Right to Be Forgotten: Much Ado About Nothing*, in "Colorado Technology Law Journal", vol. 15, 2017, n. 2, p. 329. Oltre che sulle decisioni europee, il dibattito si è concentrato in particolar modo sul contrasto tra la decisione della Corte Suprema del Canada nella controversia *Google Inc., v. Equustek Solutions, Inc.*, [2017] 1 S.C.R. 34 (Can.), che riconosceva il diritto del ricorrente di ottenere la deindicizzazione di taluni URL a livello globale e la pronuncia del Northern District of California che – viceversa – negava efficacia nel territorio statunitense alla pronuncia per probabile violazione dell'articolo 230 del Communication Decency Act del 1996. V. J. Daskal, *Speech Across Borders*, in "Virginia Law Review", vol. 105, 2019, n. 8, p. 1605-1666; R. Diab, *Search Engines and Global Takedown Orders: Google v Equustek and the Future of Free Speech Online*, in "Osgoode Hall Law Journal", vol. 56, 2020, n. 2, p. 231-270.

[26]GNI Statement on Domestic Cases Asserting Global Internet Jurisdiction.

[27]K. Garstka, D. Erdos, *Hiding in Plain Sight: The "Right to be Forgotten" and Search Engines in the Context of International Data Protection Frameworks*, in L. Belli, N. Zingales (eds.), "Platform Regulations: How Platforms are Regulated and How They are Regulating Us", FGV Direito Rio, 2017. Tra gli enti indagati si annoverano l'Unione africana (AU), la Cooperazione economica asiatico-pacifica (APEC), l'Associazione delle nazioni del sudest asiatico (ASEAN), il Consiglio d'Europa, la Comunità economica degli Stati dell'Africa occidentale (ECOWAS) l'Organizzazione per la cooperazione economica e lo sviluppo (OCSE).

[28]F. Werro, *The Right To Be Forgotten. A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia*, Springer, 2020.

[29]D. Erdos, K. Garstka, *The 'right to be forgotten' online within G20 statutory data protection frameworks*, in "International Data Privacy Law", vol. 10, 2020, n. 4, p. 294-313. Restano privi di una normativa in materia Cina, India, Arabia Saudita e Stati Uniti. Il Brasile ammette l'esercizio del diritto all'oblio solo in presenza di dati non accurati. La Turchia prevede che il diritto non operi laddove i dati siano stati resi pubblici direttamente dall'interessato (cfr. Data Protection Act 2016, art. 28(2)(b)).

[30]Gruppo di lavoro ex art. 29 per la protezione dei dati personali, *Guidelines*, cit.

[31]European Data Protection Board, *Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del RGPD*, parte I, versione 2.0, 7 luglio 2020.

[32]Si rinvia ai riferimenti contenuti in D. Erdos, *op. cit.*, p. 14 ss.

[33]W.G. Voss, C. Castets-Renard, *Proposal for an International Taxonomy on the Various Forms of the "Right to be Forgotten": A Study on the Convergence of Norms*, in "Colorado Technology Law Journal", vol. 14, 2016, n. 2, p. 281, 342.

[34]D. Erdos, *op. cit.*, p. 12.

[35]A. Bradford, *The Brussels effect*, in "Northwestern University Law Review", vol. 107, 2012, n. 1, p. 1-67; Id., *The Brussels effect: How the European Union rules the world*, Oxford University Press, 2020.

[36]Ai sensi e per gli effetti dell'art. 25 Dir. 95/46/CE, «gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato».

[37]D. Erdos, *op. cit.*, p. 5.

[38]Consiglio d'Europa, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, 2017; Id., *Practical Guide on the Use of Personal Data in the Police Sector*, 2018; Id., *Guidelines on Artificial Intelligence and Data Protection*, 2019; Id., *Privacy and Data Protection Principles Guide for ICANN Related Data Processing*, 2018; Id., *Guidelines on Safeguarding Privacy in the Media*, 2018.

[39]La lista completa è disponibile sul sito di GPA.

[40]ICDPPC, *Resolution on Privacy Protection in Social Network Services*, 2008; Id., *Resolution on Social Media and Violent Extremist Content Online*, 2019.

[41]Si veda in particolare il commento alla sentenza *Google Spain* da parte della House of Lords inglese, secondo cui «[t]he expression 'right to be forgotten' is misleading. Information cannot be deliberately 'forgotten'. It cannot be 'consigned to oblivion' (the expression used by the Spanish court in its request for a preliminary ruling)». V. House of Lords - European Union Committee, *EU data protection law: a 'right to be forgotten'?*, 2014-15, n. 40, p. 9. V. anche P.A. Bernal, *A Right to Delete?*, in "European Journal of Law & Technology", vol. 2, 2011, n. 2, che osserva come sia più corretto parlare di diritto alla cancellazione. Cfr. anche i riferimenti *sub* nota 6.

[42]M.L. Rustad, S. Kulevska, *Reconceptualizing the right to be forgotten to enable transatlantic data flow*, in "Harvard Journal of Law & Technology", vol. 28, 2015, n. 2.

[43]Sulla compatibilità dell'approccio europeo e di quello statunitense v. U. Pagallo, M. Durante, *Human rights and the right to be forgotten*, in M. Susi (ed.), "Human Rights, digital society and the law", Routledge, 2019, p. 197, 201 e D.C. Nunziato, *Forget about it? Harmonizing European and American Protections for Privacy, Free Speech, and Due Process*, GWU Law School Public Law Research Paper No. 2017-52, p. 2.

[44]A. Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to be Forgotten'*, in "Computer Law & Security Review", vol. 29, 2013, n. 3, p. 229-235; J. Rosen, *The Right to Be Forgotten*, in "Stanford Law Review online", vol. 64, 2012, February, p. 88-92.

[45]C. de Terwangne, *Internet Privacy and the Right to Be Forgotten*, cit.

[46]Il solo decorso di un lasso temporale standard non pare tuttavia in grado di giustificare tale primato, anche considerato che le esigenze informative non vengono automaticamente meno con il decorso di un arco temporale pur ampio, necessitando, per converso, di una valutazione caso per caso.

[47]C. de Terwangne, *The Right to be Forgotten and the Informational Autonomy in the Digital Environment*, European Commission Joint Research Centre, 2013, p. 27.

[48]Anche nel nostro ordinamento è presente un diritto alla riabilitazione (artt. 178 e 179 c.p.) che include la cancellazione dal casellario giudiziale, ma si tratta di una misura confinata a tale specifica forma di pubblicità notizia e dunque soggetta alla presenza di requisiti peculiari, particolarmente restrittivi. La riabilitazione non è invece applicabile alla pubblicazione della sentenza di condanna per cui occorre presentare una specifica richiesta di "aggiornamento dei dati" dell'archivio CED indirizzata al Ministero dell'interno - Dipartimento della pubblica sicurezza - Direzione centrale della polizia criminale. Sugli effetti della riabilitazione nel nostro ordinamento si v. M. Garavelli, voce *Riabilitazione*, in "Digesto. Discipline penalistiche", UTET, 1997. La distinzione ci pare dunque mal posta. La cancellazione dei dati giudiziari su altre fonti

di comunicazione segue invece regole analoghe a quelle previste per gli altri dati personali, con la conseguenza che non parrebbe necessario, in linea di principio, introdurre una distinzione tra diritto all'oblio del passato giudiziario e diritto all'oblio in generale. D'altro canto, introdurre differenziazioni sulla sola base della tipologia o natura dell'informazione diffusa aprirebbe a classificazioni di complessità ben superiori a quanto risulta utile per le finalità di avviare un processo di cooperazione internazionale su basi comuni.

[49]W. Hartzog, F. Stutzman, *The Case for Online Obscurity*, in "California Law Review", vol. 101, 2013, n. 1, p. 4, osservano come tale forma di oblio sia più confacente alle caratteristiche dell'ordinamento statunitense: «instead of forcing websites to remove sensitive information, courts could mandate some form of obscurity».

[50]CGUE, 13 maggio 2014, cit., p. 70.

[51]Cass., sez. un., 22 luglio 2019, n. 19681.

[52]Cass. civ., sez. III, 5 novembre 2018, n. 28084, critica rispetto all'individuazione dei criteri di bilanciamento tra diritto di cronaca e diritto all'oblio operata da Cass., 20 marzo 2018, n. 6919, con nota di R. Pardolesi, S. Bonavita, *Diritto all'oblio e buio a mezzogiorno*, in "Il Foro italiano", 2018, n. 4, pt. 1, pp. 1151-1160 e D. Feola, *Massimario della responsabilità civile*, in "Responsabilità civile e previdenza", 2018, n. 2, p. 631 e così riassumibili: 1) contributo della notizia ad un dibattito di interesse pubblico; 2) l'interesse effettivo ed attuale alla diffusione; 3) grado di notorietà del soggetto rappresentato; 4) modalità impiegate per ottenere e nel dare l'informazione; 5) la preventiva informazione circa la pubblicazione o trasmissione della notizia, in modo da consentire all'interessato il diritto di replica prima della sua divulgazione. La corte rimettente rilevava come dalla lettura della menzionata pronuncia e dalla giurisprudenza delle Corti europee "non è dato evincere se i presupposti indicati siano richiesti in via concorrente ovvero, come sembra a questo Collegio, in via alternativa".

[53]Si vedano i commenti di R. Pardolesi, *Oblio e anonimato storiografico "usque tandem"?*, in "Il Foro italiano", 2019, n. 10, pp. 3082-3089; G. Citarella, *Diritto all'oblio: un passo avanti e tre indietro*, in "Responsabilità civile e previdenza", 2019, n. 5, pp. 1556-1562; D. Muscillo, *Oblio e divieto di lettera scarlatta*, in "Danno e responsabilità", 2019, n. 5, pp. 611-614; A. Bonetta, *Diritto al segreto del disonore. Navigare a vista affidato ai giudici di merito*, *ivi*, pp. 614-620 e G. Calabrese, *Rievocazione storica e diritto all'oblio*, *ivi*, pp. 620-624; F. Zanovello, *Diritto all'oblio e rievocazione storica: un difficile bilanciamento*, in "Studium iuris", 2019, n. 12, pp. 1478-1482; G. Finocchiaro, *Le Sezioni Unite sul diritto all'oblio*, in "Giustiziacivile.com", 29 luglio 2019. *Contra*, A. Cuffaro, *Una decisone assennata sul diritto all'oblio*, in "Il corriere giuridico", 2019, pp. 1195-1197, che approva l'approccio cauto delle Sezioni Unite e A. Spatuzzi, *Diritto all'oblio e rievocazione storica. Il bilanciamento delle Sezioni Unite*, in "Il diritto di famiglia e delle persone", 2020, n. 4, pp. 1260-1269, che giudica positivamente la scelta di non «rincorrere soluzioni eccessivamente ariose nel tentativo di ricondurre il diritto all'oblio entro una disciplina generale».

[54]V. *supra* nota 2.

[55]L'articolo oggetto di doglianza si inseriva in una rubrica settimanale che aveva rievocato il racconto di diciannove omicidi sui quali l'opinione pubblica si era a lungo confrontata. Secondo i giudici del merito, dunque, la pubblicazione non era avvenuta «per il solo fine di "riempire" strumentalmente una pagina della edizione della domenica», bensì allo scopo di «offrire, all'interno di una rubrica ben definita e strutturata nel tempo, una sponda di riflessione per i lettori su temi delicati quali l'emarginazione, la gelosia, la depressione, la prostituzione, con tutti i risvolti e le implicazioni che queste realtà possono determinare nella vita quotidiana». Alla luce di ciò, i giudici avevano ritenuto che l'articolo si inserisse in un progetto editoriale che «indiscutibilmente rientra nel costituzionale diritto di cronaca, di libertà di stampa e di espressione».

[56]Secondo i giudici del merito, l'omicidio era stato descritto «senza accostamenti suggestionanti e/o fuorvianti sottintesi», non vi era stata «nessuna gratuita e strumentale rievocazione del delitto, nessuna ricerca di volontaria spettacolarizzazione», cosi come «nessuna offesa triviale o irridente del sentimento umano».

[57]V. Trib. Milano, 28 settembre 2016, n. 10374 secondo cui la diffamatorietà e la dedotta lesione del diritto all'onore ed alla reputazione «costituiscono elementi del tutto estranei all'accertamento in esame, avente ad oggetto esclusivamente l'asserita lesione del diritto all'identità personale (*sub specie* del c.d. diritto all'oblio)». In dottrina, v. A. Baldassarre, *Il diritto di privacy e la comunicazione elettronica*, in "Percorsi costituzionali", 2010, n. 1, p. 49, ricorda: «Non si tratta [...] di un diritto che ha a che fare con l'onore e che, percio, esige una difesa di fronte ad affermazioni ingiuriose o diffamatorie, ma la lesione di cui si chiede la tutela giuridica deriva in tal caso dalla pura esposizione in pubblico di dati e/o di fatti attinenti alla "sfera privata", trattandosi di notizie o di informazioni la cui conoscenza pubblica deve dipendere soltanto dalla volontà dell'interessato». In senso analogo, O. Pollicino, M. Bassini, *Diritto all'oblio: i piu recenti spunti ricostruttivi nella dimensione comparata ed europea*, in F. Pizzetti (a cura di), "Il caso del diritto all'oblio", Giappichelli, 2013, p. 186.

[58]V. S. Martinelli, *Il diritto all'oblio nel bilanciamento tra riservatezza e libertà di espressione: quali limiti per i personaggi dello spettacolo?* (nota a Cassazione civile, I Sezione, 20 marzo 2018, n. 6919), in "Giurisprudenza italiana", 2019, n. 5, pp. 1049-1054, che rileva difficoltà interpretative ed una tendenza alla confusione e sovrapposizione tra i due diritti derivante dalla loro stretta correlazione.

[59]Intesa come la rappresentazione di un soggetto che emerge da un insieme di dati e di informazioni che recano le caratteristiche dell'interessato e permettono di identificarlo. In dottrina cfr. M. Tampieri, *L'identità personale. Il nostro documento esistenziale*, in "Europa e diritto privato", 2019, n. 4, pp. 1195-1226; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in "Contratto e impresa", 2017, n. 3, pp. 723-727; M.F. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, in "Il diritto di famiglia e delle persone", 2016, n. 3, pp. 949-968; S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, in "Rivista di diritto industriale", 2017, n. 4-5, pp. 180-201; F. Cristiani, *Il diritto alla protezione dei dati personali oltre la vita nell'era digitale*, in "Responsabilità civile e previdenza", 2015, n. 6, pp. 2031-2045; F. Delfini, *Gli approcci di Unione europea, Stati Uniti d'America e Cina nella gestione dell'identità digitale*, in "Rivista di diritto privato", 2015, n. 3, pp. 335-339; M. Durante, *Rethinking human identity in the age of autonomic computing. The philosophical idea of trace*, in M. Hildebrandt, A. Rouvroy (eds.), "Law, human agency and autonomic computing. The philosophy of law meets the philosophy of technology", Routledge, p. 85-103.

[60]Ciò si ricava, in particolare, dalla definizione di diritto all'oblio formulata da Cass. civ. sez. I, 19 maggio 2020, n. 9147, in "Responsabilità civile e previdenza", 2021, n. 1, p. 174, con nota di M. Cocuccio, *Deindicizzare per non censurare: il «ragionevole compromesso» tra diritto all'oblio e diritto di cronaca*: «Il diritto all'oblio consiste nel non rimanere esposti senza limiti di tempo ad una rappresentazione non più attuale della propria persona con pregiudizio alla reputazione ed alla riservatezza, a causa della ripubblicazione, a distanza di un importante intervallo temporale, di una notizia relativa a fatti del passato». *Contra* però la giurisprudenza di merito e la dottrina menzionata *supra* in nota 57.

[61]Sul punto sia consentito rinviare a J. Ciani, *Cronaca rosa e diritto alla riservatezza della vita privata: non basta il carattere anonimo della notizia, se la persona offesa resta identificabile* (nota a Cass. civ., 27 gennaio 2014, n. 1608), in "Il diritto dell'informazione e dell'informatica", 2014, n. 3, pp. 349-362.

[62]Tanto risulta confermato da Cass., 20 aprile 2021, n. 10347, cit., secondo cui «l'elemento, per cosi dire, "unificante" tutte le ipotesi in cui viene in rilievo il conflitto tra il diritto della persona all'oblio di notizie che la riguardino ed il contrapposto interesse alla conservazione delle stesse in archivi informatici, è costituito dalla liceità dell'iniziale pubblicazione. All'opposto, nel presente caso, tale presupposto difetta, essendo stata la notizia ritenuta diffamatoria».

[63]V. Trib. Roma, 24 novembre 2015, n. 23771 che ha sottolineato che il breve lasso di tempo intercorso non era sufficiente ad integrare il diritto all'oblio. I fatti di cui alla vicenda giudiziaria non erano nemmeno ancora definiti e risalivano ad appena due anni prima della richiesta del ricorrente, con la conseguenza che le notizie che riferivano dei detti fatti erano tutt'altro che inattuali. Per un commento alla sentenza si veda G.M. Riccio, *L'esordio del diritto all'oblio nella giurisprudenza italiana*, in "Il diritto dell'informazione e dell'informatica", 2016, n. 2, p. 271. Il Garante privacy ha costantemente rigettato le istanze nelle ipotesi di provvedimenti giudiziari recenti, oppure nei casi in cui non siano stati espletati tutti i gradi di giudizio. V. i casi elencati in Garante per la protezione dei dati personali, *Newsletter del 22 dicembre 2014, n. 397 - Diritto all'oblio: prime pronunce del Garante dopo i no di Google*. La stessa Corte Costituzionale, sebbene pronunciandosi con riguardo al diverso istituto della prescrizione di diritto penale, ha riconosciuto quale elemento costitutivo del diritto all'oblio «il lungo tempo decorso», che abbia comportato «un affievolimento progressivo dell'interesse della comunità». Cfr. C. Cost. 23 dicembre 2020, n. 278; Id. sentenze n. 115 del 2018, n. 24 del 2017, n. 45 del 2015, n. 143 del 2014 e n. 23 del 2013.

[64] Cass sez. III 5 aprile 2012, n. 5525. Per un commento alla sentenza si veda V. D'Antonio, S. Sica, *La procedura di de-indicizzazione*, in G. Resta, V. Zeno-Zencovich (a cura di), *op. cit.*, pp. 147-176.

[65]«I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali».

[66]Gruppo di lavoro ex art. 29 per la protezione dei dati personali, *Opinion 03/2013 on purpose limitation*, 2 aprile 2013, 00569/13/EN WP 203, p. 23 ss.

[67]La tripartizione è stata successivamente riproposta anche da Cass., 20 aprile 2021, n. 10347, cit.

[68]In tal senso Cass. sez. III 9 aprile 1998, n. 3679, con note di P. Laghezza, *Il diritto all'oblio esiste (e si vede)*, in "Il Foro italiano", 1998, n. 6, pt. 1, pp. 1835-1838 e di C. Lo Surdo, *Diritto all'oblio come strumento di protezione di un interesse sottostante*, in "Danno e responsabilità", 1998, n. 10, pp. 882-894.

[69]Contra G. Finocchiaro, *op. cit.*, secondo cui «le tre accezioni del diritto all'oblio affondano le loro radici in diritti della personalità distinti. Sotto il primo profilo, il diritto all'oblio appartiene, come magistralmente è stato scritto da Ferri, "alle ragioni e 'alle regioni' del diritto alla riservatezza". Se si considera il secondo profilo, il diritto all'oblio appartiene alla sfera del diritto all'identità personale. Se, infine, si prende in esame il terzo profilo, il diritto all'oblio va iscritto nel diritto alla protezione dei dati personali». La distinzione non mi trova tuttavia concorde, posto che mi pare che i diritti menzionati non si trovino su piani differenti bensì in rapporto di complementarietà e la relativa interazione può essere rappresentata attraverso l'immagine dei cerchi concentrici. Sia consentito rinviare sul punto a J. Ciani, *Il pubblico dominio nella società della conoscenza. L'interesse generale al libero utilizzo del capitale intellettuale comune*, Giappichelli, 2021, pp. 453-454.

[70]In questo senso v. Cass. civ. sez. III, 26 giugno 2013, n. 16111, che ha sottolineato la circostanza secondo cui una notizia che rivestiva un interesse pubblico in un certo contesto non necessariamente continua a poter essere divulgata con tutti i suoi riferimenti personali quando il lungo tempo trascorso ha reso ormai inesistente quell'interesse.

[71]La suddetta necessità risulta anche dalle regole di cui al Testo unico dei doveri del giornalista, che all'art. 3, co. 1, afferma che il giornalista «rispetta il diritto all'identità personale ed evita di far riferimento a particolari relativi al passato, salvo quando essi risultino essenziali per la completezza dell'informazione». Mentre l'art. 3, co. 2, aggiunge che il giornalista, «nel diffondere a distanza di tempo dati identificativi del condannato, valuta anche l'incidenza della pubblicazione sul percorso di reinserimento sociale dell'interessato e sulla famiglia».

[72]Conferma viene da CEDU, sez. V, 19 ottobre 2017 n. 71233-13, là dove ha posto in evidenza che la notorietà pubblica del soggetto dava ragione dell'interesse della collettività alla conoscenza della sua vicenda personale, da ritenere prevalente rispetto al contrapposto interesse di chi voleva mantenere il riserbo sulla medesima.

[73]Cass. sez. III, 5 aprile 2012, n. 5525, cit.

[74]Punto 97 della pronuncia.

[75]In relazione a quest'ultimo punto, le *Linee Guida* del Gruppo ex art. 29, cit. affermano che: «It is not possible to establish with certainty the type of role in public life an individual must have to justify public access to information about them via search result. However, by way of illustration, politicians, senior public officials, business people and members of the (regulated) professions can usually be considered to fulfill a role in public life. There is an argument in favour of the public being able to search for information relevant to their public roles and activities. A good ride of thumb is to try to decide where the public having access to the particular information – made available through a search on the data subject's name – would protect them against improper public or professional conduct. It is equally difficult to define the subgroup of "public figures". In general, it can be said that public figures are individuals who, due to their functions/commitments, have a degree of media exposure».

[76]Rendendoli accessibili a qualsiasi utente di Internet che, effettuando una ricerca, a partire dal nome della persona interessata, non avrebbe altrimenti reperito la pagina web su cui i predetti dati siano pubblicati.

[77]Come chiaramente affermato dalla Corte di Giustizia nel caso *Google Spain*, cit., al punto 37, infatti, «l'organizzazione e l'aggregazione delle informazioni pubblicate su Internet, realizzate dai motori di ricerca allo scopo di facilitare ai loro utenti l'accesso a dette informazioni, possono avere come effetto che tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l'elenco di risultati una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che consente loro di stabilire un profilo piu o meno dettagliato di quest'ultima». Ancora, la Corte chiarisce che: «l'effetto dell'ingerenza nei suddetti diritti della persona interessata risulta moltiplicato in ragione del ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono alle informazioni contenute in un sfatto elenco di risultati carat-

tere ubiquitario (v., in tal senso, sentenza eDate Advertising e a., C-509/09 e C-161/10, EU; C:2011:685, punto 45)».

[78]Cfr. Cass., Sez. Un. penali, 22 settembre 2011, n. 34476.

[79]V. Cass. civ. sez. I, 27 marzo 2020, n. 7559, con nota di V. Amendolagine, *Il diritto all'oblio tra rievocazione storiografica on line e cronaca giudiziaria*, in "Giustiziacivile.com", 18 agosto 2020, contenente ampi riferimenti giurisprudenziali e dottrinali.

[80]Garante per la protezione dei dati personali, Provvedimento del 18 dicembre 2014 [doc. web n 3736353] che ha respinto il ricorso di una persona implicata in una inchiesta giudiziaria che contestava la decisione del motore di ricerca di non deindicizzare un articolo che ne riferiva.

[81]CEDU, sentenza del 25 novembre 2021 (*Bianciardi c. Italia*).

[82]G. Settimio, *Deindicizzazione e diritto all'oblio al vaglio della Suprema Corte*, in "Giustiziacivile.com", 27 settembre 2021. In giurisprudenza, proprio in questi termini, si veda Cass. civile sez. I, 19 maggio 2020, n. 9147, cit., che ha cassato la decisione dei giudici del merito di ordinare la cancellazione della notizia relativa ad una vicenda giudiziaria mantenuta online, sul presupposto che questi non avessero verificato i profili di applicabilità della misura della deindicizzazione dai motori di ricerca quale rimedio sufficiente, in vista del bilanciamento con l'interesse pubblico alla conoscenza del fatto.

[83]V. Cass. civ. sez. I, 27 marzo 2020, n. 7559, cit., secondo cui, in ipotesi di presenza nell'archivio storico online di un quotidiano di articoli di cronaca giudiziaria pubblicati anni prima nell'edizione cartacea dello stesso giornale riguardanti fatti rilevanti per la collettività, la deindicizzazione e l'aggiornamento degli articoli in questione sono la «soluzione idonea a bilanciare i contrapposti interessi in gioco, che pur consentendo la conservazione del dato personale pubblicato, lo rende però accessibile non più tramite gli usuali motori di ricerca presenti nella Rete, bensì, esclusivamente dall'archivio storico dello stesso quotidiano».

* * *

Right to be forgotten and international cooperation: problems and perspectives

Abstract: Given the ubiquitous presence of personal data online, an effective protection of the right to be forgotten depends on the cross-border recognition of blocking or delisting injunctions. Thanks to the wide scope of application of the GDPR, addressing any personal data controller, even if established outside the European Union, worldwide blocking orders have been already issued. However, without an international regulatory framework providing for common grounds under which claiming a right to be forgotten, different national legal traditions work as an obstacle to its global enforcement. Indeed, international cooperation for the protection of such right is conditioned on a substantial harmonization of its grounds for application. Recent decisions of the Italian Supreme Court open interesting perspectives in this regard, providing valuable hints on how balancing the protection of personal data and the right to information as well as drawing the dividing line between the right to be forgotten and the tort of defamation.

Keywords: GDPR – Personal data – Right to be forgotten – Erasure – Delisting – Cross-border enforcement

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0067
Articolo sottoposto a peer review

Le piattaforme digitali come "poteri privati" e la censura online

Ottavio Grandinetti

Sempre più spesso gli studiosi europei ed americani qualificano le piattaforme digitali gestite dalle Big Tech come "poteri privati" e, per quel che riguarda la libertà di espressione e di informazione, come "censori privati". Il saggio, dopo aver richiamato le più recenti teorie antitrust sulle piattaforme online negli USA e in Europa, si focalizza sulle conseguenze costituzionali di questa qualificazione (potere privato) sulla disciplina della censura online, arrivando alla conclusione che, secondo il diritto costituzionale italiano ed europeo (perlomeno dell'Europa continentale), mentre gli utenti delle piattaforme sono garantiti dalla libertà di espressione e di informazione, le piattaforme online esercitano solo la loro libertà di impresa. Di conseguenza, le piattaforme digitali possono essere sottoposte a limiti a tutela della libertà di espressione e di informazione anche più penetranti dei media tradizionali, che esercitano pur sempre la loro libertà di informazione. E, sulla base dell'art. 10 CEDU e della relativa giurisprudenza della Corte europea dei diritti dell'uomo, gli Stati hanno l'obbligo "positivo" di garantire la libertà di espressione ed il pluralismo dell'informazione. Infine, alla luce di queste considerazioni generali, il saggio analizza criticamente le proposte di Regolamento UE sui servizi (*Digital Services Act*) e sui mercati digitali (*Digital Markets Act*).

Piattaforme digitali – Poteri privati – Censura online – Internet – Standard della Community

Sommario: *1. Premessa – 2. I più recenti approcci antitrust alle piattaforme online – 2.1. Dalla scuola di Chicago alla Hipster Antitrust – 2.2. Recenti analisi negli USA – 2.3. Analisi nell'UE ed in alcuni Paesi – 3. Inquadramento costituzionale e ricadute normative – 3.1. Le piattaforme come "poteri privati" – 3.2. Le libertà di espressione (e di informazione) e la censura online – 4. Le proposte di* Digital Markets Act *(DMA) e* Digital Services Act *(DSA) – 5. Considerazioni finali*

1. Premessa

In un numero monografico dedicato alla governance di Internet, il tema delle piattaforme digitali e della loro qualificazione giuridica è senz'altro centrale. Infatti, negli ultimi anni «dal tema della governance in senso stretto, legato alla possibilità per attori statali di predicare l'applicazione e la giustiziabilità delle proprie regole, il fulcro si è spostato alla tutela dei diritti di fronte all'affermazione di un nuovo spazio pubblico digitale, in cui un ruolo di cruciale rilievo è affidato ai fornitori di servizi che agiscono come intermediari di natura privata»[1].

Sebbene il presente lavoro si focalizzi soprattutto sul problematico ruolo assunto dagli intermediari di Internet riguardo alla tutela delle libertà di espressione e di informazione, prima di affrontare questi profili si procederà ad un ricostruzione delle più recenti analisi antitrust delle piattaforme digitali (§ 2). Ciò per varie ragioni: anzitutto, perché l'analisi eco-

O. Grandinetti è professore a contratto di Diritto dell'informazione presso l'Università degli Studi di Napoli Suor Orsola Benincasa e avvocato.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

nomica dei mercati è tutt'altro che slegata dalle valutazioni funzionali alla tutela del pluralismo informativo, al punto che un'efficace disciplina antitrust è da sempre considerata una condizione necessaria, benché non sufficiente, per una sua effettiva tutela[2]; in secondo luogo, perché per molti studiosi la disciplina antitrust rappresenta uno strumento che concorre a contrastare i poteri privati[3]; in terzo luogo, perché le più recenti analisi antitrust (benché tradizionalmente avverse all'adozione di misure *ex ante*) tendono sempre più a convergere sulla necessità di adottare un'analoga tipologia di rimedi per fronteggiare le nuove sfide derivanti dal potere assunto dalle *big tech*, cioè misure tipiche della normativa a tutela del pluralismo, così ancor più confermandone la necessità in questo campo.

Dopo tale inquadramento, si affronterà il tema della qualificazione delle piattaforme online a livello costituzionale e delle conseguenti ricadute sulla censura privata (§ 3) e poi si esamineranno i più recenti progetti di disciplina in materia a livello UE (§ 4), per trarne alcune considerazioni finali (§ 5).

2. I più recenti approcci antitrust alle piattaforme online

2.1. Dalla scuola di Chicago alla Hipster Antitrust

Nell'ambito di una crescente[4], ma non incontrastata[5], insoddisfazione degli studiosi per le impostazioni ispirate alla c.d. scuola di Chicago, gli Stati Uniti, l'UE ed anche singoli Paesi si sono via via interrogati sull'efficacia dell'attuale impostazione antitrust nel contrastare lo straripante potere di mercato delle piattaforme digitali.

Muovendo dagli Stati Uniti, in cui le *big tech* hanno i loro quartieri generali, tra gli studiosi è sembrato emergere con evidenza – non solo per quanto riguarda le piattaforme digitali, ma più in generale rispetto alla concentrazione dei mercati in numerosi settori economici[6] – l'insufficienza di un approccio basato sui capisaldi della "moderna" teoria antitrust (ossia quella sviluppatasi tra gli anni '70/'80 del Novecento ed assolutamente predominante sino ai primissimi anni del nuovo millennio): cioè, il binomio del "benessere del consumatore"[7] e dell'"efficienza economica"[8].

All'approccio c.d. strutturalista predominante sino agli anni '60 (in cui l'assetto monopolistico o anche solo oligopolistico dei mercati veniva visto in sé come un rischio per lo sviluppo di una sana concorrenza[9]) si sostituisce infatti, prima nell'applicazione giurisprudenziale della Corte Suprema[10] e poi nella prassi del Dipartimento di Giustizia (*DoJ*), l'approccio ispirato alla scuola di Chicago, secondo la quale – sintetizzando un discorso ben più complesso – è la dinamica dei prezzi nel breve termine a rappresentare il vero criterio per discriminare tra operazioni/condotte anticompetitive e non: ove i prezzi al consumo si riducano e non vi siano restrizioni nella produzione, il benessere del consumatore sarebbe soddisfatto, grazie ad una migliore efficienza allocativa.

Tuttavia, negli ultimi anni a questo approccio si contrappongono sempre più spesso altre scuole di pensiero – variamente denominate, talvolta con sottintesa ironia[11], *hipster*, *Woodstock* o *newbrandeisian*[12] antitrust – che però, almeno nelle loro più elaborate prospettazioni, non propongono un mero ritorno allo "strutturalismo" del passato, bensì un deciso ridimensionamento dell'applicazione del criterio basato sulla dinamica dei prezzi nel breve termine e, per contro, la valorizzazione di criteri correlati ad elementi strutturali dei mercati ed alle loro dinamiche competitive, come: l'esistenza di barriere all'entrata; i conflitti di interesse che possono sorgere ove uno stesso soggetto dominante in un dato mercato estenda la sua presenza in mercati collegati; il sorgere di "colli di bottiglia" o di *gatekeeper*[13]; la dinamica del potere di contrattazione; il controllo e l'utilizzo dei dati[14].

Sebbene, come detto, le critiche non riguardino solo i nuovi mercati digitali, non v'è dubbio che l'approccio della scuola di Chicago si è rivelato maggiormente inadatto proprio con riferimento alle dinamiche concorrenziali dei mercati digitali, in relazione ai quali il criterio della dinamica dei prezzi entra in crisi innanzitutto a causa dell'assenza di un corrispettivo monetario dei servizi offerti dalle *big tech*, data la loro remunerazione attraverso l'uso dei dati degli utenti. In particolare, secondo i critici della scuola di Chicago, sarebbe stata proprio l'inadeguatezza dei criteri unicamente valorizzati da questa dottrina ad aver impedito un efficace contrasto alla crescita abnorme delle maggiori *tech company*, note con l'acronimo GAFAM (Google, Apple, Facebook, Amazon e Microsoft)[15].

I sostenitori delle nuove teorie contestano anzitutto che il "benessere del consumatore" sia l'unico interesse perseguito dalla normativa antitrust e, richiamandosi allo spirito dei padri dello Sherman Act e del Clayton Act, rivendicano che la legislazione contro i monopoli sia volta a perseguire anche altre finalità, come: la tutela contro la concentrazione e l'abuso del potere economico; la difesa contro la possibilità per le grandi imprese di realizzare profitti monopolistici, dannosi per la generalità; la tutela delle libertà eco-

nomiche e la libertà dell'iniziativa economica privata, da realizzarsi soprattutto lasciando aperti i mercati; *la garanzia delle libertà dei singoli*[16].

2.2. Recenti analisi negli USA

Ai fini del presente lavoro, è peraltro sufficiente prendere atto che le istituzioni USA, a fronte del crescente allarme per il potere accumulato dalle piattaforme digitali, sembrano da ultimo aver sposato le teorie più recenti.

Nell'ottobre del 2020 il rapporto di maggioranza redatto all'esito di un'inchiesta della Camera dei rappresentanti ha affermato, dopo un'approfondita e molto documentata indagine sulla concorrenza nei mercati digitali, che il potere di mercato delle maggiori piattaforme rischia di compromettere *non solo le libertà economiche ma anche quelle politiche*[17].

Ancor più chiaramente, nell'*Executive Order* sulla promozione della concorrenza nell'economia americana, adottato il 9 luglio 2021 dal presidente Biden, si afferma che la normativa antitrust (dallo Sherman Act in poi) ha avuto come *ratio* non soltanto la tutela degli interessi economici, ma "al contempo la realizzazione di un ambiente favorevole al *mantenimento delle ... istituzioni democratiche, sociali e politiche*"[18]. Come ivi affermato, la concentrazione in atto nell'economia americana verificatasi negli ultimi decenni ha provocato un indebolimento della concorrenza negando agli americani i benefici di un'economia aperta[19] ed allargando le diseguaglianze. Per quel che più specificamente riguarda il nostro tema, il maggior pericolo viene individuato nel consolidarsi, in capo ad un piccolo numero di *big tech*, del potere di inibire l'ingresso nei relativi mercati a nuovi entranti, di conseguire profitti monopolistici, di raccogliere i più intimi dati personali per sfruttarli a proprio vantaggio, di svolgere il ruolo di *gatekeeper* per molte piccole e medie aziende la cui sopravvivenza dipende dall'accesso a queste piattaforme, nonché di provocare, a causa della dominanza nel mercato della pubblicità (indispensabile fonte di finanziamento per i media tradizionali), la chiusura o il ridimensionamento di molti giornali. Cosicché il contrasto al potere delle piattaforme digitali rappresenta una priorità dell'Amministrazione Biden, con particolare riferimento alle *killer acquisition* (ancorché verificatesi anni addietro[20]), alla raccolta di dati, alla connessa sorveglianza degli utenti, alla concorrenza sleale sul mercato dell'attenzione ed alle esternalità di rete (c.d. *network effect*).

Nel contesto americano, per ciascuna delle piattaforme dominanti sono state individuate le principali distorsioni nei mercati digitali.

In estrema sintesi[21], per quanto riguarda Facebook (FB), essa detiene una quota di mercato sostanzialmente monopolistica nei servizi di social networking e tale posizione appare difficilmente contendibile a causa delle barriere all'ingresso rappresentate dai *network effect*[22] e dai costi di transizione (c.d. *switching cost*) che gli utenti devono affrontare, non tanto in termini di spesa economica, quanto di tempo[23] per ricreare il proprio gruppo di contatti e la propria immagine sul nuovo social, derivanti anche dalla mancanza di interoperabilità di FB con gli altri social. Un altro punto di forza di FB, che finisce col creare un'ulteriore barriera all'entrata, è la grande mole di dati a disposizione, utilizzata non solo per offrire ai propri utenti servizi sempre più personalizzati (con il risultato di attrarre così sempre più utenti), ma anche per inviare loro pubblicità targettizzata, così rafforzando la dominanza di FB anche sull'altro versante del mercato della piattaforma, vale a dire quello degli inserzionisti pubblicitari. FB gioca inoltre un indubbio ruolo di *gatekeeper* nel consentire o meno ad altre imprese l'accesso a detti dati. Anche grazie ai dati derivanti da questo accesso da parte di imprese terze per offrire i loro servizi, FB ha poi potuto mettere a punto una strategia volta ad identificare potenziali concorrenti e a duplicare i loro servizi, emarginarli (anche privilegiando sulla piattaforma i propri prodotti) ovvero acquistarli, come nel caso di Instagram e WhatsApp. Queste due ultime acquisizioni hanno infatti ulteriormente ampliato la dominanza di FB, tra l'altro, estendendola al mercato degli utilizzatori di smartphone, così come l'acquisizione di Oculus (la società di realtà aumentata a base degli ultimissimi sviluppi di FB in Meta) proietta la dominanza di FB anche nel prossimo futuro.

Per quanto riguarda Google, essa offre il notissimo social medium YouTube ed una serie di servizi online che costituiscono il c.d. ecosistema Google, come il browser Chrome, il motore di ricerca Google Search, i servizi Gmail, Google Maps, Google Photos, Google Drive, Google Play Store. In particolare, Google detiene una quota di mercato sostanzialmente monopolistica nei servizi dei motori di ricerca generici (cioè non specializzati in determinati settori) e nella c.d. *search advertising* (cioè la pubblicità mostrata in occasione di query su un motore di ricerca), anche mediante la progressiva attenuazione della differenza grafica tra risultati sponsorizzati e non. Si tratta anche qui di posizioni di dominanza difficilmente contendibili per la presenza di notevoli barriere all'ingresso, rappresentate dalle economie di scala nell'attività di indicizzazione delle pagine web e nella raccolta dei dati relativi alle ricerche (*click-and-query data*). Grazie alla titolarità di Android (il

sistema operativo per dispositivi mobili più diffuso al mondo) Google ha potuto ottenere dai produttori di hardware la preinstallazione dei propri servizi e persino il divieto di installazione di servizi concorrenziali con i propri, talvolta assumendo condotte ritorsive sui servizi prestati a terzi nel proprio ecosistema, dei quali anche i concorrenti non possono far a meno (si pensi all'intermediazione della pubblicità tra fornitori di contenuti ed inserzionisti, rispetto ai quali Google assume il ruolo di *gatekeeper*, con il crearsi di notevoli conflitti di interesse). Il contestuale controllo di tanti e tali servizi, da un lato, incentiva la società a riservare nell'ecosistema Google un trattamento preferenziale ai propri prodotti (*self-preferencing*), dall'altro produce in via sinergica un'enorme mole di dati personali, attraverso i quali Google può tracciare le condotte dei propri utenti (a partire dall'uso del browser in avanti) e influire sugli altri operatori, decidendo se farli o meno accedere a detti dati. Con l'assistente virtuale Google Assistant, ma soprattutto con il Google Cloud, la società sta anche estendendo la propria influenza alla c.d. *Internet of Things* (IoT) e, con accordi con i produttori di dispositivi, alle ricerche effettuate da smartphone attraverso query vocali.

Per quanto riguarda Amazon, essa da un lato è titolare della famosissima omonima piattaforma di commercio elettronico (rivestendo il ruolo di *gatekeeper* per far incontrare la domanda dei consumatori e l'offerta di aziende terze), dall'altro lato produce e vende sulla stessa piattaforma prodotti propri, con l'inevitabile insorgere di conflitti di interesse e del rischio del *self-preferencing* in un numero crescente di settori merceologici. Ad es., Amazon detiene una posizione sostanzialmente monopolistica, nel commercio dei libri ed ancor di più degli e-book, ma è altresì un importante editore. A ciò si aggiunge il ruolo di produttore di audiovisivi e di hardware, di titolare di un'estesissima rete di logistica e trasporto, di un sistema di pagamento elettronico e di leader mondiale nei servizi cloud. Si tratta, anche in questo caso, di una dominanza difficilmente contendibile a causa di barriere all'ingresso, tra cui i *network effect* (maggiori compratori attirano maggiori venditori in un circuito autoalimentantesi), l'esistenza di costi di transizione (rafforzato dall'utilizzo di programmi di fidelizzazione come Amazon Prime, per giunta offerto in perdita) e gli altissimi costi per duplicare un sistema di logistica molto ampio e capillare. Il doppio ruolo giocato da Amazon (di gestore della piattaforma e di concorrente dei venditori terzi) le consente altresì di sfruttare i dati sulle vendite dei prodotti terzi per trarne vantaggio. A questi dati si aggiungono poi quelli derivanti dall'enorme mole di transazioni realizzate sulla piattaforma e, da ultimo, i dati derivanti da dispositivi di domotica e di assistenza virtuale (Alexa), attraverso i quali Amazon ha acquisito una notevole forza di mercato nell'IoT, grazie anche al suo servizio cloud. Dati attraverso i quali Amazon può offrire ai propri utenti beni e servizi sempre più ritagliati sui loro gusti e preferenze.

Infine, per quanto riguarda Apple, essa, sebbene abbia sinora tratto gran parte dei suoi ricavi dalla vendita di dispositivi (come iPhone, iPad, Apple TV, ecc.) e dei loro accessori, ha acquisito un notevole potere di mercato nei sistemi operativi su dispositivi mobili (Apple è titolare del sistema iOS[24]) ed un potere monopolistico nella vendita (attraverso il suo canale esclusivo App Store) di tutte le applicazioni basate su iOS, anche se sviluppate da terze parti, controllando l'accesso a milioni di iPhone e di iPad (anche mediante la preinstallazione delle sue app) e creando un ecosistema da essa interamente dominato. La perfetta conoscenza dei dati di commercializzazione delle app terze consente ad Apple di proporre sul mercato applicazioni concorrenziali basate sulle stesse funzionalità di quelle di maggior successo. Con il suo assistente virtuale (Siri), la società ha persino rafforzato questa sua posizione anche nella disponibilità di dati, benché Apple offra in media ai propri utenti maggiori garanzie sul piano della privacy rispetto agli altri operatori. Apple ha poi acquisito, con Apple Music, un notevole potere di mercato anche nella commercializzazione di brani musicali ed è ben presente nell'audiovisivo attraverso Apple TV+.

Ebbene, per fronteggiare queste problematiche situazioni competitive, negli USA vengono ora proposti vari rimedi che vanno dall'introduzione di una presunzione di anticoncorrenzialità in ordine a nuove acquisizioni di imprese da parte delle piattaforme dominanti, a divieti per le *big tech* di tenere condotte discriminatorie (compreso il *self-preferencing*), sino all'imposizione di separazioni strutturali e divieti di operare in mercati contigui a quelli in cui le maggiori piattaforme sono già presenti[25], ovvero di obblighi propri dei gestori di servizi essenziali (*common carrier*)[26]. Rimedi, come si può notare, di marcato stampo regolatorio (specialmente gli ultimi indicati).

2.3. Analisi nell'UE ed in alcuni Paesi

Non sorprendentemente (visto che i mercati digitali sono globali) anche l'UE e singoli Paesi, non solo europei, hanno manifestato una generale insoddisfazione per i tradizionali rimedi antitrust ed individuato analoghe criticità in capo alle stesse piattaforme, pure per quel che riguarda il loro problematico rapporto con le libertà dei singoli[27].

Per gli aspetti antitrust, la Commissione europea ha avviato un progetto di riforma finalizzato ad identificare nuovi rimedi (*New Competition Tool* - NCT) idonei a risolvere i problemi strutturali riscontrati in alcuni mercati nel corso dei casi esaminati negli ultimi anni ai sensi degli artt. 101 e 102 TFUE[28]. Sebbene tali problemi strutturali si riscontrino anche in mercati tradizionali[29], è proprio nei nuovi mercati digitali (in cui i titolari delle piattaforme assumono, appunto, il ruolo di *gatekeeper* e posseggono per questo una completa conoscenza dei mercati) che c'è il rischio di una riduzione del grado complessivo di concorrenza e della possibilità – per le imprese *dominanti* in un mercato – di adottare strategie distorsive della concorrenza nei mercati adiacenti e – per le imprese persino *non dominanti*, ma dotate comunque di potere di mercato – di adottare nel loro stesso mercato strategie non contrastabili attraverso i tradizionali rimedi antitrust. La presenza nei mercati digitali di estreme economie di scala e di scopo nonché di forti esternalità di rete (che portano facilmente al *lock-in* degli utenti, anche per scarso ricorso al *multi-homing*[30]), assieme ad un alto grado di concentrazione dei mercati ed all'esistenza di barriere all'entrata, anche dovute al c.d. *zero pricing* ed alla centralità dei dati, sono tutti fattori che favoriscono il rischio di un'improvvisa caduta della concorrenza una volta che un'impresa abbia raggiunto in quel mercato una determinata soglia critica (c.d. *tipping market*).

Del resto, a conclusioni del tutto convergenti sono giunte anche le analisi economiche svolte in singoli Paesi[31], com'è avvenuto ad es. in Francia[32], in Germania[33], in Italia[34], nel Regno Unito[35] ed in Australia[36].

Va peraltro sottolineato che gli NCT non vengono proposti come unico rimedio al dominio delle piattaforme, come dimostra la presentazione da parte della Commissione di due proposte di regolamenti (il *Digital Services Act* (DSA)[37] e il *Digital Markets Act* (DMA)[38]) volti ad introdurre una regolazione *ex ante* e *platform-specific* (proposte che, per gli aspetti di rilievo per il presente lavoro, verranno esaminate nel § 5).

3. Inquadramento costituzionale e ricadute normative

3.1. Le piattaforme come "poteri privati"

In considerazione di quanto osservato sopra, non dovrebbero sussistere dubbi sulla posizione di dominanza economica rivestita dalle maggiori piattaforme, peraltro – come si è visto – foriera di conseguenze sul piano dei diritti di libertà non solo in campo economico. E, per quanto qui più rileva, è ormai comunemente condiviso l'assunto che le maggiori piattaforme svolgono un ruolo di *gatekeeper* anche nel campo delle libertà di espressione e di informazione, atteso che le piattaforme incidono *direttamente* sulla diffusione delle notizie e in generale delle idee[39]. Al riguardo, basti pensare alle attività di moderazione[40] e raccomandazione[41] dei contenuti svolte da quasi tutte le piattaforme (ivi comprese le attività di prioritarizzazione dei risultati e di completamento automatico delle query) nonché alla selezione algoritmica delle sole notizie rispondenti alle preferenze degli utenti individuate mediante la loro profilazione. Si pensi, ancora: per Facebook *almeno* al suo notissimo servizio di *newsfeed*; per Google *almeno* a Google News; per Amazon *almeno* alla sua attività di editore e venditore di libri[42] nonché a Prime Video; per Apple *almeno* ad Apple News e ad Apple TV+. Si consideri infine l'influenza *indiretta* esercitata mediante il controllo sulla pubblicità, che rappresenta la maggiore fonte di finanziamento dei media tradizionali.

Nelle più recenti analisi giuridiche, è ormai invalsa la qualificazione delle piattaforme come "poteri privati": cioè, soggetti che agiscono nelle forme del diritto privato, ma che, per la loro posizione di forza economica e/o sociale, sono capaci di incidere sull'esercizio delle libertà fondamentali dei singoli[43]. È, difatti, attraverso la mera predisposizione unilaterale di condizioni generali di contratto (CGC) variamente denominate[44] che vengono individuati i contenuti diffondibili (e non), nonostante si tratti di c.d. contratti *click wrap*, le cui condizioni vengono accettate dagli utenti senza neanche leggerle[45].

Come detto, la definizione di "poteri privati" è ampiamente utilizzata dai giuristi sia negli USA che da noi: sembra peraltro opportuno distinguere le diverse ragioni del suo utilizzo nei due contesti. Oltreoceano il tema viene evocato poiché, di norma, è esclusa l'efficacia delle previsioni costituzionali nei rapporti interprivati[46], salvo che un soggetto privato rivesta nei fatti un ruolo assimilabile a quello svolto da un soggetto pubblico (*state actor*) esercitando nei confronti di altri privati poteri assimilabili a quelli pubblici (si tratta delle nota e risalente *state action doctrine*[47]). Peraltro, le rigorose condizioni richieste per superare il test per la qualificazione come *state actor* rendono difficile trarre da questa sola qualifica (potere privato) conseguenze giuridiche nell'ordinamento statunitense.

In Europa ed in Italia, la tradizione dell'efficacia diretta delle disposizioni costituzionali (nota come *Drittwirkung*) invece consente di ricollegare a quella qualifica alcune conseguenze giuridiche ed apre, quantomeno per la giurisprudenza maggioritaria[48],

all'introduzione del rispetto delle libertà costituzionali tra i parametri per valutare i limiti all'autonomia contrattuale delle parti, anche relativamente alle CGC delle piattaforme digitali[49].

Un altro elemento che distingue, per quel che qui rileva, il contesto americano dal nostro è che negli USA, data l'ampia portata riconosciuta al *free speech*, le piattaforme possono richiamarsi al Primo Emendamento, nonostante la loro attività per legge non possa essere equiparata a quella di un editore[50]. Al contrario, un corretto inquadramento dell'attività delle piattaforme in un contesto europeo (ed italiano) dovrebbe ricollegarla alla (sola) libertà di iniziativa economica privata[51]. Di conseguenza, per quel che concerne la nostra Costituzione, l'attività delle piattaforme ben può essere limitata per tutelare sicurezza, libertà e dignità umana nonché per evitare che essa si svolga in contrasto con l'"utilità sociale"[52].

Al riguardo è significativo, per un verso, che nelle controversie presentatesi dinanzi ai giudici nazionali, le piattaforme non abbiano invocato, a sostegno delle loro tesi, l'art. 21 Cost. (anche solo sotto il profilo del rispetto della libertà dei media, restando in ciò fedeli all'impostazione in forza della quale esse non rispondono dei contenuti caricati dagli utenti) e, per altro verso, che nelle CGC l'enfasi venga posta sull'impegno a permettere agli utenti l'esercizio della loro libertà di espressione (e non delle piattaforme)[53]. Risulta perciò poco persuasivo il paragone, talvolta effettuato, tra la posizione delle piattaforme e quella degli editori e segnatamente delle imprese televisive, cercando di trarne conseguenze in merito alla (il)legittimità dell'imposizione alle piattaforme di limiti volti ad assicurare le libertà di espressione e di informazione nella moderazione dei contenuti[54].

Concludendo sul punto, quando si parla di potere privato va pertanto tenuto ben presente che si tratta di "potere d'impresa" *ex* art. 41 Cost., come avrebbe detto Stefano Rodotà[55].

3.2. Le libertà di espressione (e di informazione) e la censura online

Il fatto che, nella ricostruzione proposta, l'art. 21 Cost. non venga in considerazione per definire lo "statuto costituzionale delle piattaforme digitali"[56] non vuol ovviamente dire che esso non entri in gioco, sia sotto il profilo della libertà *individuale* di espressione degli utenti, sia sotto quello dell'interesse *generale* ad un'informazione pluralista. Significa piuttosto che, nel bilanciamento tra la libertà degli utenti e quella delle piattaforme, non ci si trova dinanzi all'arduo compito di dover contemperare – così come avviene, ad es., nella disciplina sulla *par condicio* – posizioni di privati che, *entrambi*, godono della tutela di cui all'art. 21 Cost. (nel caso dei media, quantomeno *sub specie* di libertà a darsi una propria linea editoriale). Ne consegue che i limiti ritenuti legittimamente imponibili ai media sono senz'altro riproponibili a carico delle piattaforme e che queste ultime sono, anzi, suscettibili di essere sottoposte a discipline anche più stringenti, al fine (e nei limiti) di garantire che l'attività economica da esse svolta non violi le libertà dei singoli.

Ciò ha una diretta ricaduta sui distinti (ma connessi) temi degli obblighi imponibili alle piattaforme e della c.d. censura privata da loro esercitata online.

Quanto alla censura privata (questione che ovviamente si poneva anche prima dell'avvento dei social network), va peraltro detto che la posizione della giurisprudenza costituzionale è, oltre che molto risalente, anche perplessa su alcuni aspetti di fondo. Se in una sentenza del 1970 la Corte affermava, infatti, con risolutezza che «non è lecito dubitare che la libertà di manifestare il proprio pensiero debba imporsi al *rispetto di tutti, delle pubbliche autorità come dei consociati*, e che nessuno possa recarvi attentato senza violare un bene assistito da rigorosa tutela costituzionale»[57], in due sentenze di poco successive la Consulta ha invece sostenuto che la censura vietata dal secondo comma dell'art. 21 debba identificarsi solo con l'«istituto tipico del diritto pubblico, secondo cui gli organi dello Stato (...) esercitano autoritativamente un controllo preventivo sulla stampa, adottato con provvedimento contenente un giudizio sulla manifestazione del pensiero rimesso alla Pubblica amministrazione»[58].

In dottrina, nonostante sia ampiamente condivisa l'opinione secondo cui l'art. 21 Cost. opera anche nei rapporti interprivati[59], il tema della censura privata non sembra essere stato particolarmente investigato, salvo che con riferimento alle decisioni del direttore responsabile nell'ambito dei media tradizionali ed agli edicolanti per la responsabilità nell'esposizione di stampati pornografici. In particolare, quando il tema della censura privata è stato affrontato *all'interno* dei media tradizionali, il bilanciamento tra le contrapposte situazioni (tutte riferibili all'art. 21 Cost.) è stato risolto facendo prevalere, per un verso, il soggetto (cor)responsabile per i contenuti che l'altro soggetto pretendesse di diffondere (esemplare è l'ipotesi del direttore responsabile, *ex* art. 57 c.p.[60]) e, per altro verso, l'editore del medium, il quale, oltre ad essere civilmente corresponsabile per quei contenuti, sopporta un rischio di impresa *strettamente correlato* all'indirizzo editoriale che ha diritto di imprimere al medium, anche in forza del riconoscimento della libertà di espressione pure in capo alle persone

giuridiche private (si pensi al contrasto sul mutamento dell'indirizzo della testata tra la società editoriale ed il singolo redattore, che può soltanto dimettersi a condizioni per lui meno sfavorevoli, invocando la c.d. clausola di coscienza[61]).

Solo poche, pur autorevoli, voci hanno posto l'attenzione sul problema della censura privata operata dal "monopolista di un mezzo di diffusione" che assuma "veste di censore", per concludere peraltro che «una censura esercitata da privati nei confronti di privati ... è qualcosa di ben peggio» rispetto alla censura esercitata dai pubblici poteri[62].

Ora, tornando su queste basi al tema della censura privata online, la qui esclusa invocabilità dell'art. 21 Cost. da parte delle piattaforme trova conferma nel fatto che l'intervento censorio non potrebbe essere giustificato dalla titolarità in capo alla piattaforma della libertà di espressione e/o dal suo diritto di imprimere al social una determinata linea editoriale. E ad un risultato del tutto analogo dovrebbe pervenirsi anche applicando il sopra richiamato "criterio della responsabilità", considerata la ben nota esenzione di responsabilità disposta a favore delle piattaforme per i contenuti caricati dagli utenti[63].

Sul piano costituzionale dovrebbe perciò escludersi che la censura privata delle piattaforme possa prevalere sulla libertà di manifestazione dei singoli[64], salvo che essa non si risolva nel reprimere espressioni già considerate illecite dall'ordinamento giuridico (compresa ovviamente la Costituzione[65]).

È pur vero che spesso sono proprio gli Stati a "delegare"[66] alle piattaforme quell'attività di censura che essi non effettuano per ragioni legate ad asserite difficoltà tecniche o economiche. Ma anche "uno Stato che miri ad essere minimo" dovrebbe considerare "irrinunziabile" il compito di decidere cosa possa essere pubblicamente diffuso in rete[67], quantomeno limitandosi ad attribuire ai titolari dei social una delega solo "funzionale"[68]. In ogni caso, uno Stato non dovrebbe rinunziare a regolare l'esercizio di questi poteri privati, prevedendo idonee garanzie a tutela delle libertà dei suoi cittadini, visto che ragioni di ordine costituzionale non soltanto lo consentono, ma addirittura lo impongono, come si dirà subito.

Passando infatti al tema degli obblighi imponibili alle piattaforme per garantire le libertà di espressione e di informazione, tanto che si ritenga che le piattaforme decidano *tout court* cosa vediamo o leggiamo[69], quanto che si ritenga invece che esse si "limitino" ad organizzare l'informazione mondiale[70] o persino che vengano paragonate solo a dei distributori o alle edicole[71], non può disconoscersi il ruolo comunque determinante da loro giocato nell'ambito informativo.

Di conseguenza, così come non si è, ad es., mai dubitato – quantomeno da noi – della legittimità dell'obbligo di parità di trattamento imposto ai distributori di giornali o alle edicole[72], proprio per tutelare il diritto all'informazione, non dovrebbe neppure dubitarsi della legittimità di un'eventuale imposizione di siffatti obblighi a carico delle piattaforme. Alla stessa stregua, sembra *a fortiori* legittima l'imposizione a carico delle piattaforme degli obblighi già imposti ai media al fine di tutelare il pluralismo informativo, tanto più che la Corte europea dei diritti dell'uomo (CtEDU) ha in più occasioni affermato che, in forza dell'art. 10 CEDU, sugli Stati incombe l'*obbligo positivo* di predisporre un quadro legislativo e amministrativo idoneo ad assicurare un pluralismo effettivo dell'informazione, di cui lo Stato dev'essere l'*ultimate guarantor*[73].

Il ruolo monopolistico o quasi-monopolistico assunto da alcune piattaforme nei rispettivi mercati dovrebbe inoltre rendere ancor più giustificato un intervento[74] e, forse, superare possibili critiche (dogmaticamente liberali) volte a contestare in radice la pretesa di trattare e disciplinare il "potere sociale" delle piattaforme alla stregua di un "potere giuridico"[75]. La presenza di posizioni dominanti dovrebbe, infatti, suscitare minori perplessità in chi ritiene che siano contrarie anche ai principi liberali le «attività gestite in situazioni di monopolio o in posizioni del tutto "dominanti"»[76,77].

A queste osservazioni non varrebbe obiettare che le sfide poste dalle piattaforme sono senza precedenti nella storia dell'informazione e che non va compiuto l'errore di guardare ad esse utilizzando vecchi schemi (più o meno come si fece considerando le auto "carrozze senza cavalli"[78]) ed ancora che oggi non sono più i media ad essere gli *intermediari*[79], venendo invece essi *intermediati* dalle piattaforme[80]. Infatti, qui non si vuole affatto proporre di applicare acriticamente le stesse regole ai nuovi intermediari, quanto piuttosto di prendere atto che, ferma restando la necessità di applicare strumenti di tutela adatti ai nuovi attori, alcuni problemi di fondo sollevati dalle piattaforme possono trovare un buon punto di partenza nella pluridecennale elaborazione sui media[81], tanto più che l'inapplicabilità ad esse dell'art. 21 Cost. consente un più ampio intervento sulle piattaforme.

Neppure varrebbe obiettare che l'esclusione dai social non comporta in sé l'impossibilità per un soggetto di esercitare la propria libertà di espressione con altri mezzi, poiché una simile obiezione avrebbe potuto muoversi, ad es., anche alla disciplina sulla *par condicio* (visto che sarebbero sicuramente rimasti fruibili media diversi dalla radio e dalla televisio-

ne) e che, in teoria, persino nel caso dei tradizionali servizi pubblici potrebbe predicarsi la non indispensabilità degli stessi per esercitare i propri diritti[82].

È peraltro vero che, per pervenire ad una disciplina a tutela dell'informazione che sia efficace ma al contempo proporzionata ai problemi da affrontare, bisogna utilizzare un set di criteri adatti ai fenomeni che si vogliono regolare: quindi se, ad es., per un motore di ricerca potrebbe esser lecito guardare alla quota di mercato (in mancanza di altri dati più pertinenti), nel caso dei social network potrebbe risultare più appropriato tener presente il numero degli utenti (una sorta di audience, almeno potenziale) della piattaforma[83]. E, considerato l'ambito ancora prevalentemente nazionale del pluralismo informativo (dovuto anche al fattore linguistico ed al livello nazionale della gran parte delle consultazioni elettorali e referendarie), a tal fine bisognerebbe guardare alle quote di mercato ed agli utenti di *ciascun* Paese[84].

Inoltre, la previsione di questi criteri, da un lato, eviterebbe di trattare situazioni diverse in modo eguale (si pensi a social network assolutamente nascenti o irrilevanti ai fini del pluralismo informativo dato il loro ridotto numero di utenti), dall'altro promuoverebbe l'ingresso nel mercato di nuovi player (i quali altrimenti non potrebbero paradossalmente giovarsi dei vantaggi sin qui goduti dalle piattaforme ora dominanti).

4. Le proposte di *Digital Markets Act* (DMA) e *Digital Services Act* (DSA)

Alla luce delle considerazioni sopra svolte è possibile esaminare il primo tentativo, ancora *in fieri*, di regolare il potere privato delle piattaforme digitali, cioè la presentazione delle *proposte* di DSA e DMA, evidenziandone luci ed ombre, limitatamente ai temi qui di interesse.

Va detto in premessa che, sebbene le due coeve proposte debbano essere valutate in connessione tra loro[85] (anche in considerazione dell'utilizzo promiscuo delle piattaforme per fini informativi e commerciali), il DMA ha ad oggetto solo gli squilibri *economici* e le pratiche *commerciali* sleali delle piattaforme digitali (collocandosi perciò in un rapporto di più diretta complementarità con la normativa antitrust e con le proposte sui NCT), laddove il DSA intende introdurre, con portata *orizzontale*[86], norme relative a tutte le attività degli intermediari online – quindi anche non economiche – ed alle responsabilità di questi ultimi. Questa diversità di ambiti ha un suo riscontro, oltre che nel contenuto delle due proposte, anche sul piano lessicale, poiché nel DMA i soggetti sottoposti agli specifici obblighi ivi previsti vengono definiti "*gatekeeper*"[87], mentre nel DSA i differenti obblighi ivi previsti si applicano ai "prestatori di servizi intermediari" (*mere conduit*, *caching* e hosting[88]) ed alle "piattaforme online"[89], discostandosi così le proposte dall'uso comune dei tre sintagmi. Peraltro, alcune tipologie di operatori (ad es., social media e mercati online) ben possono soddisfare i requisiti di tutte le definizioni[90], così riconfermandosi l'obiettiva correlazione tra le due proposte normative.

In particolare, il DSA ha come obiettivo dichiarato quello di assicurare che i cittadini UE possano esercitare liberamente i propri diritti fondamentali, in particolare la libertà di espressione e di informazione, imponendo anche a tal fine obblighi asimmetrici ai prestatori di servizi intermediari in funzione della loro natura e dimensione[91].

Il DSA prevede, infatti, una disciplina "a cerchi concentrici". *Nel primo cerchio* (il più ampio) rientrano *tutti* i prestatori di servizi intermediari, nei confronti dei quali, per un verso, sono ribadite le regole di (esenzione da) responsabilità già contenute nella direttiva sul commercio elettronico, per altro verso vengono però introdotti nuovi obblighi di diligenza. *Nel secondo cerchio* rientrano i soli prestatori di servizi di hosting – appunto, le "piattaforme online" – assoggettati ad obblighi più puntuali. *Nel terzo cerchio* (il più ristretto) vengono introdotti obblighi ancor più rigorosi per le sole "piattaforme di dimensioni molto grandi" (in prosieguo "grandi piattaforme"), cioè quelle che prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio di almeno 45 milioni nell'UE, pari al 10% della popolazione europea.

Di conseguenza, per tutti i prestatori dei servizi intermediari sono previsti obblighi: di istituire un punto di contatto unico cui gli Stati, la Commissione e gli altri organismi pubblici possano rivolgersi ai fini dell'applicazione del regolamento (art. 10); di designare, qualora non siano stabiliti in alcuno Stato membro, un rappresentante legale in uno degli Stati in cui offrono i propri servizi (art. 11); di inserire nelle CGC informazioni sulle politiche di moderazione dei contenuti (art. 12); di pubblicare annualmente una relazione sulle misure adottate nella moderazione dei contenuti (art. 13); altri obblighi contenuti nei piani di crisi (per affrontare circostanze straordinarie che incidano sulla sicurezza o sulla salute pubbliche) e negli strumenti di auto(e co)regolamentazione anche nel campo della pubblicità online (artt. 34-37).

Per i prestatori di servizi di hosting, sono previsti anche obblighi di dotarsi di un sistema per la notifica di contenuti illegali da parte degli utenti e per l'intervento sugli stessi contenuti da parte dell'*hoster* (c.d. *notice and action*: art. 14) nonché di fornire

una motivazione per la rimozione o la disabilitazione dell'accesso per contenuti illegali o contrari alle CGC (art. 15).

Per le piattaforme online (escluse le piccole e le micro imprese) sono previsti ulteriori obblighi: dotarsi di un sistema efficace di gestione dei reclami (art. 17); consentire agli utenti di rivolgersi ad un organismo di risoluzione extragiudiziale delle controversie di loro scelta (art. 18); dotarsi di sistemi che consentano agli utenti di conoscere la natura pubblicitaria delle informazioni, il loro committente ed i parametri in base ai quali all'utente viene mostrata quella pubblicità (art. 24).

Infine, per le grandi piattaforme, sono altresì previsti – sempre per quel che qui rileva – i seguenti ulteriori obblighi: valutare annualmente i rischi sistemici, quali la diffusione di contenuti illegali, gli effetti negativi sui diritti fondamentali per l'esercizio dei diritti fondamentali (comprese le libertà di espressione e di informazione), la manipolazione del servizio, con ripercussioni negative tra l'altro sul dibattito civico o i processi elettorali, e gli effetti prodotti dai sistemi di moderazione e raccomandazione dei contenuti nonché di visualizzazione della pubblicità (art. 26), adottando misure di attenuazione dei suddetti rischi (art. 27); informare gli utenti dei principali parametri dei sistemi di raccomandazione, offrendo loro almeno un'opzione di fruizione dei servizi non basata sulla profilazione (art. 29); tenere e rendere accessibile pubblicamente un registro relativo al contenuto delle pubblicità, ai committenti, al periodo di diffusione, a quali gruppi di utenti fosse destinata ed in base a quali parametri, al numero dei destinatari raggiunti (art. 30).

Passando allora ad una valutazione di questo apparato di previsioni, va senz'altro ascritto a merito degli organismi UE il fatto stesso di aver prefigurato un articolato *corpus* normativo dotato di apparato sanzionatorio e volto ad affrontare i temi qui analizzati, dando per giunta giusto rilievo al criterio del numero degli utenti raggiunti, per qualificare le piattaforme come "grandi" e per assoggettarle ad obblighi più stringenti anche a garanzia delle libertà di espressione ed informazione (cons. 94), in linea con quanto sopra evidenziato (§ 3). Di tale scelta si ha significativa conferma anche nelle previsioni secondo cui, per un verso, persino piccole o micro imprese possono essere qualificate come grandi piattaforme ove raggiungano le previste soglie di utenti (cons. 43) e, per altro verso, alti fatturati o elevate valorizzazioni di mercato costituiscono (solo) un elemento a favore di tale qualificazione (cons. 55).

L'individuazione di un criterio basato sugli utenti *soltanto a livello UE* sembra, tuttavia, un punto critico della proposta, vista la già rilevata dimensione eminentemente nazionale dei fenomeni da regolare (§ 3.2): meglio sarebbe integrare questo requisito con una soglia di utenti *per singolo Stato membro*, analogamente a quanto fatto nel DMA per individuare i *gatekeeper* (ancorché in quel caso si faccia riferimento all'offerta del servizio in almeno *tre* Stati).

Entrando ancor più nello specifico, sembra possibile individuare nel DSA due tipi di regole: quelle "sostanziali" e quelle "procedimentali".

Le prime individuano anzitutto i contenuti illegali (cioè quelli contrari al diritto UE o degli Stati membri[92]) e quelli contrari alle CGC, che – rispettivamente – devono e possono essere rimossi o limitati nell'accesso in conseguenza dell'attività di moderazione svolta dalle piattaforme. Peraltro, a questo riguardo si rileva un'equiparazione del tutto impropria tra le due categorie di contenuti, in tal modo finendo col lasciare mano libera alle piattaforme nel rimuovere anche contenuti giuridicamente del tutto *leciti*, così fallendo nel rimediare a quella violazione delle libertà degli utenti che deriva appunto dalla censura privata[93]. Non a caso i partecipanti alla fase di consultazione pubblica avevano concordato sul fatto che «i contenuti "dannosi" (ma non illegali ...)[94] non ... dovrebbero essere soggetti a rimozione, giacché si tratta di una questione delicata con gravi implicazioni per la libertà di espressione»[95].

Possono farsi rientrare tra le regole sostanziali anquelle relative alla pubblicità, assolutamente opportune, ma che sollevano una criticità in quanto potrebbero essere di ostacolo all'introduzione, in materia di pubblicità politico-elettorale, di divieti da parte dei singoli Stati membri. E, in proposito, la recente proposta di regolamento della pubblicità politica[96] appare confermare queste perplessità, là dove sembrerebbe far salva solo la possibilità che gli Stati membri possano prevedere «periodi di silenzio che precedono le elezioni o i referendum»[97], ma non divieti *tout court* di pubblicità politico-elettorale online.

Si tratta di aspetti problematici che non possono essere superati dalle ben più ampie regole procedimentali previste a favore degli utenti[98], le quali – sebbene anch'esse estremamente opportune – contengono un'altra criticità là dove, nel caso di decisioni relative alla rimozione/limitazione di contenuti caricati da utenti, prevedono un coinvolgimento di questi ultimi *solo dopo o, al più, al momento dell'esecuzione della decisione*[99], mentre per non sacrificare del tutto le libertà dei fornitori di contenuti andrebbe previsto perlomeno un loro coinvolgimento *anteriormente* all'esecuzione della decisione.

Le proposte, pur rappresentando un buon punto di partenza, potrebbero perciò essere migliorate.

5. Considerazioni finali

All'esito dell'*excursus* svolto, si può tentare di trarre qualche conclusione.

Per ciò che concerne il potere privato esercitato dalle piattaforme, sembra evidente che – come sottolineato in altra occasione[100] – il cittadino, soprattutto in attesa dell'approvazione di una disciplina *ad hoc*, possa trovare tutela solo mediante un insieme, per così dire, olistico di misure che spaziano dall'applicazione rigorosa della disciplina antitrust e della privacy[101] sino all'applicazione della normativa codicistica sui limiti all'autonomia contrattuale derivanti da una *Drittwirkung* almeno "mediata" dalle clausole dell'ordine pubblico e del buon costume[102], nonché sulla tutela del contraente debole e, ancor di più, sulla disciplina consumeristica[103], per finire con la normativa elettorale, ivi compresa la *par condicio*. In effetti, in un moderno Stato costituzionale, a fronte del crescere di poteri privati è proprio lo Stato che può e deve ergersi a garante delle libertà dei singoli.

Quanto alla censura privata online ed alla connessa tutela delle libertà di espressione ed informazione, occorre constatare che, per ora, il legislatore (anche UE) tende ad introdurre misure di carattere soprattutto procedimentale (peraltro indispensabili), lasciando in sostanza mano libera alle piattaforme, quantomeno in prima battuta, nel decidere quali contenuti possano circolare o meno, come può evincersi dalla scelta di equiparare contenuti illeciti e contenuti potenzialmente "dannosi" (ma leciti) e dal potere attribuito alle stesse piattaforme, in entrambi i casi, di rimuovere/limitare i contenuti, senza neppure dover passare attraverso l'intervento dell'autorità giurisdizionale al fine di effettuare un bilanciamento con i diritti fondamentali dei cittadini: passaggio invece paradossalmente imposto alle autorità pubbliche quando adottano provvedimenti aventi effetti del tutto analoghi[104]. Quasi che gli stessi legislatori fossero sempre più incerti in ordine al *carattere prioritario* della tutela delle libertà di espressione e di informazione e, in ogni caso, desiderassero che le piattaforme continuino a fare "pulizia", limitandosi i poteri pubblici ad intervenire solo nei casi più eclatanti e controversi, tuttavia lasciando così maggiormente indifesi proprio quelle idee e quei soggetti minoritari nella società, cioè proprio quel che nel costituzionalismo occidentale le suddette libertà mirano invece a proteggere.

Note

[1] M. Bassini, *Internet e libertà di espressione*, Aracne, 2019, p. 76.

[2] Il concetto è acquisito da lungo tempo: cfr. Commissione Europea, *Pluralism and media concentration in the internal market*, Libro verde, 13 gennaio 1993, p. 82 e, da ultimo, la direttiva (UE) 2018/1972 che istituisce il codice europeo delle comunicazioni elettroniche, dell'11 dicembre 2018.

[3] In questo senso, per la dottrina italiana v. R. Niro, *Profili costituzionali della disciplina antitrust*, CEDAM, 1994: M. Manetti, *I fondamenti costituzionali della concorrenza*, in "Quaderni costituzionali", 2019, n. 2, pp. 315-332; con specifico riferimento alle piattaforme digitali, M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in "La Rivista Gruppo di Pisa", 2021, n. 2, p. 187. Per la dottrina americana si rinvia al § 2.

[4] Per una completa panoramica R. Pardolesi, *Hipster antitrust e sconvolgimenti tettonici: back to the future?*, in "Mercato Concorrenza Regole", 2019, n. 1, pp. 81-94.

[5] Per la letteratura americana, si v., tra gli altri, J.D. Wright, E. Dorsey, J. Klick, J.M. Rybnicek, *Requiem for a Paradox: The Dubious Rise and Inevitable Fall of Hipster Antitrust*, in "Arizona State Law Journal", vol. 51, 2019, n. 1, p. 293-369; T.J. Muris, J.E. Nuechterlein, *Chicago and Its Discontents*, in "The University Chicago Law Review", vol. 87, 2020, n. 2, p. 495-521; S.B. Sacher, J.M. Yun, *Twelve Fallacies of the «Neo-Antitrust» Movement*, in "George Mason Law Review", vol. 26, 2019, n. 5, p. 1491-1530.

[6] Ad es., il tema delle c.d. *killer acquisition* è stato esplorato anche con riferimento all'industria farmaceutica: C. Cunningham, F. Ederer, S. Ma, *Killer Acquisitions*, in "Journal of Political Economy", vol. 129, 2021, n. 3, p. 649-702. Con riferimento alle piattaforme digitali si v. C. Scott Hemphill, T. Wu, *Nascent Competitors*, in "University of Pennsylvania Law Review", vol. 168, 2020, n. 7, p. 1879-1910.

[7] *Rectius*, dal benessere complessivo della società, indipendentemente da preoccupazioni relative agli aspetti distributivi di tale benessere tra imprese e consumatori.

[8] Tra i primi sostenitori di questo "nuovo" corso della dottrina antitrust negli USA vengono citati in genere i lavori di R.H. Bork, *The Antitrust Paradox: a Policy at War With Itself*, Basic Books, 1978, e R.H. Bork, W.S. Bowman Jr, *The Crisis in Antitrust*, in "Columbia Law Review", vol. 65, 1965, n. 3, p. 363-376. Più esattamente, alla scuola di Chicago si affianca, nella critica dell'originario approccio antitrust, il movimento c.d. revisionista, che riconduce l'efficienza del sistema al problema dei costi di transazione: in proposito, per tutti F. Denozza, *Chicago, l'efficienza e il diritto antitrust*, in "Giurisprudenza commerciale", 1988, n. 1, pp. 5-34.

[9] L.M. Khan, *Amazon's Antitrust Paradox*, in "The Yale Law Journal", vol. 126, 2017, n. 3, p. 710 ss., che sin dal titolo si pone in rapporto critico con la scuola di Chicago, così sintentizza i punti chiave dell'approccio precedente: «(1) monopolistic and oligopolistic market structures enable dominant actors to coordinate with greater ease and subtlety, facilitating conduct like price-fixing, market division, and tacit collusion; (2) monopolistic and oligopolistic firms can use their existing dominance to block new entrants; and (3) monopolistic and oligopolistic firms have greater bargaining power against consumers, suppliers, and workers, which enables them to hike prices and degrade service and quality while maintaining profits» (p. 718). L'A. è l'attuale presidente della *Federal Trade Commission* (FTC).

[10] Tra le altre, *U.S. v. General Dynamics*, 415 U.S. 486 (1974), *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574 (1985).

[11] Peraltro ingiustificata, vista l'autorevolezza di alcuni sostenitori ed il fatto che queste tendenze possono vantare un diretto collegamento con la c.d. scuola di Harvard, su cui v. R. Niro, *Profili costituzionali della disciplina antitrust*, cit., p. 64.

[12]Dal nome del noto giurista progressista ed influente membro della Corte Suprema Louis Brandeis, autore tra l'altro nel 1934 del libro *The Curse of Bigness*, titolo non a caso riproposto per una sua recente opera da uno dei più autorevoli sostenitori della *neo-brandeisian agenda* T. Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*, Columbia Global Reports, 2018.

[13]Si segnala che, nel presente lavoro (salvo che nel § 4), l'espressione *gatekeeper* (controllore dell'accesso), così come quella di "piattaforme online", vengono utilizzate in senso generico e non nella specifica accezione utilizzata dalla Commissione europea nelle proposte di regolamento per i mercati ed i servizi digitali esaminati nel § 4.

[14]Per maggiori riferimenti si rinvia a L.M. Khan, *op. cit.*, p. 746 ss.

[15]Si v. S. Zuboff, *Il capitalismo della sorveglianza*, Luiss University Press, 2019, p. 37 ss., e in termini più divulgativi R. Foroohar, *Don't Be Evil*, Penguin, 2019, p. 23 ss.

[16]Al riguardo L.M. Khan, *op. cit.*, p. 740 (nota 158) richiama la definizione dello Sherman Act fornita dallo stesso senatore John Sherman nei termini di "a bill of rights, a chart of liberty" (51 CONG. REC. 13,231 (1914): *statement of Sen. Reed*). Per una puntuale ricostruzione delle finalità originarie dello Sherman Act, si rinvia a R. Niro, *Profili costituzionali della disciplina antitrust*, cit., p. 22 ss. e p. 44 ss.

[17]U.S. House of Representatives, *Investigation of Competition in Digital Markets. Majority Staff Report and Recommendations*, p. 18.

[18]*Executive Order on Promoting Competition in the American Economy*, Sec. 2 (b), citando *Northern Pacific Railway Co. v. United States*, 356 U.S. 1, 4 (1958).

[19]Producendo un aumento dei prezzi, una riduzione della qualità di beni e servizi, riducendo l'innovazione e la scelta a disposizione dei consumatori.

[20]Significativamente, il 13 gennaio 2021, il DoJ ha avviato un'azione contro Facebook, in cui ha tra l'altro contestato il fine anticoncorrenziale delle acquisizioni di Instagram e di WhatsApp (avvenute rispettivamente nel 2012 e nel 2014 senza rilievi sia nel primo caso, che nel secondo), chiedendo al giudice di ordinare a FB la dismissione delle due piattaforme.

[21]Per i dettagli si rinvia a U.S. House of Representatives, *op. cit.*

[22]Gli utenti di un social network come FB vogliono condividere le loro idee ed esperienze con i propri familiari ed amici e quindi molto difficilmente sono disposti a cambiare social, una volta che hanno lì stabilito il proprio centro di relazioni; alla stessa maniera nei servizi di messaggistica come WhatsApp la diffusione di un'applicazione, una volta raggiunta una certa massa critica, tende ad affermarsi come piattaforma assolutamente dominante. Il che, trattandosi di un fenomeno che si autoalimenta, fa sì che in questi mercati viga il principio *the winner takes all*.

[23]Non da ultimo, il tempo da spendere per imparare ad usare la nuova app e trasferirvi i vecchi file: cfr. *United States v. Microsoft Corp.* (1999).

[24]Che si spartisce con Android di Google l'intero mercato mondiale dei sistemi operativi mobili.

[25]V. U.S. House of Representatives, *op. cit.*

[26]L.M. Khan, *op. cit.* Con *common carrier* si individuano di solito i gestori di servizi essenziali, assoggettati ad una serie di obblighi nel pubblico interesse, primo fra tutti l'obbligo di contrarre con tutti i richiedenti, talvolta accompagnato dal riconoscimento di esenzioni da certe responsabilità o di altre condizioni di favore: per approfondimenti, T. Wu, *Is filtering Censorship? The Second Free Speech Tradition*, Governance Studies at Brookings, 2010; da ultimo v. la *concurring opinion* del giudice conservatore Clarence Thomas nel caso *Joseph R. Biden et al. v. Knight First Amendment Institute at Columbia University*, 5 aprile 2021 (*opinion* resa in occasione della dichiarazione di improcedibilità, per la sopravvenuta elezione di Biden, del caso originariamente riguardante Trump).

[27]Su quest'ultimo punto, Commissione europea, *Comunicazione sul piano d'azione per la democrazia in Europa*, COM(2020) 790 final, del 3 dicembre 2020.

[28]In via riassuntiva, l'*Inception Impact Assessment*, 2020; per approfondimenti v. J. Crémer, Y.-A. de Montjoye, H. Schweitzer, *Competition policy for the digital era*, European Commission, 2019; A. Fletcher, *Market Investigations for Digital Platforms: Panacea or Complement?*, 2020; G.S. Crawford, P. Rey, M. Schnitzer, *An Economic Evaluation of the EC's Proposed "New Competition Tool"*, Publications Office of the European Union, 2020; M. Motta, M. Peitz, *Intervention triggers and underlying theories of harm*, Publications Office of the European Union, 2020; R. Whish, *New Competition Tool*, Publications Office of the European Union, 2020.

[29]Dall'energia all'agricoltura, dai farmaci ai media, alcuni dei quali sono già digitalizzati o sono comunque destinati a divenirlo.

[30]Vale a dire, in questo contesto, l'utilizzo da parte dell'utente di più servizi con analoghe funzionalità (ad es., più social network).

[31]Per maggiori approfondimenti, si v. F. Petrocelli, *Nuovi approdi e proposte di regolazione contro gli abusi di dominanza nei mercati digitali: una analisi comparativa*, in "Federalismi.it", 2021, n. 15.

[32]Authorité de la Concurrence – Bundeskartellamt, *Competition Law and Data*, 2016.

[33]V. il Bundeskartellamt in Provv. 6 febbraio 2019, B6-22/16.

[34]V. Autorità garante della concorrenza e del mercato, Autorità per le garanzie nelle comunicazioni, Garante per la protezione dei dati personali, *Indagine sui Big Data*, 2020.

[35]V. Competition and Market Authority, *Online Platforms and digital advertising, Market Study, Final Report*, July 2020, p. 54.

[36]Australian Competition and Consumer Commission – ACCC, *Digital Platforms Inquiry, Final Report*, June 2019.

[37]Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE COM(2020) 845 final del 15 dicembre 2020.

[38]Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) COM(2020) 842 final del 15 dicembre 2020.

[39]Cfr., ad es., la *Relazione di accompagnamento al DMA*, nota 2, nonché per tutti J. Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, in "Fordham Law Review", vol. 80, 2012, n. 4, p. 1536 ss.

[40]In base all'art. 3 del DSA, per "moderazione dei contenuti" si intendono le attività svolte dai prestatori di servizi intermediari al fine di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le loro condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o di dette informazioni, quali la loro retrocessione o rimozione o la disabilitazione dell'accesso agli stessi, o sulla capacità dei destinatari di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio.

[41]In base all'art. 2 del DSA, per "sistema di raccomandazione" si intende un sistema interamente o parzialmente automatizzato che una piattaforma online utilizza per suggerire

ai destinatari del servizio informazioni specifiche tramite la propria interfaccia online, anche in base ad una ricerca avviata dal destinatario o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate.

[42]V. gli esempi fatti al riguardo nella *concurring opinion* di Justice Thomas, cit., p. 8.

[43]Su cui, per la letteratura italiana, v. G. Lombardi, *Potere privato e diritti fondamentali*, Giappichelli, 1970; C.M. Bianca, *Le autorità private*, Jovene, 1977; nonché più di recente M. Esposito, *Profili costituzionali dell'autonomia privata*, CEDAM, 2003; ed a quarant'anni dalla pubblicazione del volume di Bianca, P. Sirena, A. Zoppini (a cura di), *Poteri privati e diritto della regolazione*, RomaTrE-Press, 2018.

[44]Condizioni d'uso, Standard della Community, ecc.

[45]Sul tema M.A. Lemley, *Terms of Use*, in "Minnesota Law Review", vol. 91, 2006, p. 459-483; T.J. Maronick, *Do Consumers read Terms of Service when installing Software? A Two-Study Empirical Analysis*, in "International Journal of Business and Social Research", vol. 4, 2014, n. 6, p. 137-145; per la sottolineatura dell'asimmetria anche tecnologica che rende questi rapporti contrattuali ancor più sperequati G. De Gregorio, *From Constitutional Freedoms to Power: The Law of the Platforms. Protecting Fundamental Rights Online in the Algorithmic Society*, in "European Journal of Legal Studies", vol. 11, 2019, n. 2, p. 65-103.

[46]Sul tema si v. O. Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in "MediaLaws", 2018, n. 3, p. 138-163.

[47]Su cui, per riferimenti relativi al tema del potere esercitato dalle piattaforme sul *free speech*, v. M. Bassini, *Internet e libertà di espressione*, cit., p. 189 ss. e, da ultimo, Id., *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in questa Rivista, 2021, n. 2.

[48]V., ad es., i provvedimenti cautelari concessi nel giudizio *CasaPound c. FB*, commentati in O. Grandinetti, *Facebook v. CasaPound e Forza Nuova, ovvero la disattivazione di pagine social e le insidie della disciplina multilivello dei diritti fondamentali*, in "MediaLaws", 2021, n. 1 ed *ivi* alcune considerazioni su tale giurisprudenza.

[49]Sul punto sia consentito rinviare per brevità a O. Grandinetti, *Facebook v. CasaPound e Forza Nuova*, cit.

[50]Il punto è ben sottolineato nella *concurring opinion* di Justice Thomas, cit., che richiama anche la ben nota sec. 230 del *Communications Decency Act* (CDA).

[51]Per l'inquadramento dell'attività dei social network nell'ambito dell'art. 41 Cost. v. M. Betzu, *Regolare Internet*, Giappichelli, 2012, pp. 42-43 e p. 149; M. Orofino, *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Giappichelli, 2014, p. 19; M. Cuniberti, *Potere e libertà nella rete*, in "MediaLaws", 2018, n. 3; e, se si vuole, O. Grandinetti, *Facebook v. CasaPound e Forza Nuova*, cit. Per la differenza di inquadramento tra USA ed UE, G. De Gregorio, *op. cit.*

[52]Non sembrano invece persuasive le posizioni dottrinali che qualificano come "formazioni sociali" *ex* art. 2 Cost., alternativamente, l'intera rete Internet (P. Passaglia, *Le formazioni sociali e Internet*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), "Diritti e libertà in Internet", Mondadori Education, 2017) o i soli social network (M.R. Allegri, *Ubi Social, Ibi Ius*, Franco Angeli, 2018). Sebbene anche queste ricostruzioni siano mosse dal lodevole intento di arginare il potere delle piattaforme digitali (visto che l'art. 2 Cost. garantisce i diritti inviolabili dell'uomo anche "*nelle* formazioni sociali"), esse sembrano in realtà seguire un itinerario giuridico tortuoso e forse persino pericoloso (in proposito si rinvia a M. Cuniberti, *op. cit.*). Del resto, appare inverosimile che l'elemento "psicologico" (rappresentato dall'interesse comune, diverso e superiore rispetto a quello dei singoli componenti: E. Rossi, *Le formazioni sociali nella Costituzione italiana*, CEDAM, 1988, p. 152) possa sussistere in una comunità che verrebbe ad instaurarsi, ad es., tra i tre miliardi di utenti di FB, costituiti da soggetti animati dai più vari interessi (da quello puramente "sociale" a quello invece esclusivamente "commerciale") e da sentimenti anche di radicale reciproca ostilità (si pensi che su FB vi sono comunità che aspirano persino alla loro reciproca eliminazione fisica, come nel caso degli estremisti palestinesi e sionisti, sciiti e sunniti e così via): in realtà, l'unico interesse omogeneo e "superiore" è quello egoistico e imprenditoriale del gestore del social. In secondo luogo, in accordo con le più recenti ed approfondite analisi antitrust, ciò che distingue i "social network" dai "social media" è proprio la circostanza che gli utenti dei primi sono mossi dal desiderio di interagire con "persone che già conoscono" (in tal senso, il *Bundeskartellamt*: «It can be assumed that there is a specific demand for social networks, which is fundamentally different from the demand for other social media. The key purpose of social networks is finding and networking with people the users already know, and to exchange on a daily basis experiences, opinions and contents among specific contacts which the users define based on identity», Provv. 6 febbraio 2019, B6-22/16, § 249; giudizio condiviso dalla CMA inglese nell'indagine *Online Platforms and digital advertising, Market Study, Final Report*, July 2020, p. 54, e dall'Indagine della Camera dei rappresentanti USA, U.S. House of Representatives, *op. cit.*, p. 91), sicché la qualifica di formazioni sociali si attaglia semmai alle comunità che si creano sui social e non a questi ultimi. Del resto, ciò trova conferma, quantomeno per FB, nelle stesse dichiarazioni del suo CEO che afferma pubblicamente di offrire «un'intera gamma di prodotti per la costruzione di gruppi e di comunità, che contribuiranno ad una società più informata, alla sicurezza delle nostre comunità» (Facebook CEO Mark Zuckerberg's keynote at F8 2017 Conference): il che, da un lato, conferma che FB si limita a svolgere un'attività di carattere spiccatamente commerciale, senza alcuna pretesa di creare un'*unica comunità* che persegua interessi comuni, e che dall'altro lato sono semmai gli utenti a creare comunità attraverso FB. Le tesi in esame sembrano in realtà farsi fuorviare dalla retorica con cui le stesse piattaforme fanno insistito riferimento alle *community*, trascurando tuttavia che oggigiorno nella regolazione di Internet agli originari modelli *community-based* si sono sostituiti quelli *platform-based* (G. De Gregorio, *op. cit.*).

[53]V. ad es. gli Standard della Community: sul punto sia consentito rinviare a O. Grandinetti, *Facebook v. CasaPound e Forza Nuova*, cit. Per una linea argomentativa del tutto sovrapponibile v. ora la *concurring opinion* di Justice Thomas, cit.

[54]In questo senso invece P. De Sena, M. Castellaneta, *La libertà di espressione e le norme internazionali ed europee prese sul serio: sempre su CasaPound c. Facebook*, in "SIDIBlog", 20 gennaio 2020; P. Zicchittu, *I movimenti "antisistema" nell'agorà digitale: alcune tendenze recenti*, in "Liber Amicorum per Pasquale Costanzo", Collana di studi di Consulta Online, 2020; C. Melzi d'Eril, G.E. Vigevani, *Facebook vs. Casapound: un social network è davvero un servizio pubblico?*, in "Il Sole 24Ore", 15 dicembre 2019. *Contra* O. Grandinetti, *Facebook v. CasaPound e Forza Nuova*, cit.; cui *adde* la *concurring opinion* di Justice Thomas, cit., il quale nota come «unlike newspapers, digital platforms hold themselves out as organizations that focus on distributing the speech of the broader public».

[55]Citato da E. Rossi, *op. cit.*, p. 125, nota 30. Del resto, anche gli AA. cui si ispirano le tesi esaminate nella nota 52 sot-

tolineano come, da un lato, dalla nozione di formazioni sociali *ex* art. 2 Cost. dovrebbero essere escluse quantomeno le "grandi imprese" (in relazione alle quali possono al più ipotizzarsi formazioni sociali costituite *al loro interno*, come nel caso di associazioni ricreative aziendali: E. Rossi, *op. cit.*, p. 150) e, dall'altro lato, la grande impresa (ove pure la si volesse qualificare come formazione sociale) rientri sempre nell'ambito di applicazione dell'art. 41 Cost. ogniqualvolta entri in rapporto con le libertà dei terzi (G. Lombardi, *op. cit.*, p. 131).

[56]L'espressione è utilizzata da M. Bassini, *Libertà di espressione e social network*, cit., il quale ricorda come da tale preliminare inquadramento dipenda il tipo di disciplina cui è legittimo assoggettare le piattaforme digitali.

[57]C. cost. 9 luglio 1970, n. 122.

[58]C. cost. 18 novembre 1970, n. 159 (conf. 18 maggio 1972, n. 93), in tema di responsabilità degli edicolanti nella esposizione di stampati ritenuti pornografici; sentenza peraltro aspramente criticata, tra gli altri, da E. Bettinelli, *Controllo sul contenuto delle pubblicazioni da parte dei rivenditori di giornali in relazione all'art. 725 c.p. e libertà di manifestazione del pensiero attraverso la stampa*, in "Giurisprudenza costituzionale", 1970, p. 2010 ss., e da P. Barile, *Libertà di manifestazione del pensiero*, in "Enciclopedia del diritto", vol. XXIV, 1974, p. 465 ss.

[59]C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, 1958, p. 29, nota 61; A. Pace, M. Manetti, *La libertà di manifestazione del proprio pensiero*, in "Commentario della Costituzione Branca", Zanichelli, 2006, p. 37, cui si rinvia anche per altre citazioni dottrinali.

[60]Si pensi anche all'art. 8 della l. 8 febbraio 1948, n. 47 che, nel caso in cui la rettifica abbia un contenuto che possa dar luogo a responsabilità penale, esenta dal pubblicarla il soggetto obbligato: ipotesi richiamata da P. Barile, *op. cit.* Per uno spunto in merito alla correlazione tra responsabilità e prevalenza nel bilanciamento v. anche M. Betzu, *Regolare Internet*, cit., p. 152.

[61]Su tutti questi temi v. A. Pace, M. Manetti, *op. cit.*, p. 542 ss. Come nota oltreoceano T. Wu, *op. cit.*, «When a newspaper or magazine includes some stories and rejects others ... it can also be described as an act of speech: the selection itself is an act of self-expression».

[62]P. Barile, *op. cit.*, p. 467 ss. (il quale cita anche F. Pierandrei, *Radio, televisione e Costituzione*, in "Raccolta di scritti in onore di A. C. Jemolo", vol. III, Giuffrè, 1963), con riferimento al limite esplicito del buon costume, ma proprio per questo *a fortiori* estensibile a tutti i tipi di limiti.

[63]Per gli USA si v. la sec. 230 del DCA, per l'UE gli artt. 12-15 della direttiva 2000/31/CE, cui dovrebbe aggiungersi l'introduzione della c.d. *Good Samaritan Clause*, ad opera dell'art. 6 del DSA.

[64]Nello stesso senso, R. Niro, *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolamentazione: note ricostruttive*, in "Osservatorio sulle fonti", 2021, n. 3.

[65]In questa ottica sembrano andare anche le osservazioni di M. Manetti, *Facebook, Trump e la fedeltà alla Costituzione*, in "Forum di Quaderni costituzionali", 2021, n. 1.

[66]Sulla distinzione tra "censura privata funzionale", cioè quella imposta alle piattaforme dallo Stato a seguito di un provvedimento giudiziale/amministrativo, e "censura privata sostanziale", in cui invece «il bilanciamento fra libertà di espressione ed altri beni giuridici viene delegato dallo Stato direttamente alle piattaforme digitali», v. M. Monti, *Privatizzazione della censura e Internet platforms: la libertà di espressione e i nuovi censori dell'agorà digitale*, in questa Rivista, 2019, n. 1, p. 39 ss.

[67]In questo senso v. M. Manetti, *Regolare Internet*, in "MediaLaws", 2020, n. 2, p. 48.

[68]V. la precedente nota 66.

[69]In tal senso, ad es., E. Bell, *The Unintentional Press*, in L.C. Bollinger, G.R. Stone (eds.), "The Free Speech Century", Oxford University Press, 2019, p. 235 ss., che propende per qualificare i social come veri e propri media.

[70]Come dichiarato dalla stessa Google alla BBC il 13 settembre 2017, per escludere il suo ruolo di *publisher*.

[71]Questo il famoso paragone di *Cubby Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

[72]Cfr. rispettivamente l'art. 16 della l. 5 agosto 1981, n. 416 e l'art. 4 del d.lgs. 24 aprile 2001, n. 170.

[73]Sulle *positive obligation* si v. ad es. CEDU, Grande Camera, sent. 7 giugno 2012, *Centro Europa 7 e Di Stefano c. Italia* (ric. n. 38433/09), § 156; nonché in dottrina R. Mastroianni, *Riforma del sistema radiotelevisivo italiano e diritto europeo*, Giappichelli, 2004; A. Lamberti, *Violazione del diritto alla libertà di comunicare informazioni e idee*, in A. Di Stasi (a cura di), "Cedu e ordinamento italiano", CEDAM, 2016. Per un analogo ordine di idee v. oltreoceano Z. Chafee, *Government and Mass Communications: a Report from the Commission on Freedom of the Press*, 1947: «If we think of the role of news and opinions as the flow of intellectual traffic Government can also try to widen the channels and keep traffic moving smoothly» (IX), citato da T. Wu, *Is filtering Censorship? The Second Free Speech Tradition*, cit.

[74]Sul punto si v. anche la *concurring opinion* di Justice Thomas, cit., peraltro in riferimento all'applicabilità della disciplina dei *common carrier*.

[75]V. ad es. la posizione assunta riguardo ai media da S. Fois, *Informazione: potere o libertà?*, in P. Barile, R. Zaccaria (a cura di), "Rapporto '93 sui problemi della radiotelevisione in Italia", Giappichelli, 1994, p. 401 ss.

[76]S. Fois, *op. cit.*, il quale però ritiene, coerentemente alla sua impostazione di fondo, che tali posizioni dominanti dovrebbero essere ridimensionate solo mediante le tradizionali misure a tutela della concorrenza.

[77]Sul punto della rilevanza del potere di mercato di FB con riferimento alla cancellazione di una pagina di un partito di estrema destra sul social, v. l'ord. 22 maggio 2019 del *Bundesverfassungericht*, citata da M. Bassini, *Libertà di espressione e social network*, cit.; nonché in modo molto puntuale, Commissione per la Cultura e l'Istruzione del Parlamento europeo, *Parere sull'atto sui servizi digitali e le questioni sollevate in materia di diritti fondamentali* (2020/2022(INI)), 20 luglio 2020, § 2.

[78]Su ciò insiste, ad es., S. Zuboff, *op. cit.*

[79]Sui media tradizionali quali intermediari del XX secolo, v. T. Wu, *Is filtering Censorship? The Second Free Speech Tradition*, cit., ancorché per giungere a conclusioni in parte diverse da quelle del testo, trattandosi del resto di uno scritto del 2010.

[80]V. per tutti J.M. Balkin, *Free speech is a triangle*, in "Columbia Law Review", vol. 118, 2018, n. 7, p. 2011 ss.

[81]Nello stesso senso sembrerebbe orientarsi R. Borrello, *Arte e rete digitale: i Social Networks e le policies sulla nudità*, in "Nomos", 2020, n. 3, lavoro contenente anche altre acute osservazioni sui temi qui affrontati.

[82]Sul punto, nella sua *concurring opinion* Justice Thomas osserva ironicamente come «A person always could choose to avoid toll bridge or train and instead swim the Charles River or hike the Oregon trail».

[83]Il criterio è stato già adottato dalla legge francese n. 2018-1202, pubblicata a dicembre 2018, e da quella tedesca, la c.d. *Netzwerkdurchsetzungsgesetz*, approvata nel giugno 2017; per la più ampia applicazione di questo criterio, O. Grandinetti, *Facebook v. CasaPound e Forza Nuova*, cit., p. 190.

[84]Si pensi ad es. a Twitter che, pur avendo un fatturato relativamente contenuto rispetto a FB ed un numero di utenti

di molto inferiore a livello globale, potrebbe assumere importanza a fini informativi per numero elevato di utenti in un determinato Paese; viceversa il motore di ricerca Bing, pur facendo capo ad una *big tech* come Microsoft, non sembra idoneo ad incidere significativamente sull'informazione a causa della sua bassa quota di mercato.

[85] A cui potrebbe aggiungersi almeno il Regolamento (UE) 2019/1150, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.

[86] Come del resto quelle della direttiva 2000/31/CE sul commercio elettronico: v. la *Relazione di accompagnamento al DMA*, p. 3.

[87] Cioè, in base all'art. 3 del DMA, i fornitori di servizi di piattaforma di base (ossia: servizi di intermediazione online; motori di ricerca; social network; piattaforme per la condivisione di video; servizi di comunicazione interpersonale indipendenti dal numero; sistemi operativi; servizi di cloud; servizi di pubblicità erogati da uno dei precedenti operatori) che: hanno un impatto significativo sul mercato interno; gestiscono un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; detengono una posizione consolidata e duratura o è prevedibile che l'acquisiscano, in base ad ulteriori criteri dettagliati nello stesso art. 3.

[88] Secondo le definizioni della direttiva sul commercio elettronico.

[89] Cioè, in base all'art. 2 del DSA: i prestatori di servizi intermediari di hosting che, su richiesta di un destinatario del servizio, memorizzano e diffondono al pubblico informazioni, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio.

[90] Cfr. la *Relazione al DSA*, p. 2.

[91] *Ivi*, pp. 7 e 13.

[92] *Ivi*, p. 4; per un elenco v. cons. 12.

[93] Rischio certamente non scongiurato dal vago richiamo all'obbligo di "tenere conto" in tali attività dei diritti fondamentali sanciti dalla Carta: art. 12 DSA.

[94] Tra cui rientra anche la gran parte dei casi di disinformazione.

[95] *Relazione DSA*, p. 10.

[96] *Proposta di regolamento del Parlamento europeo e del Consiglio, relativo alla trasparenza e al targeting della pubblicità politica* del 25 novembre 2021.

[97] *Ivi*, cons. 13.

[98] In tal senso M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, cit. (che svolge anche altre osservazioni condivisibili) e G. De Minico, *Fundamental Rights, European digital regulation and algorithmic challenge*, in "MediaLaws", 2021, n. 1.

[99] Cfr. artt. 2, lett. n), e p. 15 DSA.

[100] O. Grandinetti, *La par condicio al tempo dei social, tra problemi "vecchi" e "nuovi", ma per ora tutti attuali*, in "MediaLaws", 2021, n. 1.

[101] Alla quale qui, per ragioni di spazio, si sono fatti solo alcuni fugaci riferimenti.

[102] Per indicazioni sulla distinzione tra *unmittelbare* e *mittelbare Drittwirkung*, M. Giorgianni, *La Corte di giustizia e l'efficacia diretta della Carta dei diritti fondamentali nell'Unione Europea nei rapporti fra privati*, in "Le nuove leggi civili commentate", speciale 2016, p. 194 ss.

[103] Su cui dal punto di vista costituzionale v. M. Esposito, *op. cit.*

[104] Art. 41.3, lett. b), DSA.

* * *

Digital Platforms as "Private Powers" and Online Censorship

Abstract: American and European scholars are increasingly defining the digital platforms owned by Big Tech as "private powers" and, as far as freedom of expression and information is concerned, as "private censors". The essay, after recalling the most recent antitrust theories on online platforms in the US and Europe, focuses on the constitutional consequences of this qualification (private power) on the discipline of online censorship, reaching the conclusion that, according to Italian and European constitutional law (at least in continental Europe), while platform users exercise their freedom of expression and information, digital platforms only exercise their freedom of enterprise. As a consequence, digital platforms may be subject to even more penetrating limits to protect freedom of expression and information than traditional media, which still exercise their freedom of information. According to Article 10 ECHR and the caselaw thereof, the State has a "positive obligation" to protect the freedom of expression and information. In the light of those general findings, the essay critically analyzes the proposals of EU Regulations about, respectively, digital services and markets (Digital Services Act and Digital Markets Act).

Keywords: Digital platforms – Private power – Online censorship – Internet – Standard of Community

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0070
Articolo sottoposto a peer review

Le pubbliche amministrazioni nell'era delle tecnologie cloud ed *edge computing* tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali

Elena Montagnani

Le smart city e l'Industria 5.0 costituiscono elementi fondamentali nella strategia europea per la transizione verso un modello economico circolare. L'insieme di nuove tecnologie indispensabili al loro funzionamento, come *Internet of Things*, Intelligenza artificiale, *edge computing*, costringe ad un'attenta riflessione sullo stato dell'arte delle infrastrutture digitali dispiegate sul territorio nazionale in relazione alle missioni del PNRR, alla base della strategia digitale del paese. In tale contesto è proprio la pubblica amministrazione a rivestire un ruolo di raccordo tra i vari stakeholder (imprese, cittadini, terzo settore). Scopo del lavoro è dunque quello di verificare le criticità legate all'introduzione di tali nuove tecnologie e le possibili similitudini in termini di governance con i temi dell'implementazione e regolamentazione afferenti al cloud computing, al fine di avviare una serie di riflessioni sull'incidenza che la transizione verso una società integrata e digitale ha sulla sovranità digitale e sul trattamento del dato.

Sovranità digitale – *Internet of Things* – *Cloud* ed *edge computing* – Smart city – Economia circolare

Sommario: *1. Introduzione – 2. Affacciati sul futuro: smart city, Industria 5.0, economia circolare – 3. Tecnologie abilitanti: tra innovazione e sperimentazione – 4. Il concetto di sicurezza alla prova della nuova società digitale – 5. Stato dell'arte e prospettive future dell'*edge computing *nel processo di trasformazione digitale dell'Italia – 6. Conclusioni*

È inutile stabilire se Zenobia sia da classificare tra le città felici o tra quelle infelici.
Non è in queste due specie che ha senso dividere le città, ma in altre due:
quelle che continuano attraverso gli anni e le mutazioni a dare la loro forma ai desideri
e quelle in cui i desideri o riescono a cancellare la città o ne sono cancellati.
Italo Calvino

1. Introduzione

L'emergenza pandemica ha messo in evidenza come le infrastrutture digitali siano fondamentali e strategiche per il nostro Paese, accelerando quel processo di trasformazione digitale della società iniziato da anni ed ormai irreversibile. Al pari delle infrastrutture tradizionali, quelle digitali costituiscono mezzi essenziali per permettere nuove modalità di erogazione e fruizione dei servizi pubblici, di studio, di lavoro, nonché occasione di sviluppo per l'economia digitale (e non solo) del paese[1].

E. Montagnani è dottoranda di ricerca in Scienze giuridiche presso l'Università di Pisa.
Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

In tale contesto socio-economico caratterizzato da un irreversibile processo di trasformazione digitale, ormai avviato da diversi anni, tale da non potersi considerare una novità dell'ultima ora imposta dalla pandemia, è divenuta dunque, improcrastinabile un'analoga trasformazione digitale delle pubbliche amministrazioni.

Obbiettivo prioritario è quello di offrire ai cittadini e alle imprese servizi pubblici di maggiore qualità, responsività, efficacia ed efficienza al quale si affianca l'esigenza di rendere le aree urbane sempre più "smart" e sostenibili da un punto di vista ambientale attraverso l'*Internet of things* (c.d. IoT), l'utilizzo di sistemi di Intelligenza artificiale (c.d. A.I.) e *machine learning* (c.d. M.L.) e le loro tecnologie abilitanti quali 5G, cloud computing ed *edge computing*, al fine di permettere l'innovazione in quei settori oggi affidati a metodologie tradizionali (si pensi al settore della mobilità con le auto a guida autonoma; a quello ambientale con il monitoraggio tramite droni del territorio e delle emissioni di Co2, ma anche alla raccolta dei rifiuti robotizzata e al benessere dei cittadini, alla valorizzazione dei beni culturali e del settore turismo)[2].

È proprio intorno al tema delle smart city, come vedremo, che oggi si concentrano maggiormente i contributi innovativi e gli investimenti privati[3] e pubblici, come mostrano anche le sperimentazioni messe in atto dal programma "Smarter Italy"[4] promosso da MISE, MIUR e MITD, in ambiti come mobilità, ambiente, benessere della persona e beni culturali.

Tuttavia, i servizi legati alle smart city e all'IoT impongono delle scelte tecnologiche che sembrano oggi, se non in contrasto, quantomeno dimenticate dalla direzione generale delineata dal Piano Nazionale di Ripresa e Resilienza (PNRR), dal Piano Triennale per l'informatica nella pubblica amministrazione 2021-2023 e dalla Strategia Italia digitale 2026, i quali riservano un ruolo da protagonista nella trasformazione digitale della P.A. al cloud computing sulla base del paradigma *cloud first*, prevedendo una progressiva dismissione del patrimonio tecnologico delle pubbliche amministrazioni centrali e periferiche dislocato capillarmente sul territorio, in favore di una migrazione proprio verso il cloud.

Infatti, la natura "real-time" di alcuni dei servizi legati alle smart city implica la necessità di eseguire la computazione del dato proveniente dai dispositivi elettronici (*things*) attraverso sistemi allocati in prossimità di questi e quindi *data center* dislocati sul territorio in modo capillare. Questa tipologia di infrastrutture, denominata *edge computing*, non rappresenta ancora una realtà consolidata nel nostro territorio sebbene alcuni *cloud provider* (Google, Microsoft, Amazon) e alcune TELCO (TIM, Fastweb) abbiano avviato nelle principali città italiane ed europee delle sperimentazioni.

È possibile, quindi, pensare di valorizzare il patrimonio tecnologico ed infrastrutturale in dismissione delle pubbliche amministrazioni trasformandolo in una infrastruttura nazionale di *edge computing* che, affiancata alla nuova connettività 5G, vada a costituire un asset strategico fondamentale per la realizzazione proprio di quei servizi smart delle pubbliche amministrazioni sui quali verranno ridisegnate le città e le società del prossimo futuro? Quali sono i rischi per la sovranità digitale legati all'assenza di una infrastruttura *edge* nazionale a favore di infrastrutture gestite dai grandi attori del Web? Quali sono le nuove sfide che tali infrastrutture portano con sé in termini di trattamento del dato?

2. Affacciati sul futuro: smart city, Industria 5.0, economia circolare

L'avvento della digitalizzazione e di una società sempre più liquida e globale, caratterizzata da una capillare diffusione di smartphone e tablet e da una progressiva stabilità e disponibilità della connessione ad Internet, ha imposto nuove modalità di fruizione dei servizi informatici e contestualmente ha prodotto un aumento esponenziale della produzione dei dati da parte degli utenti e della loro circolazione.

È proprio intorno alla disponibilità di un'enorme mole di dati e delle tecnologie in grado di valorizzarli che si stanno progressivamente forgiando nuovi modelli sociali ed economici: si pensi in particolare alle città intelligenti (c.d. smart city), all'Industria 4.0 e 5.0, ai nuovi paradigmi di sviluppo in grado di armonizzare gli obiettivi dell'economia di mercato e quelli ambientali (c.d. *circular economy*).

La città diventa quindi una piattaforma integrata di sistemi ICT, una rete intelligente di oggetti e macchine connessi, che trasmettono dati usando la tecnologia wireless ed il cloud[5].

Si tratta in realtà di qualcosa di molto più ampio, un nuovo modo di concepire il modo di vivere negli agglomerati urbani, dove il capitale infrastrutturale legato anche alle nuove tecnologie (che potremmo definire capitale fisico-digitale), il capitale umano, intellettuale, ambientale e sociale vengono massimizzati[6]. L'eterogeneità degli ambiti abbracciati dalle smart city pare anche essere confermata dall'approccio seguito dall'Unione europea[7], la quale ne declina le specificità secondo sei dimensioni (*smart people*, *smart governance*, *smart economy*, *smart living*, *smart mobility*, *smart environment*) confermando co-

me quello tecnologico sia solo uno dei tanti aspetti che governeranno le future città intelligenti.

Se fino ad oggi il cittadino è stato considerato mero fruitore di servizi, digitali e non, il nuovo paradigma, incentrato sul concetto di *smart people*, impone un modello di *smart citizenship* in cui esso diviene soggetto attivo anche nell'erogazione e non solo nella fruizione del servizio, fornendo dati, decisioni e feedback, nello sviluppo della città e nelle decisioni dell'amministrazione locale secondo una logica *bottom-up*.

Per poter parlare di *smart citizenship* è però necessario fornire al cittadino gli strumenti indispensabili, quali infrastrutture di rete (banda ultra-larga, 5G, Wi-fi), sistemi di identità digitale, piattaforme di accesso ai dati. Le informazioni ed i dati prodotti dai sensori dovranno, infatti, essere resi disponibili agli utenti-cittadini attraverso servizi che consentano loro di vivere la città in *real time* ed assumere decisioni consapevoli, fornendo a loro volta nuovi dati necessari alla smart city per alimentare i sistemi di intelligenza artificiale (A.I.) in un ciclo continuo.

Se già da anni nei grandi agglomerati urbani si è rilevata, ad opera di soggetti pubblici e privati, la tendenza ad introdurre intelligenza nella gestione dei servizi fondamentali al cittadino[8], più di recente abbiamo assistito, in risposta all'emergenza sanitaria, all'introduzione di pratiche quali smart working, didattica a distanza e fruizione digitale di servizi delle pubbliche amministrazioni[9].

Non solo, è interessante anche notare come in un territorio come quello italiano, caratterizzato dalla presenza di pochi grandi agglomerati urbani e di numerosi piccoli comuni e borghi, siano state avviate sia ad iniziativa pubblica che privata, una serie di sperimentazioni volte a replicare il modello della smart city all'interno di comunità di piccole dimensioni e diffuse capillarmente sul territorio, le quali presentano esigenze molto diverse da quelle di una grande città[10].

Proprio osservando gli obiettivi delle sperimentazioni più recenti risulta evidente un netto cambio di paradigma nel percorso di trasformazione delle comunità in chiave digitale. Se in un primo momento, infatti, risultava preponderante l'aspetto tecnologico finalizzato ad un miglioramento dei parametri economici per gli operatori del settore, oggi viene privilegiato un approccio antropocentrico, adottato anche dall'Ue, attento ai bisogni e al miglioramento della qualità della vita del cittadino.

La progettazione di smart city del futuro avrà bisogno, quindi, di un continuo adattamento, dove le nuove tecnologie costituiranno leve strategiche nell'adozione di pratiche sostenibili dal punto di vista economico, energetico, ambientale e sociale, il che implicherà una gestione cooperativa e inclusiva della società e del territorio per migliorare la qualità, le prestazioni e l'interattività dei servizi; ridurre i costi e il consumo di risorse; ottimizzare la relazione tra i cittadini e gli operatori della città.

La governance delle smart city deve essere, quindi, finalizzata a valorizzare l'interoperabilità tra i sistemi, creando una singola infrastruttura di base e un'unica piattaforma di delivery dei servizi in grado di elaborare le informazioni trasmesse dai sensori per erogare servizi a valore aggiunto per i cittadini.

Tale modello di sviluppo delle comunità in chiave digitale ed integrata acquisisce ancora più importanza se pensiamo al problema del rapporto tra ambiente e sviluppo, che sta alla base della questione ambientale e della grave crisi ecologica ed alla necessità sempre più impellente di superare il modello capitalistico e di mercato caratterizzato da un eccessivo sfruttamento delle risorse naturali e dal forte impatto delle attività antropiche sull'intero ecosistema, secondo la logica lineare "estrai, produci, usa, getta" (c.d. "paradigma meccanicistico" del mondo come macchina).

Se in un primo momento nel contesto delle Nazioni Unite si è trovata una risposta nei concetti di sviluppo sostenibile e di green economy, più di recente si è approdati a livello internazionale al concetto di *circular economy*[11], il quale garantirebbe un vero cambio di paradigma dell'economia tradizionale in chiave circolare, coessenziale alla nuova concezione del mondo come "rete" (c.d. "paradigma economico-sistemico")[12].

Sia il "Nuovo piano d'azione per l'economia circolare" dell'Ue del marzo 2020[13] sia la "Strategia nazionale per l'economia circolare" del settembre 2021[14], hanno tuttavia messo in evidenza come la transizione all'economia circolare sia fortemente dipendente dall'introduzione di nuove tecnologie e servizi digitali, quali sensori di monitoraggio, servizi IoT ed A.I., necessari a governare la maggior complessità ed interdipendenza delle filiere di approvvigionamento e dei processi produttivi legati a tale modello economico.

Al di là dell'evidente affinità tecnologica tra le tematiche legate alle smart city ed all'economia circolare è da rilevare come queste siano lo strumento fondamentale attraverso il quale il cittadino diviene parte attiva nei processi produttivi circolari e mediante il quale tali processi generano conoscenza (sensori ed IoT) ed impatto sulla comunità (A.I.)[15].

Il modello di smart city dovrà, quindi, andare di pari passo con gli obiettivi di efficienza energetica e di sostenibilità ambientale. Obiettivi che sono chiara-

mente espressi nell'Agenda 2030 delle Nazioni Unite e nel *Green Deal* europeo[16].

Proprio in relazione ai processi produttivi la Commissione europea ha recentemente gettato le basi di un'Industria 5.0[17] che, espandendo il concetto di Industria 4.0[18], incorpora i principi e le tecnologie presenti all'interno delle smart city, introducendo al contempo i concetti di sostenibilità ed equità sociale. Il paradigma dell'Industria 5.0 mira a migliorare l'efficienza delle fabbriche intelligenti (c.d. *smart factory*) ed al contempo a minimizzare l'impatto sull'ambiente e le ricadute sulla società[19].

Per implementare la visione di un'economia circolare basata sulla trasformazione digitale, sulla smart city e sull'Industria 5.0 risulta necessario fornire soluzioni in grado di integrare il mondo fisico e quello virtuale in modo efficiente e sostenibile.

3. Tecnologie abilitanti: tra innovazione e sperimentazione

Sebbene il panorama tecnologico, in continua evoluzione, offra un numero sempre crescente di soluzioni, strumenti, servizi ed infrastrutture, sono riconducibili a quattro gli abilitatori tecnologici fondamentali per una transizione digitale che privilegi la sostenibilità ed equità sociale: IoT, 5G, Intelligenza artificiale, *cloud* ed *edge computing*.

I dispositivi IoT[20] sono ad oggi impiegati in molteplici settori come ad esempio il monitoraggio remoto, l'automazione casalinga ed industriale (c.d. IIoT), l'agricoltura di precisione.

Cifra distintiva dell'IoT è evidentemente la capacità di interconnessione necessaria per trasmettere in tempo reale i dati raccolti da un lato e le decisioni da attuare dall'altro. Particolare importanza riveste quindi l'infrastruttura di rete che garantisce tale connettività. Fino ad oggi le reti geografiche a basso consumo energetico necessarie all'interconnessione dei dispositivi hanno mostrato numerose lacune e criticità, superate con l'introduzione delle nuove reti 5G attualmente in dispiegamento in Italia, che risultano un fattore determinante per garantire il percorso di digitalizzazione delle comunità e dell'industria, necessario ad avviare un processo di trasformazione dell'economia in chiave circolare. Non è un caso che vi siano numerose sperimentazioni a livello europeo e nazionale in ambito IoT che vanno progredendo di pari passo con lo stato di avanzamento dei lavori sull'infrastruttura di rete di nuova generazione[21].

Come le reti di nuova generazione ed i dispositivi IoT possono essere paragonati al sistema nervoso centrale ed all'apparato sensoriale mediante cui un organismo biologico conosce e riconosce l'ambiente che lo circonda, l'apparato neurale tramite il quale le informazioni acquisite vengono tradotte in soluzioni ed azioni da tale organismo può essere rappresentato dai sistemi di *machine learning* ed A.I.

Tale intelligenza, definita oggi dal Programma strategico Intelligenza Artificiale 2022-2024 come "l'insieme dei modelli digitali, algoritmi e tecnologie che riproducono la percezione, il ragionamento, l'interazione e l'apprendimento"[22], consente di creare sistemi di raccomandazione, soluzioni di riconoscimento del linguaggio naturale, veicoli a guida autonoma che sono in grado di prendere decisioni in tempo reale senza bisogno dell'intervento umano.

Nel caso dei sistemi IoT, i sistemi di *machine learning* ricevono costantemente dati dai sensori della rete grazie ai quali riescono ad allenare e perfezionare le A.I. in un ciclo di apprendimento continuo[23]. I sistemi di intelligenza artificiale possono, quindi, processare tali dati ed elaborare un risultato che viene comunicato ad un utente o agli attuatori della rete IoT sotto forma di decisione.

Se pensiamo ai servizi digitali che alimenteranno le città e le industrie del prossimo futuro, come le auto a guida autonoma, il monitoraggio ambientale tramite droni, la gestione della mobilità, i sistemi di logistica etc., risulta evidente come sia di fondamentale importanza che il tempo intercorso tra il rilevamento di un parametro ambientale (per esempio la presenza di un pedone sulla carreggiata), l'elaborazione di una decisione da parte di un sistema di A.I., e l'applicazione di tale decisione (l'attivazione dei sistemi di arresto dell'auto) sia il minore possibile.

Tuttavia, molti dei sistemi IoT che operano in tempo reale non riuscirebbero a garantire tale requisito attraverso architetture centralizzate basate su cloud, dal momento che i valori elevati di latenza (il tempo che intercorre tra una richiesta inoltrata ad un servizio e la relativa risposta) impediscono al sistema di fornire la reattività necessaria.

In tali casi l'uso di infrastrutture di computazione dispiegate in prossimità dei sensori (c.d. *edge computing*) può fornire un'adeguata soluzione al problema evitando potenziali "colli di bottiglia" e ritardi nella comunicazione tra dispositivi e sistemi di A.I.

Le soluzioni centralizzate basate sul cloud pongono, però, determinate limitazioni che non si esauriscono nei già citati requisiti di latenza. È prima di tutto necessario notare come il cloud stesso sia da considerarsi un singolo punto di vulnerabilità per la disponibilità del servizio (quello che in gergo tecnico viene definito *single point of failure*)[24] dal momento che attacchi informatici, vulnerabilità o anche semplici operazioni di manutenzione programmata possono interrompere l'erogazione del servizio. Inoltre,

si prevede che il numero di dispositivi IoT connessi alla rete aumenterà sensibilmente nei prossimi anni[25] e, di conseguenza, il numero di comunicazioni simultanee con i sistemi centralizzati potrebbe, in assenza di una progettazione adeguata, sovraccaricare il cloud[26].

L'*edge computing* si presenta anche in questo caso come uno strumento complementare al cloud computing in grado di alleggerire i sistemi centralizzati eseguendo le computazioni su una infrastruttura locale, dedicata ad un numero limitato di dispositivi IoT presenti su un territorio circoscritto e fornendo al contempo una sorta di camera a tenuta stagna (c.d. *bulkhead*) capace di limitare la propagazione all'intero sistema degli effetti di eventi disastrosi (si pensi ad esempio ad un attacco informatico che blocchi un sistema regionale il quale, su una infrastruttura centralizzata, verrebbe ad estendersi anche ai sistemi delle altre regioni).

Se è chiaro che il cloud computing continuerà a crescere fino a diventare lo standard definitivo delle architetture ICT, l'*edge computing* sarà la nuova area in cui i *cloud provider*, le Telco e i fornitori di servizi concentreranno i loro investimenti per l'innovazione nel prossimo futuro[27].

La vera sfida sarà piuttosto quella di integrare le nuove infrastrutture e le tecnologie abilitanti con le strutture esistenti sul territorio sfruttando l'interoperabilità tra sistemi.

4. Il concetto di sicurezza alla prova della nuova società digitale

Carlo Ratti, architetto ed ingegnere, fondatore e direttore di SENSEable City Lab del MIT di Boston, che studia lo sviluppo dei sensori dell'elettronica in relazione all'ambiente urbano, ha affermato che «l'impiego crescente di sistemi e sensori elettronici sta permettendo un nuovo approccio allo studio dell'ambiente costruito. Il nostro modo di descrivere e comprendere le città viene radicalmente trasformato, insieme agli strumenti che usiamo per crearle e all'impatto sulla struttura fisica. La dimensione digitale delle città esiste da tempo. L'importante è capire come usare i dati, come analizzarli ed elaborarli per rendere i contesti urbani più vivibili, più sicuri e più efficienti»[28].

Ecco che la vita della smart city, come agglomerati urbani più vivibili, sicuri ed efficienti, è strettamente dipendente dall'utilizzo di soluzioni e tecnologie IoT, che permettono il rilevamento, l'analisi e il trasferimento di grandi flussi di dati.

Tutto ciò ha evidenziato la necessità di dare rilevanza alla sicurezza nelle sue varie declinazioni (*security*, *safety*, *certainty*, *privacy*) a seconda dell'ottica in cui viene osservata[29], alle quali oggi si aggiunge un quinto tipo di sicurezza, quella cyber, che si propone come macro settore sotto al quale porre tutti gli altri[30].

Un primo aspetto chiave che va preso seriamente in considerazione è, quindi, quello della cybersicurezza urbana ovvero del rapporto con le tecnologie dell'informazione e della comunicazione, radicato nell'essenza stessa della città, al fine di rendere resiliente l'insieme delle infrastrutture sulle quali tutta la smart city è fondata. Il rischio è quello di essere esposti ad attacchi o minacce cyber da parte di criminali informatici in settori sensibili quali quello sanitario, dei trasporti, della distribuzione e più in generale di tutti quei servizi essenziali per il funzionamento di una città.

La cyber security diventa un aspetto essenziale per qualsiasi iniziativa digitale applicata alle città intelligenti, un bisogno la cui soddisfazione diviene primaria per l'uomo, andando ad assumere un ruolo importante anche per la protezione della privacy dei cittadini da un lato, e per la protezione delle aree sensibili della città dall'altro. E questo è tanto più vero oggi a fronte dell'incremento esponenziale sia della digitalizzazione dei servizi offerti dalle P.A., sia degli attacchi informatici, decuplicati nell'arco di un anno[31]. Siamo di fronte a problematiche che per natura, gravità e dimensione hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica[32], in grado di mettere in crisi la stabilità del sistema andando a colpire i dati delle strutture organizzative più sensibili[33].

Affinché il cittadino mantenga un alto grado di "fiducia computazionale" nelle istituzioni che governano questo modello di città, e conseguentemente nel modello stesso di smart city, queste saranno chiamate a garantire anche un livello adeguato di sicurezza della sua privacy sia da parte di soggetti pubblici che privati[34]. È proprio questo aspetto di *multistakeholderism* che vede coinvolti soggetti di natura eterogenea che richiederà una particolare attenzione nell'elaborazione di protocolli di sicurezza e policy relative al trattamento dei dati.

Anche il PNRR ha dedicato attenzione alla cybersicurezza, destinando 620 milioni di euro a tale settore, a fronte, come vedremo, dello sviluppo di un ampio piano di digitalizzazione delle P.A.[35]

Il cloud computing, in quanto infrastruttura centralizzata gestita nella maggior parte dei casi da soggetti privati, potrebbe presentare più di una criticità rispetto al tema della sicurezza in tutte le sue accezioni. Ecco che le infrastrutture di *edge computing*

potrebbero costituire una valida risposta non solo a criticità di tipo tecnico, come sopra messo in evidenza, ma anche garantire un elevato grado di resilienza del sistema smart city alle violazioni dei protocolli di sicurezza o delle policy relative alla gestione del dato, attraverso la creazione di infrastrutture locali autonome e segregate.

Non bisogna dimenticare, inoltre, che l'ambito IoT, fondamentale per la trasformazione digitale delle città, presenta numerose peculiarità sia da un punto di vista tecnico che del trattamento del dato, le quali lo distinguono fortemente dall'ambito dei servizi digitali che hanno come fruitore il cittadino ed il consumatore (si pensi ai portali informativi delle P.A., alle piattaforme di prenotazione dei vaccini etc.).

Nei servizi digitali che prevedono una interazione diretta con il cittadino o il consumatore la tutela della privacy viene garantita da un lato attraverso l'applicazione del principio di minimizzazione dei dati espresso dall'art. 5 c.1 lett. c) nel combinato disposto con l'art. 6 del regolamento europeo 679/2016, e dall'altro dalla possibilità di avere un contatto diretto con l'utente al quale viene data la facoltà di esprimere il proprio consenso al trattamento dei dati secondo le consuete formule di *opt-in* e *opt-out*.

Di contro i sistemi di IoT trattano dati che sono spesso semanticamente molto distanti da quelli trattati dai servizi appena descritti (ad esempio, rilevazioni di dati ambientali, immagini, video, posizioni) dove la raccolta del dato personale nella maggior parte dei casi avviene in modo incidentale (ad esempio, un drone di rilevamento del traffico che registra immagini nelle quali compaiono i volti degli individui intenti a fare shopping)[36].

Inoltre, se escludiamo i dispositivi personali o indossabili (ad esempio, smart watch o smart phone) i dispositivi IoT spesso operano nell'impossibilità di interfacciarsi direttamente con un utente i cui dati vengano incidentalmente rilevati, al fine di richiedere il consenso al loro trattamento o conservazione, aprendo sicuramente la strada ad un articolato dibattito intorno alla gestione ed al trattamento del dato personale in tale contesto[37].

Nell'attesa che vengano delineate delle policy in grado di superare tali problematiche le infrastrutture *edge* possono fornire un supporto essenziale nella loro mitigazione.

In primo luogo, vi sono numerosi casi d'uso in ambito IoT in cui i sistemi sono interessati unicamente al processamento dei dati e non alla loro conservazione. In tali casi il processamento dei dati su infrastrutture *edge*, vicine ai dispositivi IoT, consente di evitare la conservazione del dato funzionale ad un successivo processamento. In sostanza, una volta che un dato viene catturato da un sensore ed una applicazione di A.I. lo ha utilizzato per prendere una decisione, tale dato diviene immediatamente superfluo e potrà essere cancellato[38].

In secondo luogo, anche nei casi in cui i sistemi centrali cloud avessero necessità di ricevere le rilevazioni contenenti dati personali al fine di conservarli, tali dati potrebbero essere anonimizzati o pseudonimizzati direttamente sui sistemi periferici *edge*, senza quindi essere mai scritti su alcun supporto informatico. Di conseguenza ogni successivo accesso a tali rilevazioni, sia che avvenga sui sistemi *edge* che sui sistemi cloud, sia che avvenga ad opera di un automa che di un essere umano, non comporterà l'esposizione di dati personali, ottenendo così una tutela della *privacy by design* e consentendo al contempo di minimizzare gli effetti di eventuali *data breach*[39].

Questo è ancora più importante se messo in relazione al fatto che l'ambito IoT, come abbiamo visto, rende particolarmente complessa se non quasi impossibile la richiesta del consenso ai soggetti i cui dati verranno trattati, il che rende di fatto l'*edge* una infrastruttura strategica nella pianificazione della transizione verso le nuove comunità digitali, l'Industria 5.0 e il modello economico circolare.

L'importanza di questo tipo di infrastruttura e della sua distribuzione capillare sul territorio è ben evidenziata anche dalla "*Roadmap* della tecnologia industriale europea per l'offerta *cloud-edge* di nuova generazione", in cui si evidenzia non solo la necessità di una sinergia tra cloud ed *edge* ma anche di un intervento delle istituzioni europee e nazionali nella loro realizzazione al fine di garantire un adeguato livello di sovranità sul dato e sulle infrastrutture[40].

5. Stato dell'arte e prospettive future dell'*edge computing* nel processo di trasformazione digitale dell'Italia

È proprio nel solco della strada tracciata dall'Europa per avviare una transizione verso una società smart e green sorretta da un'economia di tipo circolare, dove la trasformazione digitale delle comunità e dell'industria è orientata ad una maggiore sostenibilità, che sembra muoversi il PNRR[41] sviluppato dall'Italia. Sebbene il tema della transizione al digitale sia trasversale a tutte le missioni nelle quali il piano si articola, è nella prima missione "Digitalizzazione, innovazione, competitività, cultura e turismo" che si concentrano gli investimenti per l'ammodernamento non solo delle P.A. ma anche del sistema produttivo e del turismo, vero motore economico del paese[42].

Con riferimento alle infrastrutture di connettività, il PNRR include ingenti investimenti volti a garantire la copertura di tutto il territorio con reti a banda ultra-larga (fibra FTTH, FWA e 5G)[43] per consentire alle P.A., alle imprese e ai cittadini di catturare i benefici della transizione digitale, ponendosi in linea con la strategia europea per la creazione di un mercato unico europeo del dato.

Per quanto riguarda le infrastrutture computazionali il PNRR adotta un approccio *cloud first*, con lo scopo non solo di migrare i dati e gli applicativi informatici esistenti delle singole amministrazioni verso un ambiente cloud, ma anche di stabilire un nuovo paradigma per la governance dei dati e lo sviluppo dei futuri servizi delle P.A.

Questo processo si pone quale obiettivo la razionalizzazione e il consolidamento di molti dei *data center* delle P.A. oggi distribuiti sul territorio, attraverso una dismissione progressiva del patrimonio ICT secondo una classificazione stilata da AgID che tiene conto dell'obsolescenza e del livello di sicurezza delle tecnologie impiegate, a favore delle infrastrutture cloud.

Si prevede altresì che la migrazione venga attuata secondo due modelli complementari, l'uno che prevede la creazione di un Polo Strategico Nazionale (PSN) costituito da una nuova infrastruttura cloud dedicata (completamente privata o ibrida) localizzata sul territorio nazionale in linea con gli standard di prestazione e sicurezza tipici dei cloud pubblici; l'altro che prevede l'uso di un cloud pubblico di uno tra gli operatori di mercato certificati da AgID.

La scelta di quali servizi migrare verso soluzioni cloud qualificate da AgID o verso il PSN avverrà sulla base della classificazione dei dati definita all'interno della Strategia Cloud Italia[44].

In particolare, i dati e servizi categorizzati come strategici ovvero la cui compromissione può avere un impatto sulla sicurezza nazionale dovranno necessariamente migrare[45] sull'infrastruttura cloud fornita dal PSN, con l'obiettivo di garantire la massima resilienza ed autonomia tecnologica e controllo sui dati per quei servizi ritenuti essenziali al funzionamento del paese.

Sia il PNRR sia le strategie ed i piani nazionali ad esso collegati pongono particolare enfasi sul principio *cloud first*, favorendo la creazione di poli centralizzati per il processamento e la conservazione dei dati, nulla predisponendo tuttavia con riferimento all'adozione di sistemi di *edge computing* e all'implementazione di piattaforme IoT.

La Strategia Cloud Italia, basandosi sulla situazione del patrimonio ICT delle P.A. fotografata da AgID[46], è orientata nel medio-lungo termine alla completa dismissione della maggior parte dei *data center* locali ad eccezione di poche infrastrutture che si sono dimostrate adeguate in termini di performance e sicurezza e che andranno in parte a costituire l'infrastruttura del PSN[47].

È quindi evidente come la maggior parte delle infrastrutture computazionali oggi presenti capillarmente sul territorio sia destinata a scomparire, per lasciare il posto ad un PSN dispiegato su due regioni, che costituirà una infrastruttura cloud non adatta ai casi d'uso relativi alle infrastrutture di *edge computing*.

È da notare come ad oggi non esista un piano di finanziamenti volto ad adeguare tali strutture in dismissione ai requisiti richiesti dai sistemi IoT e conseguentemente dalle infrastrutture *edge*, ma è previsto solo il finanziamento delle attività volte a garantire la continuità del servizio durante il periodo di migrazione o le attività di consolidamento di alcuni *data center* centrali.

Tuttavia l'assenza di una strategia per le infrastrutture *edge* ed IoT rischia di porre il Paese in una situazione di forte ritardo rispetto alla transizione verso il nuovo modello di società che va ad integrare proprio i nuovi paradigmi di economia circolare; e questo è tanto più vero se pensiamo a quanto affermato dall'Ue nella "Strategia europea per i dati", secondo la quale entro il 2025 l'80% dei dati raccolti dai sistemi informatici verrà processata su infrastrutture periferiche di tipo *edge* e solo il 20% su infrastrutture centralizzate[48].

Possibili strategie per affrontare le sfide poste dagli ambiziosi obiettivi delineati dall'Ue in tema di transizione digitale e green, potrebbero essere rinvenute nel modello operativo impiegato per l'adozione del cloud nelle P.A.

In primo luogo, potrebbe essere approntato un PSN dedicato all'*edge computing*, distribuito capillarmente sul territorio nazionale ed in grado di ospitare i servizi strategici per l'implementazione delle smart city e dell'Industria 5.0 di cui anche le P.A. sono parte integrante. Questa infrastruttura potrebbe essere implementata a partire proprio dai 35 *data center* delle P.A. che AgID ha individuato come possibili candidati per un PSN cloud (solo quattro, infatti, costituiranno il PSN cloud, gli altri saranno destinati alla progressiva dismissione) previa verifica della loro distribuzione omogenea sul territorio, in mancanza della quale saranno ovviamente richiesti ulteriori investimenti per la creazione dei *data center* mancanti.

In secondo luogo, attraverso un processo di certificazione e la stesura di linee guida per l'adozione di infrastrutture e servizi *edge* da parte di AgID, in modo

analogo a quanto avvenuto per l'adozione del cloud pubblico, potrebbero essere utilizzate infrastrutture e servizi messi a disposizione dal mercato per tutti quei casi catalogati come non strategici o che non trattino dati personali o sensibili.

È da notare, tuttavia, come quest'ultima strada risulti ad oggi di difficile percorribilità non esistendo sul mercato, a differenza del cloud computing, un'offerta di infrastruttura e servizi *edge* sufficientemente matura, distribuita sul territorio e completa di servizi[49].

L'affidamento della gestione di tali infrastrutture ai grandi attori del Web, tipicamente aziende extra-Ue (si pensi a Google ed AWS), obbliga, inoltre, ad una riflessione particolarmente attenta sul trattamento dei dati. Tale problema già presentatosi in ambito cloud, ha dato vita a nuovi modelli di governance del dato, come il c.d. *Data Trust*[50], che potrebbero riproporsi con riferimento all'*edge*.

Ancora più importante diviene, in tale circostanza, la perdita di sovranità sull'infrastruttura con il rischio che aziende extra-Ue possano decidere di interrompere l'erogazione del servizio bloccando di fatto il funzionamento di intere comunità e processi industriali, fortemente dipendenti dai servizi IoT.

6. Conclusioni

La creazione di una infrastruttura tecnologica per la connettività (5G, banda ultra-larga) e la computazione (cloud, *edge*, IoT) sia a livello nazionale che europeo, necessaria a favorire la nascita di un "Mercato unico digitale", acquisisce quindi un'importanza strategica, essendo chiamata a sostenere la transizione digitale dell'intera società, dell'industria e dell'economia, così come evidenziato anche dalla Commissione europea[51].

Visto lo stato di forte ritardo nel quale versa l'infrastruttura *edge* in Italia, quella che ci si pone di fronte non è soltanto una sfida tecnologica ma, proprio a causa della pervasività dei sistemi IoT nei processi produttivi e di governance della comunità, anche normativa, dove il legislatore sarà chiamato di concerto con le istituzioni eurounitarie ad affrontare tematiche relative ai problemi di sovranità sulle infrastrutture e ai nuovi scenari che si prospettano in tema di privacy e trattamento del dato.

Note

[1] M. Breque, L. De Nul, A. Petridis, *European Commission, Industry 5.0, Towards a sustainable, human-centric and resilient European industry*, EU publication, 2021.

[2] T. Muhammed, R. Mehmood, A. Albeshri, *Enabling Reliable and Resilient IoT Based Smart City Applications*, in R. Mehmood, B. Bhaduri, I. Katib, I. Chlamtac (eds.), "Smart Societies, Infrastructure, Technologies and Applications", Proceedings of the First International Conference SCITA 2017, LNICST, vol. 224, 2018, Springer, p. 169-184. M. Mazhar Rathore, P. Anand, A. Awais, J. Gwanggil, *IoT-Based Big data: from Smart city towards next generation super city planning*, in "International Journal on Semantic web and information system", vol. 13, 2017, n. 1, p. 28-47. D. Luckey, H. Fritz, D. Legatiuk, K. Dragos, K. Smarsly, *Artificial intelligence techniques for smart city applications*, in E. Toledo Santos, S. Scheer (eds.), "Proceedings of the 18th International Conference on Computing in Civil and Building Engineering" – ICCCBE 2020 (São Paulo, Brazil on August 18-20), p. 3-15.

[3] Le principali società di telecomunicazioni presenti in Italia hanno avviato progetti volti ad introdurre infrastrutture *edge* sul territorio nazionale complementare al dispiegamento dell'infrastruttura di rete 5G. In particolare, si veda il progetto AI@EDGE, cui partecipa anche il gruppo TIM.

[4] V. l'approfondimento sul Progetto *Smarter Italy*.

[5] L'enciclopedia Treccani definisce la Smart city come l'insieme delle «strategie di pianificazione urbanistica correlate all'innovazione e in particolare alle opportunità offerte dalle nuove tecnologie della comunicazione per migliorare la qualità della vita dei cittadini. Il concetto di "città intelligente" parte dall'assunto dell'intelligenza distribuita, inscritta nello spazio pubblico, in una sorta di ridefinizione dell'antico *genius loci*. Con s.c. si tende sempre più a mettere in relazione le infrastrutture materiali delle città con il capitale umano, intellettuale e sociale di chi le abita. Un capitale potenziato e messo a sistema dalle infrastrutture immateriali del Web. Nella s.c. la connettività telematica è quindi considerata una fonte di crescita e di sviluppo urbano per promuovere l'idea di città inclusiva, attraverso la promozione di nuove forme di coesione sociale. Una città sostenibile per le misure ecologiche sia di controllo sia di risparmio energetico e tesa a ottimizzare le soluzioni per la mobilità e la sicurezza grazie a pratiche d'innovazione territoriale. Una s.c. è tale in via direttamente proporzionale alla qualità della partecipazione attiva dei suoi cittadini, in un contesto in cui lo spazio pubblico della città viene interpretato con particolari forme di creatività sociale, come quelle di *urban experience* nell'interazione tra Web e territorio (ambito di progettazione culturale e di azione multimediale attraverso le reti)». A livello globale sono 153 le città che hanno pubblicato una strategia ufficiale di smart city. Secondo lo studio *The Smart City Breakaway* 2019 condotto dalla società di consulenza Roland Berger, sono da annoverare tra di esse Vienna, Londra e la canadese Saint Albert. In particolare, Vienna al fine di gestire i big data ha adottato la piattaforma *VeroCity* ed è stata una delle prime città a pubblicare dati governativi aperti. Attraverso la sua piattaforma è in grado di aggregare ed analizzare tali dati basandosi su *Context Broker* della Commissione europea, sistema in grado di ordinare i dati di tutti i tipi e provenienti da fonti di tutta la città, consentendo di offrire informazione in tempo reale su mobilità urbana, monitoraggio ambientale, infrastrutture urbane, efficienza energetica, facilitando così le attività quotidiane. Interessante anche il caso di Saint Albert la quale annovera tra i suoi progetti smart l'implementazione di un nuovo sistema di gestione delle prenotazioni e registrazione per migliorare i servizi per la salute mentale dei cittadini, la creazione di una foresta comunitaria per le locali banche del cibo, supportata da una mappatura on-line, lo sviluppo della tecnologia necessaria a supporto degli anziani nelle loro case (reti a banda larga, telematica, medicina); la realizzazione di un sistema di trasporto intelligente con segnali adattivi come sistemi di monitoraggio centrale, situazioni di conteggio permanente, stazioni RWIS. Per il *City mobility index 2020* di Deloitte, invece, è Stoccolma la città più smart nella mobilità.

[6]R. Giffinger, C. Fertner, H. Karmar et al., *Smart cities. Ranking of European medium sized cities*, final report, October 2007; D. Harvey, *L'esperienza urbana*, il Saggiatore, 1998; R.G. Hollands, *Will the Real Smart City Stand Up? Intelligent, Progressive, or Entrepreneurial?*, in "City. Analysis of Urban Change, Theory, Action", vol. 12, 2008, n. 3, p. 303.

[7]European Commission, *Smart cities*.

[8]Volendo fare alcuni esempi, si pensi al moltiplicarsi di iniziative pionieristiche volte a sperimentare l'introduzione di servizi digitali integrati nel tessuto urbano come sistemi di *smart grid* per la gestione intelligente delle reti elettriche ed idriche; progetti di mobilità urbana; sistemi di rilevamento di parametri ambientali; l'utilizzo dei droni per il monitoraggio del territorio o di robot per la raccolta dei rifiuti.

[9]Si pensi al potenziamento del sistema di identità digitale SpID, all'introduzione dell'app IO.it, alla creazione di piattaforme digitali per la gestione della campagna vaccinale.

[10]Un esempio significativo è rintracciabile nel programma *Smarter Italy*, che nasce con il decreto del Ministero dello sviluppo economico del 31 gennaio 2019 e diviene operativo con la convenzione tra MISE ed AgID. Con il Protocollo d'intesa, firmato ad aprile 2020, il Ministero dell'università e ricerca e il Dipartimento per la trasformazione digitale entrano a far parte del progetto, inserendo al suo interno il segmento "Borghi del futuro", una delle 20 azioni di "Italia 2025" del MITD, che sperimenta le soluzioni innovative del programma anche su comuni di minore dimensione. Il laboratorio *Smarter Italy* è così costituito da 11 centri urbani (le c.d. smart city: Bari, Cagliari, Catania, Genova, L'Aquila, Matera, Milano, Modena, Prato, Roma, Torino) che rappresentano il luogo di sperimentazione delle soluzioni proposte, ai quali si aggiungono 12 piccoli centri che costituiscono i "Borghi del futuro" (veri e propri laboratori di innovazione tecnologica che vedono quali protagonisti: Alghero, Bardonecchia, Campobasso, Carbonia, Cetraro, Concorezzo, Ginosa, Grottammare, Otranto, Pantelleria, Pietrelcina e Sestri Levante). Le prime aree di intervento del programma sono: *Smart mobility*, per il miglioramento sostanziale dei servizi per la mobilità di persone e merci nelle aree urbane; valorizzazione dei beni culturali (*Cultural Heritage*), per la valorizzazione economica e turistica delle aree di rilevanza storica e artistica; benessere sociale e delle persone (*Wellbeing*) per il miglioramento dello stato psico-fisico dei cittadini; protezione dell'ambiente per il miglioramento della situazione ambientale in tutti i suoi aspetti. Sono previste ulteriori aree di intervento con l'avanzamento del Programma, tenendo conto degli obiettivi posti dai soggetti che vi aderiranno.

[11]N.M. Gusmerotti, M. Frey, F. Iraldo, *Management dell'economia circolare*, Franco Angeli, 2020.

[12]A. Moliterni, *La sfida ambientale e il ruolo dei pubblici poteri in campo economico*, in "Rivista quadrimestrale di diritto dell'ambiente", 2020, n. 2, pp. 32-71.

[13]Risoluzione del Parlamento europeo, *Nuovo piano d'azione per l'economia circolare*, 10 febbraio 2021.

[14]Ministero della Transizione ecologica, *Strategia nazionale per l'economia circolare*, 30 settembre 2021.

[15]Volendo fare un esempio si pensi allo *Smart Bin* del progetto INNOWEE, promosso dall'ENEA, che dal 2018 si propone di creare un modello innovativo per la gestione della raccolta dei rifiuti da apparecchiature elettriche ed elettroniche (c.d. RAEE). Si tratta di un sistema di riconoscimento che consente il conferimento del rifiuto solo se l'utente si fa riconoscere tramite tessera sanitaria ed è dotato di sensori di riempimento che, collegati a piattaforma Web, forniscono in tempo reale ed in autonomia, informazioni su quantità e tipo di RAEE raccolti. R. Morabito, *La transizione verso l'economia circolare in aree e comunità urbane: approccio ENEA*, Firenze University Press, 2020.

[16]Per un approfondimento sull'*Agenda 2030 NU* e sul *Green Deal europeo*, L. Kappler, *Il recepimento dell'Agenda 2030 per lo sviluppo sostenibile: spunti metodologici dalle esperienze statunitensi dei distretti d'innovazione dell'area di Boston*.

[17]European Commission, *Industry 5.0: Towards more sustainable, resilient and human-centric industry*, 7 January 2021.

[18]Ministero dello sviluppo economico, *Piano nazionale Industria 4.0*.

[19]L'Industria 4.0, basata sulla digitalizzazione, sull'automatizzazione e sull'interconnessione dei processi produttivi, si è affermata ormai da un decennio. Si tratta di quell'industria che ha visto nascere, evolversi ed affermarsi tecnologie avanzate come cloud computing e *Information Technology*, *Internet of Things (IoT)* e Intelligenza Artificiale, realtà aumentata, Big data, l'HMI ovvero l'interfaccia uomo-macchina innovativa, volte ad incrementare flessibilità e efficienza della produzione. Se scopo dell'Industria 4.0 è quello di massimizzare efficienza, produttività e migliorare la qualità della vita del lavoratore, da più parti sono stati sollevati dubbi sulla effettiva capacità di questo tipo di organizzazione di migliorare la qualità del lavoro e delle condizioni del lavoratore, ritenendo disattese le aspettative iniziali e ravvisando nell'introduzione di robot nell'organizzazione dei cicli produttivi delle aziende un rischio proprio per i posti di lavoro. L'Industria 5.0 propone, invece, una visione dell'industria che va al di là dell'efficienza e della produttività come unici obiettivi, proponendo un ruolo attivo e da protagonista del mondo produttivo nel fornire soluzioni alle sfide che la società si troverà ad affrontare, compresa la conservazione delle risorse, il cambiamento climatico, l'equità, la sostenibilità e la stabilità sociale. Parole chiave dell'industria 5.0 sono dunque resilienza, sostenibilità e visione umanocentrica. Si tratta, infatti, di un approccio che che mette in risalto l'importanza della ricerca e dell'innovazione a supporto non solo dell'industria ma soprattutto dell'umanità. La Commissione europea ha riconosciuto all'Industria 5.0 il potere di raggiungere gli obiettivi sociali al di là della crescita e del lavoro, per diventare fornitrice resiliente di prosperità attraverso produzioni che rispettino l'ambiente ed il nostro pianeta ponendo il benessere del lavoro aziendale al centro dei processi produttivi. L'approccio Industria 5.0 contribuisce, infatti, a tre delle priorità della Commissione: "Un'economia al servizio delle persone", "Green Deal europeo" e "L'Europa pronta per l'era digitale". Gli elementi pertinenti a Industria 5.0 fanno già parte delle principali iniziative politiche della Commissione: adottare un approccio incentrato sull'uomo per le tecnologie digitali, compresa l'intelligenza artificiale; riqualificazione dei lavoratori europei, in particolare delle competenze digitali; industrie moderne, efficienti sotto il profilo delle risorse e sostenibili e transizione verso un'economia circolare; un'industria globalmente competitiva e leader mondiale, accelerando gli investimenti in ricerca e innovazione. European Commission, *Industry 5.0*. La differenza principale tra Industria 4.0 e 5.0 risiede, quindi, nella capacità di quest'ultima di creare le condizioni affinché il rapporto uomo-tecnologie intelligenti al servizio del settore del lavoro sia sempre più equilibrato e dia vita ad una collaborazione tra uomo e robot. Antonio Frisoli, docente di robotica presso la Scuola Superiore Sant'Anna, ha affermato che i robot collaborativi (c.d. Cobot) sono una leva per un'industria che si avvia verso la fase 5.0 della propria evoluzione, con notevoli cambiamenti sulla società e nuovi scenari di applicazione di tali innovazioni. Con "robotica collaborativa" ci si riferisce a quei sistemi robotici di nuova generazione che sono in grado di interagire fisicamente in sicurezza con l'uomo e di condividerne lo spazio, non rimanendo pertanto più confinati in una "gabbia" che separa lo spazio dell'uomo da quello del robot. A. Di Minin, *L'empatia dei robot – dialogo con Antonio*

Frisoli, in "Il sole 24ore", 7 ottobre 2021. Non è un caso che i concetti di Industria 5.0 e Società 5.0 siano strettamente legati tra di loro in quanto si propongono di delineare un cambio di paradigma sia da un punto di vista sociale che economico attraverso un approccio antropocentrico. Scopo della Società 5.0 è quello di bilanciare lo sviluppo economico con la risoluzione di problematiche sociali ed ambientali. Tale cambio di paradigma non è limitato solo al settore della produzione ma anche alla maggior parte dei problemi sociali ed ambientali provocati dal rapporto tra mondo reale e virtuale. La Commissione europea nel suo paper *Industry 5.0: towards a sustainable, human-centric and resilient European industry* ha affermato che la Società 5.0 è una società nella quale le tecnologie informatiche avanzate, IoT, robots, A.I. e realtà aumentata sono utilizzate nella vita di tutti i giorni, nell'industria, nell'assistenza sanitaria, ed in altre sfere di attività, a vantaggio non solo e principalmente dell'industria ma anche e soprattutto per il bene e la convenienza dei cittadini. M. Breque, L. De Nul, A. Petridis, *op. cit.*; A. Ajoudani, A. Zanchettin, S. Ivaldi et al., *Progress and Prospects of the Human-Robot Collaboration. Autonomous Robots*, Springer Verlag, 2017, p. 1-17.

[20]Il termine IoT si riferisce ad una rete di dispositivi fisici (*things*) che possono essere connessi tra loro e con altri servizi dispiegati su reti locali o globali. Tali dispositivi sono tipicamente composti da sensori, attuatori, apparati di telecomunicazioni e unità di processamento di modesta capacità computazionale (c.d. microcontrollori).

[21]Ministero dello sviluppo economico, *Programma di supporto alle tecnologie emergenti 5G*.

[22]Governo italiano, *Programma strategico Intelligenza Artificiale 2022-2024*, 24 novembre 2021. Di recente il Consiglio di Stato con sentenza n. 7891/2021 ha avuto modo di precisare la differenza tra algoritmo ed AI sottolineando come in quest'ultima "l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole sofware e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico". Anche la Commissione europea nella sua Proposta di regolazione dell'AI, del 21 aprile 2021, all'art. 3 ha definito i sistemi di Intelligenza artificiale come "software sviluppato con una o più tecniche e approcci elencati nell'allegato I e che può, per una data serie di obiettivi definiti dall'uomo, generare risultati quali contenuto, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono". *Proposta di Regolamento del Parlamento europeo e del Consiglio europeo che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione* (COM/2021/206 final).

[23]L. Hardesty, *Explained: Neural networks. Ballyhooed artificial-intelligence technique known as "deep learning" revives 70-year-old idea*, MIT News Office, April 14, 2017.

[24]K. Ranjithprabhu, D. Sasirega, *Eliminating Single Point of Failure and Data Loss in Cloud Computing*, in "International Journal of Science and Research", vol. 3, 2014, n. 4, p. 335-337.

[25]P. Middleton, J. Tully, P. Kjeldsen, *Forecast: The Internet of Things, Worldwide*, 2013.

[26]P. Fraga-Lamas, S.I. Lopes, T.M. Fernández-Caramés, *Green IoT and Edge AI as Key Technological Enablers for a Sustainable Digital Transition towards a Smart Circular Economy: An Industry 5.0 Use Case*, in "Sensors", vol. 21, 2021, n. 17, 5745.

[27]L'*edge computing* è una parte rilevante del mercato OT (*Operational Technology*) e crescerà rapidamente nei prossimi cinque anni. All'interno del mercato delle infrastrutture, il cloud computing si imporrà sia nel cluster Europe-5 che in quello Big-5, laddove l'*edge computing* costituirà un'area in forte crescita nei prossimi 5 anni. La Germania sarà il più grande mercato europeo sia per il cloud computing che per l'*edge computing* con una crescita del 28% (2025 vs 2020). Osservando il cluster Big-5, è previsto che le cifre crescano sia per il mercato del *cloud hosted* pubblico/privato sia per quello dell'infrastruttura OT e dell'*edge*, con un impressionante aumento fino al 60% (2025 vs 2020) negli USA. Cfr. *From Cloud to Edge. Una panoramica sul mercato mondiale del Cloud Computing con un focus sulle nuove opportunità offerte dall'Edge Computing*.

[28]C. Ratti, M. Claudel, *La città di domani, come le reti stanno cambiando il futuro*, Einaudi, 2017.

[29]La sicurezza ha da sempre assunto un ruolo centrale nella società: per Castel il mondo sociale «è stato organizzato in funzione della continua, affannosa ricerca di protezione e sicurezza»; Malinowsky asseriva che ogni cultura è costituita dall'insieme di risposte che la società fornisce ai bisogni dell'attore sociale, suddividendo i bisogni in fondamentali e in derivati. La sicurezza intesa sia come tutela dell'integrità fisica sia come dimensione sociale stabile e sicura, è da collocarsi proprio tra i bisogni primari, è il primo tra i bisogni primari, propedeutico a tutti gli altri bisogni, come ha affermato Maslow essa costituisce «una componente cruciale per la qualità della vita». Bauman distingue tre tipi di sicurezza che con la post-modernità sembrano essere entrati in crisi: «una sicurezza (*security*) che ha a che vedere con la propria condizione sociale e lavorativa e si poggia sulla stabilità e affidabilità del mondo; una sicurezza (*certainty*) di tipo cognitivo che ha a anche fare con la prevedibilità e intelligibilità dell'ambiente che ci circonda e della nostra posizione in esso; una sicurezza (*safety*) di tipo fisico che riguarda le minacce alla incolumità propria e dei propri beni». R. Castel, *L'insicurezza sociale. Che significa essere protetti?*, Einaudi, 2011. B. Malinowsky, *Freedom and Civilization*, Greenwood Press, 1976. A. Maslow, *Motivation and Personality*, Harper & Row Publishing, 1954. Z. Bauman, *Paura liquida*, Laterza, 2006.

[30]M. Sessa, *Smart Safe City: criticità e prospettive sociali*, in "Rivista trimestrale di scienza dell'amministrazione", 2020, n. 3.

[31]Il Ministero dell'Interno nel *Dossier* del Viminale 1° agosto 2020-31 luglio 2021, ha evidenziato come rispetto all'anno precedente gli attacchi informatici siano decuplicati (da 460 nel periodo 2019-2020 a 4.938 nel periodo 2020-2021) così come gli *alert* diramati hanno subito un aumento del 212%).

[32]Si veda al riguardo *Rapporto Clusit sulla sicurezza ICT in Italia*, marzo 2022.

[33]Si pensi a titolo esemplificativo al settore sanitario e a quello della mobilità; si ricordino gli attacchi ai sistemi informatici di LazioCrea e a tutti i siti di riferimento (Regione Lazio, Lazio salute, portale prenotazione vaccini) dell'agosto 2021.

[34]S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in "Harvard Law Review", vol. 4, 1890, n. 5, p. 193-220. Furono Samuel Warren e Louis Brandies a definire per la prima volta la privacy come «the right to be let alone» ovvero, il diritto a essere lasciati soli, a godere del proprio privato, una sorta di estensione soggettiva del diritto lockiano alla proprietà privata. «The Right to Privacy» rappresenta la pietra angolare su cui poggia il moderno istituto giuridico della privacy; diritto fondamentale su cui si fonda la libertà individuale di fronte a quello che Zuboff ha definito «Capitalismo della Sorveglianza». Sono proprio i cambiamenti sociali, politici, ed economici ad imporre una rilettura del concetto di privacy e della sua estensione.

[35]Non è un caso che negli ultimi anni e soprattutto a seguito dell'accelerazione impressa dalla Pandemia al processo di digitalizzazione della società, privacy e cybersecurity siano

stati oggetto di intervento sia da parte dell'Unione europea che dei singoli Stati. In particolare, si ricordino l'introduzione della c.d. direttiva NIS - *Network and information security* (direttiva 2016/1148 che nel 2020 ha visto una proposta di revisione c.d. NIS2) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi, nonché il *Cybersecurity Act* (Regolamento (UE) 2019/881) attraverso il quale è stato potenziato il ruolo dell'Enisa (Agenzia europea per la sicurezza delle reti e dell'informazione); l'introduzione del GDPR Regolamento (UE) 2016/679. Anche l'Italia si è mossa in tal senso. La direttiva NIS è stata recepita nell'ordinamento italiano con il d.lgs. 18 maggio 2018, n. 65, che detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS. Successivamente, è stato adottato il d.l. 21 settembre 2019, n. 105 al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal d.l. 30 dicembre 2019, n. 162, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione. In attuazione del d.l. 105/2019 sono stati definiti in particolare il d.P.C.M. 30 luglio 2020, n. 131, che ha dettato criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza cibernetica, e il d.P.C.M. 14 aprile 2021, n. 81 che definisce le modalità per la notifica nel caso di incidenti riguardanti beni ITC. Infine, con il d.l. 14 giugno 2021, n. 82, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale.

[36]L'uso di droni dotati di dispositivi tecnologici può avere un forte impatto sulla privacy e sulla protezione dei dati personali degli interessati, in quanto gli operatori di droni che registrano e/o elaborano immagini, video, suoni e che si avvalgono di dati biometrici e di geolocalizzazione relativi a una persona, possono identificarla direttamente (mediante una foto o un video) o renderla identificabile attraverso una successiva elaborazione (come nel caso delle informazioni relative alla geolocalizzazione) o l'"arricchimento" con altri dati aggiuntivi come quelli acquisiti da Internet. In questi ultimi casi, anche se una persona potrà essere identificabile, il risultato finale riguarderebbe un'identificazione possibile grazie a informazioni incrociate provenienti da diverse fonti. Sia nel caso in cui i dati raccolti dai droni identificano inequivocabilmente una persona, sia nel caso in cui ciò possa avvenire successivamente, si applica comunque la normativa in materia di protezione dei dati personali Regolamento (UE) 2016/679 (GDPR). È da notare, inoltre, che quando ci troviamo di fronte ad un insieme di "dati misti" ovvero dati personali e non personali, il Regolamento sui dati non personali RDNP (Regolamento (UE) 2018/1807) sembra vacillare: all'art. 2 stabilisce infatti che il Regolamento generale sulla protezione dei dati personali e quello sulla libera circolazione dei dati non personali si applicano alla rispettiva categoria di dati; tuttavia quando tali insieme di dati sono indissolubilmente legati, il GDPR troverà applicazione all'intero *dataset* anche quando i dati personali rappresentano solo una piccola parte dell'insieme, in ossequio alla costante logica del primato della protezione rispetto alla circolazione. In tale direzione sembra essersi mosso anche il Garante della Privacy nell'affrontare tale questione. Garante per la protezione dei dati personali, *Droni e privacy - Il Vademecum del Garante*.

[37]È da notare anche come ad oggi la maggior parte dei costruttori di device mostri gravi carenze nella tutela della privacy degli utenti. Come mostrato nell'indagine condotta nel maggio del 2017 dal *Global Privacy Enforcement Network* (GpEN) del quale fa parte anche il Garante italiano, per verificare il rispetto della privacy nella IoT, su oltre trecento dispositivi elettronici connessi a Internet, più del 60% non ha superato l'esame dei Garanti della privacy di 26 paesi. È emerso in particolare che: il 59% degli apparecchi non offre informazioni adeguate su come i dati personali degli interessati sono raccolti, utilizzati e comunicati a terzi; il 68% non fornisce appropriate informazioni sulle modalità di conservazione dei dati; il 72% non spiega agli utenti come cancellare i dati dal dispositivo; il 38% non garantisce semplici modalità di contatto ai clienti che desiderano chiarimenti in merito al rispetto della propria privacy Garante per la protezione dei dati personali, *Privacy: "Internet delle cose",utenti poco tutelati. I risultati dell'analisi internazionale svolta dalle Autorità garanti della privacy di 26 Paesi per il "Privacy Sweep 2016"*, 22 settembre 2016.

[38]Si pensi ad un sistema informatico per il rilevamento di sinistri stradali dotato: di un drone per l'acquisizione delle immagini, di una AI dispiegata su sistemi *edge* in grado di riconoscere un sinistro analizzando una serie di immagini, ed infine di un sistema centralizzato dispiegato su cloud che, ricevuta una segnalazione di sinistro dalla AI, invia i soccorsi. In tale casistica il drone potrebbe rilevare la presenza di individui nelle vicinanze delle auto fotografate. L'AI, valutando esclusivamente le immagini che rappresentano lo stato attuale del traffico, è in grado di valutare se sono presenti situazioni critiche, ma una volta presa tale decisione non avrà più la necessità di accedere alle medesime immagini, che verranno quindi cancellate. Il sistema centrale cloud non avrà mai bisogno delle singole immagini per erogare il proprio servizio, ma necessiterà solamente di ricevere una asettica segnalazione di avvenuto sinistro da parte dell'AI.

[39]M. Ahmed, P. Haskell-Dowland (eds.), *Secure Edge Computing. Applications, Techniques and Challenges*, CRC Press, 2021.

[40]*European industrial technology roadmap for the next generation cloud-edge offering*, May 2021.

[41]Il *Piano Nazionale di Ripresa e Resilienza* (PNRR), grazie ai fondi del *Next Generation Europe EU* (NGEU), prevede un investimento di oltre 190 miliardi di euro in risposta alla crisi pandemica destinati in parte a finanziare proprio l'implementazione del Piano Triennale per l'informatica nella pubblica amministrazione 2021-2023 al fine di produrre nei prossimi anni una ulteriore forte accelerazione nei processi di innovazione in atto. Il Piano triennale per l'informatica nella pubblica amministrazione, dell'ottobre 2021, è il risultato della collaborazione tra AGID ed il Dipartimento per la trasformazione digitale ed elenca tra i principi guida del processo di digitalizzazione: *digital & mobile first*; *digital identity only*; *cloud first*; servizi inclusivi e accessibili; dati pubblici un bene comune; interoperabile *by design*; sicurezza e *privacy by design*; *user-centric*, *data driven* e agile; *once only*; le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite; transfrontaliero *by design*; codice aperto. Si veda anche, European Commission, *Bussola per il digitale 2030: il modello europeo per il decennio digitale (c.d. Digital compass)*, 9 marzo 2021. Id., *2030 Digital Compass: your digital decade*.

[42]La digitalizzazione delle pubbliche amministrazioni si inserisce in un disegno di più ampio respiro di matrice europea, delineato dal *Green Deal europeo* COM(2019) 640 dell'11 dicembre 2019 e dalla Nuova strategia industriale, parte integrante della strategia Ue per riorientare il processo macroeconomico ed attuare i 17 obiettivi di sviluppo sostenibile previsti dall'Agenda 2030 (United Nations, *Transforming our world: the 2030 Agenda for Sustainable Development*) andando a costituire un primo indispensabile passo per far

sì che si realizzi l'incontro tra i diversi stakeholder (imprese, terzo settore, cittadini, P.A.) che daranno vita alle future città e comunità digitali.

[43]La diffusione della banda ultra-veloce e le reti 5G è affidata a cinque progetti: "Italia a 1 Giga", "Italia 5G", "Scuole connesse", "Sanità connessa" e "Collegamento isole minori". Il progetto di maggiore rilevanza è rappresentato da Ministro per l'innovazione tecnologica e la transizione digitale, *Piano "Italia 5G". Consultazione pubblica ai sensi del paragrafo 64 e 78, lettera b) degli Orientamenti dell'Unione europea per l'applicazione delle norme in materia di aiuti di Stato in relazione allo sviluppo rapido di reti a banda larga*, 15 novembre 2021.

[44]Dipartimento per la Trasformazione Digitale, Agenzia per la Cybersicurezza Nazionale, *Strategia Cloud Italia. Documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud della PA*; Ministro per l'innovazione tecnologica e la transizione digitale, *Italia digitale 2026. Obiettivi e iniziative per il digitale nel Piano nazionale di ripresa e resilienza*.

[45]Al fine di rendere effettivi ed efficaci gli interventi appena descritti è intervenuta poi la novità in campo normativo del Decreto Semplificazioni "bis" (d.l. 31 maggio 2021, n. 77 come convertito con la l. 29 luglio 2021, n. 108) il quale ha introdotto l'art. 18-bis del CAD (Violazione degli obblighi di transizione digitale). La norma richiede una maggior attenzione all'adempimento di tutte le indicazioni riportate nel Piano Triennale, con il supporto da parte dell'AgID, nell'orientare l'approccio operativo secondo principi di indirizzo, collaborazione, supporto e deterrenza agli attori interessati dalle norme in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione. All'AgID è altresì attribuito il compito di stabilire con proprio regolamento le procedure di contestazione, accertamento, segnalazione e irrogazione delle sanzioni per le violazioni di cui alla presente disposizione. Tutto ciò sarà necessario al fine di raggiungere gli obiettivi preposti nei tempi previsti, evitando eventuali provvedimenti sanzionatori per mancata ottemperanza degli obblighi di transizione digitale.

[46]Dal Censimento AgID del patrimonio ICT è risultato che dei 1.252 data center censiti: 35 sono risultati candidabili all'utilizzo da parte del polo strategico nazionale; 27 sono stati classificati nel gruppo A; i restanti 1.190 sono stati classificati nel gruppo B.

[47]Il *Piano triennale per l'informatica nella pubblica amministrazione 2019-2021* al capitolo 3.2.3, predispone le linee di azione per la migrazione al cloud.

[48]*Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Una strategia europea per i dati*, 19 febbraio 2020 COM(2020) 66 final: «il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2051. Ogni nuova ondata di dati offre all'UE grandi opportunità per divenire un leader mondiale nel settore. Anche le modalità di conservazione ed elaborazione dei dati cambieranno significativamente nei prossimi cinque anni. Attualmente l'80% delle elaborazioni e delle analisi dei dati si svolge in centri di dati e strutture di calcolo centralizzate, e il 20% in oggetti connessi intelligenti, quali automobili, elettrodomestici o robot di fabbricazione, e in strutture di calcolo vicine all'utente ("edge computing"). Entro il 2025 tali percentuali probabilmente si invertiranno. Una simile evoluzione, oltre a presentare vantaggi economici e in termini di sostenibilità, crea ulteriori opportunità per lo sviluppo, da parte delle imprese, di strumenti che consentano ai produttori di dati di incrementare il controllo sui propri dati».

[49]Ad oggi solo alcuni operatori di telecomunicazioni e cloud provider, pionieri del settore, hanno avviato sperimentazioni in ambito IoT ed *edge computing* sul territorio nazionale. Volendo fare alcuni esempi si vedano i progetti di Reply, Fastweb, Google ed Amazon. Sempre il gruppo TIM partecipa ad una iniziativa congiunta con Google volta a creare un nuovo soggetto Noovle.

[50]L'approvazione del *Cloud Act* da parte del Congresso USA e la pretesa di poter accedere ai dati degli utenti custoditi dai fornitori cloud americani indipendentemente dal luogo in cui sono conservati, superando così il concetto e le garanzie assicurate dal modello c.d. *Data Location*, ha alimentato i timori di indesiderate interferenze da parte degli Stati Uniti sui dati dei cittadini di altri Paesi. Nel modello *Data trust*, il fornitore di servizi cloud si avvale di un soggetto esterno (c.d. *data trustee*) per la gestione di tutto ciò che esula dalla stretta manutenzione operativa dell'infrastruttura. Attraverso la figura negoziale del trust il fornitore si spoglia completamente della facoltà giuridica di accedere ai dati che transitano sull'infrastruttura per affidarli ad una terza parte. Tutte le richieste di accesso ai dati dovranno essere indirizzate al *Trustee* (l'unico in possesso delle chiavi di cifratura), il quale sarà tenuto a valutare tali richieste sulla base del solo diritto nazionale. Per un approfondimento si veda V. Boncinelli, *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in questa Rivista, 2021, n. 1, pp. 27-45.

[51]European Commission, *Sovranità digitale: la Commissione dà il via ad alleanze per i semiconduttori e le tecnologie cloud industriali*, Bruxelles, 19 luglio 2021; Id., *European Chips Act*, 8 February 2022.

* * *

The Public administration in the age of cloud and edge computing, between opportunities and risks: PNRR and digital communities

Abstract: *Smart cities* and *Industry 5.0* are essential pieces of the European strategy for the transition to a more sustainable and fair economy. The introduction of fundamental enabling technologies, such as Internet of Things, Artificial Intelligence and Edge Computing, requires an assessment of the current state of national digital infrastructures in relation to the missions of the PNRR, which is the foundation of the Italian digital strategy. In this context, the public administration plays a leading role in connecting all the stakeholders (companies, citizens, third sector). This article aims to verify possible criticalities introduced by those technologies and possible similitudes with the governance of the implementation and regulation of cloud computing, in order to evaluate the impact of the transition to a digital and integrated society on digital sovereignty and data protection.

Keywords: Digital Sovereignty – Internet of Things – Cloud and edge computing – Smart city – Circular economy

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0066
Articolo sottoposto a peer review

L'evoluzione normativa dell'intermediazione digitale: nuovi profili di responsabilizzazione

Giulia Bazzoni

Il contributo si propone di indagare, in primo luogo, lo sviluppo delle piattaforme di intermediazione digitale e il loro notevole impatto sulla governance dell'ecosistema digitale; in secondo luogo, mira ad individuare nuovi strumenti di tutela per gli utenti in una prospettiva oscillante *de iure condito - de iure condendo*. Le piattaforme di intermediazione, per la propria natura "fluida", sia nella struttura che nei servizi, si sono rivelate entità di complessa qualificazione giuridica. Esse ricoprono un ruolo preminente nel mercato digitale privo di frontiere, avendo assunto una posizione di indubbia forza nelle relazioni negoziali con gli utenti, creando situazioni di sostanziale asimmetria, spesso a scapito dei diritti individuali coinvolti. Complice della situazione attuale, la normativa europea di settore, ritenuta spesso obsoleta e talmente incapace di governare il fenomeno in oggetto da suscitare dubbi circa la ragionevolezza di un nuovo intervento regolativo delle istituzioni in materia. In virtù di quanto espresso, attraverso l'analisi sistematica dei nuovi testi normativi attinenti alla dimensione digitale, si prenderà in considerazione come le nuove tecniche regolative ivi previste, quale la responsabilizzazione delle piattaforme attraverso obblighi conformativi, possano o meno contribuire a costituire una governance dell'ecosistema digitale maggiormente trasparente e sicura.

Piattaforme – Intermediazione – Governance – Responsabilizzazione

Sommario: *1. Introduzione alle caratteristiche delle piattaforme di intermediazione digitale nel panorama* Onlife – *2. Tra auto-regolazione ed etero-regolazione della governance delle piattaforme – 3. Gli atti normativi del cd. pacchetto digitale, in una prospettiva oscillante* de iure condito - de iure condendo – *4. La struttura "responsabilizzante" nella governance delle piattaforme all'interno del cd. pacchetto digitale – 5. Conclusioni: nuove prospettive giuridiche nella transizione digitale*

1. Introduzione alle caratteristiche delle piattaforme di intermediazione digitale nel panorama *Onlife*

L'iperconnessione costante degli individui, grazie all'apporto di Internet nella vita quotidiana, ha assunto attualmente livelli tali per cui l'epoca odierna viene spesso definita "età telematica", la quale si connota per la creazione di dinamiche e opportunità precedentemente impensabili[1]. Così, l'inscindibile compenetrazione tra dimensione online e offline si riscontra sempre più anche nel linguaggio prescelto e nella creazione di neologismi in grado di descrivere la situazione odierna, come il termine *Onlife*, che definisce chiaramente l'attuale contesto strutturalmente ibrido e che si presenta alla stregua dell'«habitat delle mangrovie», in ragione del fatto che la linea di demarcazione tra dimensione digitale e reale risulta alquanto sfumata, posto che nell'era dello smart-

G. Bazzoni è dottoranda in Diritto, mercato e persona, XXXIV ciclo, Università Ca' Foscari, Venezia. Collabora attualmente con lo studio legale Qubit Law Firm, quale consulente legale sull'innovazione digitale.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

phone non è affatto agevole comprendere se si «sia connessi o meno»[2].

In questo ambiente tramutano profondamente anche le logiche sottese alla circolazione dei beni ed erogazione dei servizi, in quanto si assiste ad una transizione importante verso nuovi modelli di business improntati maggiormente alla garanzia di nuove modalità di accesso alle risorse rapide, ubique, economiche e condivise, tentando di risolvere così, almeno in apparenza, le incongruenze presenti nelle rigide strutture dell'architettura tradizionale del mercato offline e l'*impasse* di un sistema strutturato sulla titolarità esclusiva dei beni, divenuto perlopiù proibitivo per la collettività[3].

Per oltrepassare tali crismi si volge lo sguardo, dunque, verso le potenzialità ancora inespresse del Web, sfruttando, da una parte, l'assenza di barriere fisiche e la possibilità di interazione costante tra gli utenti e usufruendo, dall'altra, della peculiare funzione assunta nel mercato digitale dalle piattaforme[4]. Il ruolo, perlomeno formale, di quest'ultime sarebbe quello di porre in contatto domanda ed offerta, grazie alla struttura fortemente relazionale della rete, favorendo così l'interazione fra i privati oltre che la condivisione di un ampio novero di beni e servizi; le piattaforme fungono così da intermediarie tra le parti e, dunque, da punto di accesso strategico al mercato digitale, divenendo il canale principale per tutte le transazioni digitali[5].

Sennonché, in concreto, si è assistito ad una netta divergenza tra piano formale e sostanziale circa la funzione svolta effettivamente dagli intermediari: abusando della propria posizione di preminenza, nonché dell'obsolescenza della normativa sul commercio elettronico, che è ormai fortemente datata nel tempo e carente nella configurazione puntuale di tali figure, essi esigono da parte degli utenti l'adesione *ex ante* a condizioni contrattuali unilateralmente prestabilite che pregiudicano spesso l'autonomia e la libertà negoziale degli *users*[6].

Tali termini contrattuali imposti dai portali non si riferiscono, difatti, solo al rapporto di intermediazione in senso stretto, ma riguardano anche le modalità di erogazione dei servizi sottostanti. La "decretazione impositiva", attraverso «tecniche conformatrici del rapporto», appare in concreto strutturale all'interno di questi contesti, poiché l'accettazione passiva degli utenti di «scambi senza accordo» è un abile congegno nella logica controllante della *platform economy*[7]. L'unica libera scelta rimessa agli *users* sarebbe, pertanto, "to click or not to click" sulla casella di accettazione delle condizioni imposte, senza poter entrare nel merito dei contenuti prescelti, i quali vengono imposti dai portali a detrimento dell'autodeterminazione dell'utente medio. Si assiste, così, ad un atteggiamento diffuso delle piattaforme che tende a soverchiare il proprio ruolo formale; *de facto*, questi soggetti mirano, infatti, a divenire "controllori dell'accesso" a beni o servizi[8].

La posizione degli *users* è ulteriormente pregiudicata nel rapporto con le infrastrutture digitali dall'interferenza strutturale tra circolazione dei dati personali e dei beni, che si verifica all'interno dei portali: si tratta, invero, di un sistema in grado di causare ampi squilibri e asimmetrie nelle relazioni negoziali instaurate tra gli utenti e le piattaforme[9]. È ormai noto, che grazie allo sfruttamento del "capitale informativo" derivante dalla profilazione dei dati personali degli utenti, i gestori dei portali sono in grado di incidere nelle scelte consumeristiche degli utilizzatori e tutto ciò avviene sovente in spregio della normativa sul trattamento dei dati personali; si pensi, a riguardo, alla prassi ormai diffusa da parte dei cd. *marketplace* di calibrare le offerte personalizzandole a seconda del prospetto algoritmico che descrive l'utente.

In sintesi, nell'arco di breve tempo, questi soggetti sono stati in grado di creare ecosistemi regolativi autonomi, strutturati spesso a detrimento di ogni garanzia per gli *users*. Tale situazione presenta notevoli rischi anche per l'ordinamento giuridico europeo in sé, in quanto è potenzialmente in grado di pregiudicare proprio ciò che la Direttiva sul commercio elettronico mirava a preservare, ossia un mercato di libero ed equo scambio aperto all'interazione continua[10]. I pilastri della regolamentazione europea di settore vacillano, così, dinnanzi a questi nuovi protagonisti del panorama *Onlife* che traggono la propria forza normativa dall'abilità di continuo trasformismo e adattamento ai mutamenti tecnologici in atto.

Tale situazione ha generato un ampio dibattito in seno alla dottrina circa l'opportunità effettiva di un nuovo intervento da parte delle autorità europee sulla materia. Sebbene sia evidente, infatti, che l'ecosistema digitale necessiti di una governance stabile e garantista dei diritti e delle libertà degli utenti, la *quaestio* che maggiormente rileva sull'argomento è se sia ragionevole ritenere che lo strumento più adatto a raggiungere tale obiettivo sia la regolazione da parte delle istituzioni o se, al contrario, sarebbe più conveniente prediligere altre vie in un ambiente così fluido e privo di confini.

2. Tra auto-regolazione ed etero-regolazione della governance delle piattaforme

Il dibattito inerente alle più opportune modalità di governance del nuovo fenomeno in oggetto si può riassumere, in questa sede, intorno a due alternative: coloro che ritengono necessario un intervento regolativo *ad hoc* da parte delle competenti autorità pubbliche e chi sostiene, al contrario, che nel contesto virtuale si dovrebbe favorire il fenomeno dell'auto-regolazione già attuato diffusamente dalle piattaforme, ossia la cd. "*deregulation* privata" in quanto più consona, grazie alla capacità di costante aggiornamento, a disciplinare questi nuovi fenomeni di business nonché i cambiamenti sociali in atto[11]. Le due visioni contrapposte si possono definire *regulation up*, nel primo caso, e *deregulating down*, nel secondo.

Presupposto necessario, su cui entrambe le linee di pensiero concordano, è l'idea secondo cui il mercato – *locus artificialis* concreto o virtuale che sia – necessiti di una governance definita, in grado di tutelare i privati e contemperare i diversi interessi al suo interno; di un ordine, dunque, come compromesso tra esigenze economiche e normative[12]. Tale assetto, richiamando una nota dicotomia greca, può costituirsi in due modalità, ovverosia nella forma di *cosmos* o in quella di *taxis*: un ordine spontaneo, endogeno e auto-regolato, non asservito ad alcuna sovranità esterna nel primo caso, ovvero attraverso un'azione esogena ed etero-imposta dall'alto nel secondo[13]. Da tale premessa filosofica si ritorna, dunque, al principale dilemma odierno relativo alla scelta non solo giuridica, ma soprattutto politica, di interventismo nella regolazione del mercato virtuale o di astensione dall'incidere con soluzioni precettive.

Coloro che parteggiano per il *cosmos*, ossia i sostenitori della cd. *deregulation down*, ritengono che le piattaforme siano dotate di un imperio che, di fatto, assume un'ontologia simile a quella delle autorità pubbliche all'interno del mercato digitale; elemento comprovato dall'adozione, da parte di quest'ultime, di efficaci sistemi regolativi interni che risultano in grado di implementarsi autonomamente e costantemente, nonché di adattarsi al dinamismo di tale contesto. In tal modo viene posta ancor più in risalto l'inadeguatezza della normativa in vigore, tacciata di essere obsoleta e, dunque, ostativa al progresso tecnologico.

Le piattaforme, in qualità di cd. «autorità private di fatto»[14], suscitano dunque il giustificato dubbio se l'intervento da parte del regolatore pubblico sia effettivamente la più efficace delle politiche normative da considerare; complice del dilemma il fatto che le logiche sottese alla legislazione pubblica non sempre risultano effettivamente volte al perseguimento del bene collettivo, poiché spesso si assiste, al contrario, a quello che gli studiosi dell'economia sono soliti definire la «cattura del regolatore»[15].

Ulteriore motivazione posta a sostegno di questa visione è il cd. *dilemma di Collingridge*, secondo cui «quando il cambiamento è ancora facile non ne comprendiamo la necessità. Quando il bisogno di un cambiamento è evidente, è ormai difficile e costoso introdurlo», evidenziando che nel rapporto tra legislazione e innovazione il tempo gioca un ruolo fondamentale; l'intervento normativo nelle dinamiche virtuali rischia, infatti, di avanzare sempre ad un ritmo differente rispetto al digitale, ostruendone il progresso[16]. In virtù di quanto espresso, secondo i sostenitori della *deregulation*, la potestà normativa dovrebbe essere delegata interamente ai gestori delle piattaforme, ai quali spetterebbe il compito di creare strumenti volti al proprio controllo interno, dato il loro interesse a tutelare buon andamento e affidabilità dei servizi ivi erogati.

Ciò che non viene ponderato adeguatamente da questa linea di pensiero, tuttavia, è la mancanza di neutralità nelle proprie scelte da parte di queste infrastrutture, le quali tendono a voler imporre il proprio *imperio*, in spregio agli interessi degli *users*. Di conseguenza, l'attribuzione a questi soggetti tecnologici di un potere regolativo così significativo, senza alcun controllo esterno, rischierebbe di pregiudicare gravemente e in modo irreparabile la posizione degli utenti che si interfacciano con tali entità[17].

Ciò nonostante, è pur vero che anche il processo di regolazione fondato esclusivamente sulla *taxis* non ha consegnato risultati finora soddisfacenti nella governance del sistema, soprattutto in ragione dell'antinomia strutturale tra dinamismo digitale e rigidità dei procedimenti legislativi.

Alla luce della situazione attuale, l'Unione europea, deputata alla regolazione del poliedrico fenomeno, nelle recenti proposte normative afferenti al tema, sembrerebbe propensa ad adottare una strategia differente, nel tentativo di superare tutte le questioni delineate: un pacchetto regolativo composto da diversi atti tutti inerenti alla transizione digitale – ad oggi ancora in parte in corso di approvazione – che si strutturerebbe quale soluzione transattiva tra le dicotomiche visioni di *regulation up* e *deregulation down* e, dunque, quale nuova sintesi tra *taxis* e *cosmos*.

Il recente percorso intrapreso dalle istituzioni europee, attraverso il cd. *Digital Package Act*, si connota difatti per una logica regolativa in netta rottura rispetto al passato, in quanto cerca maggiore "dialogo" tra gli strumenti pubblici di regolazione e

quelli privati, dal momento che gli atti normativi sembrano focalizzare la propria attenzione non tanto "all'esterno", quindi sulla comminazione di sanzioni di natura prettamente pubblicistica *ex post*, bensì all'interno, ossia sull'azione stessa del soggetto privato, strutturandosi in forma di procedure di decisione *ex ante*. La conformazione ai dettati normativi rileverebbe, dunque, quale metro della diligenza delle piattaforme, imponendo loro una effettiva responsabilizzazione circa il proprio operato[18].

Le tecniche regolatorie del diritto privato, cd. *private enforcement*, sono chiamate così a coadiuvare in questo contesto l'*enforcement pubblico*, nel tentativo di assicurare maggiore efficienza nella governance del mercato, sensibilizzando gli stessi attori privati rispetto all'impatto collettivo della propria gestione del business[19]. In assenza di un effettivo coinvolgimento degli intermediari, d'altronde, dato il ruolo di protagonisti assoluti da loro acquisito all'interno del mercato, sarebbe pressoché impossibile per il legislatore costituire una governance del sistema efficace, efficiente e ordinata.

3. Gli atti normativi del cd. pacchetto digitale, in una prospettiva oscillante *de iure condito - de iure condendo*

Il cd. pacchetto digitale si compone di una serie di atti normativi il cui obiettivo sarebbe quello di disciplinare le numerose sfaccettature del fenomeno digitale e, dunque, anche la complessa attività attuata dalle piattaforme di intermediazione. È opportuno premettere che fra tutti questi atti sussiste una forte sintonia e comunione di scopi, in ragione del fatto che l'economia delle piattaforme si connota per un'interferenza strutturale tra la circolazione dei beni e quella dei dati personali.

Giova ora dar conto dei principali regolamenti in una prospettiva sincretica *de iure condito - de iure condendo*. Va anzitutto richiamato il Reg. 2016/679/UE (cd. GDPR) in materia di protezione dei dati personali e della loro libera circolazione, il quale – come noto – da una parte ha inteso armonizzare la pregressa normativa in materia, dettando una disciplina unitaria per gli Stati membri e, dall'altra, ha attuato una vera "rivoluzione" nell'architettura della privacy, soprattutto in relazione al cd. approccio al rischio derivante dal trattamento dei dati, prefigurando un impianto di tutele *ex ante* del dato durante la sua circolazione all'interno del mercato digitale[20]. Complice di tale epocale mutamento è la nuova consapevolezza della funzione sociale rivestita oggi dalla privacy, intrinsecamente legata alla dignità, libertà e autodeterminazione informativa dell'individuo[21].

In logica coordinazione con gli obiettivi prescelti, una delle maggiori novità introdotte dal GDPR – ai sensi dell'art. 24 – è la previsione espressa del cd. principio di accountability, che prevede l'obbligo in capo al titolare del trattamento di assumere misure tecniche e organizzative preventive da attuare a garanzia espressa della tutela dei dati personali elaborati[22]. Tale precetto impone poi al titolare di fornire prova esaustiva del rispetto delle prassi da lui prescelte, garantendo così la piena tracciabilità di tutte le operazioni effettuate sui dati.

L'accountability viene configurata quale condizione stessa di legittimità del trattamento, nonché perno della transizione epocale «dalla centralità dell'autodeterminazione dell'interessato alla responsabilizzazione del titolare»; le misure previste da questo principio vengono così erte a capisaldi di una circolazione sicura e vigilata delle informazioni personali sul Web[23]. Il consenso dell'interessato, d'altronde, quale unico strumento a baluardo della tutela della privacy, si è rivelato una strategia spesso sterile, fragile e lacunosa, dal momento che l'utente medio non viene posto nelle condizioni di poter comprendere tutte le implicazioni derivanti dal suo semplice *click* di accettazione al trattamento dei propri dati personali[24].

Come se non bastasse, tale tecnica regolativa, indice di un capovolgimento di prospettiva nell'approccio al rischio, in ragione delle molteplici funzioni ad essa deputate, pare superare l'ambito della protezione dei dati personali in senso stretto, facendo da sfondo – come si vedrà – ad una più ampia disciplina delle piattaforme. Così, infatti, le tracce di questo *modus operandi* sembrano riscontrabili anche nel Reg. 2019/1150/UE attinente alla più incisiva regolazione dei rapporti instaurati tra le piattaforme di intermediazione e il professionista prestatore del servizio sottostante con lo scopo precipuo di garantire maggiore equilibrio nelle relazioni instaurate tra questi soggetti. La novità assoluta del testo in esame riguarderebbe, innanzitutto, la qualificazione giuridica dell'intermediazione digitale, la quale si presenta come sottocategoria con connotati specifici rispetto al più ampio insieme dei "servizi della società dell'informazione", così come declinata nella direttiva 2000/31/CE[25]. Sicché agli intermediari – in ragione del ruolo assunto – vengono imposti nuovi obblighi, anch'essi strutturati *ex ante*, volti alla tutela di trasparenza, equità e "comprensibilità" nella predisposizione dei termini e condizioni d'uso unilateralmente stabiliti, tutto ciò in continuità sia con la logica protettiva che connota la normativa consumeristica che con la strategia normativa prescelta dal GDPR[26].

In una prospettiva *de iure condendo*, invece, è opportuno menzionare, innanzitutto, i due regolamenti gemelli attualmente in corso di approvazione: il *Digital Service Act* - DSA (COM(2020) 825 final, 15 dicembre 2020) e il *Digital Market Act* - DMA (COM(2020) 842 final, 15 dicembre 2020)[27].

Sempre nei limiti consentiti dal discorso, il *Digital Service Act*, chiamato anche "legge sui servizi digitali", si propone un intervento di rinnovamento significativo della direttiva 2000/31/CE[28]. A riguardo, la disciplina che subirà probabilmente un cambiamento radicale rispetto al passato è il regime di responsabilità giuridica degli *Internet service provider* per la diffusione dei contenuti online nei propri siti. Il cambio di paradigma si rende opportuno in virtù della sostanziale inadeguatezza e lacunosità della Direttiva *e-commerce* sia in riferimento al profilo di gestione dei contenuti illegali, sia con riguardo alla distinzione tra i diversi modelli di *hosting provider* presenti sul mercato[29]. Preso atto di tali ragioni di intervento, il Regolamento prospetterebbe una graduazione della responsabilità degli intermediari, a fronte del potere di effettivo controllo esercitato da quest'ultimi sui contenuti caricati dagli utenti: esso prevedrebbe così in capo agli intermediari considerati "attivi", soprattutto se di grandi dimensioni, diversi obblighi di condotta, come la predisposizione di strutture tecnologiche di controllo per la rimozione di contenuti illeciti, ovvero la redazione annuale di rapporti sul grado di rischio dei propri servizi.

Parallelamente al *Digital Service Act*, viene prospettata l'adozione di un altro Regolamento, ossia il *Digital Market Act*, che avrebbe in previsione l'aggiornamento del quadro normativo relativo alla concorrenza nel mercato unico europeo, al fine di contrastare più efficacemente il regime spesso anticoncorrenziale e monopolistico delle *big tech*. L'Unione mirerebbe ad individuare *ex ante*, tramite parametri prestabiliti all'interno del medesimo, i maggiori "aggregatori" digitali – o *gatekeeper* – ossia le piattaforme che operano in qualità di intermediazione per la vendita di prodotti o servizi, con ampio potere sul mercato. Una volta identificati, il testo ambisce ad impedire loro di attuare condotte anticoncorrenziali, non solo mediante le tradizionali misure punitive *ex post*, ma soprattutto attraverso meccanismi di controllo preventivo[30].

Si annovera, infine, la proposta di regolamento sull'intelligenza artificiale (COM(2021) 206 final, del 21 aprile 2021) che si propone di costruire delle fondamenta regolative sicure e stabili per questo settore in forte espansione[31]. In coordinazione con tale prospettiva, la proposta prevedrebbe nuovi obblighi di conformazione *ex ante* per gli operatori coinvolti nella produzione o nell'utilizzo di questi sofisticati software; tali imposizioni verranno in aggiunta adeguate al livello di "rischio" specifico implicato nel sistema di intelligenza artificiale[32].

4. La struttura "responsabilizzante" nella governance delle piattaforme all'interno del cd. pacchetto digitale

Prediligendo un'analisi sistematica dei testi normativi già menzionati, per esigenza di economia del discorso, il primo aspetto che rileva senz'altro evidenziare è che ognuno di essi, seppur sotto angolature differenti, intende tracciare un segno incisivo nel governo della tecnologia e proprio questo obiettivo comune e sotteso ad ogni singolo atto regolativo citato consente di poterli analizzare in modo coordinato, quale parte integrante di un sistema ampio. Così come strutturato, difatti, il nucleo centrale del complesso normativo sembrerebbe essere la creazione di un percorso regolativo teleologicamente orientato verso la "responsabilizzazione" dei gestori dei portali, ai quali viene imposto un ampio novero di obblighi di condotta *ex ante*, differenti e specifici per ogni singolo atto ma, allo stesso tempo, accomunati dal medesimo "approccio al rischio" conforme ad una logica di deterrenza di ogni eventuale pericolo.

Il presupposto giustificativo di tale impostazione si sostanzierebbe, *in primis*, nella necessità di un limite netto al ruolo di assoluta preminenza negoziale rivestito dagli intermediari nel mercato e, in secondo luogo, nella volontà di accordare una garanzia effettiva ai numerosi interessi coinvolti.

I testi normativi citati scelgono così deliberatamente di collocare il proprio baricentro *ex ante* al fine di tentare di gestire i comportamenti dei gestori dei portali sin dal principio: così, la "responsabilizzazione" degli intermediari, declinata come obblighi di comprensibilità, trasparenza, conoscibilità e condivisione, diviene l'asse portante della struttura del governo della tecnologia.

In virtù della *ratio* sottesa a tutti gli atti regolativi menzionati, si evince che gli obblighi conformativi *ex ante*, previsti in diversa misura dalle normative che aderiscono al cd. pacchetto digitale, sono prodromici all'assunzione, da parte delle piattaforme stesse, di precetti interni appropriati alla tutela degli interessi ultra-individuali e sovraordinati implicati nell'attività di intermediazione; corollario di tale aspetto è che la responsabilità di tali soggetti non discende in via esclusiva dagli eventuali danni causati agli utenti, ma soggiace anche all'adeguamento previsto dalle diverse normative[33]. Così, dunque, la regola

imposta dal legislatore europeo «non si risolve (solo) nel limite all'agire negoziale, né postula la (mera) determinazione imperativa del contenuto del contratto: essa, piuttosto, produce un vincolo teleologico, in quanto orienta gli operatori verso quei modelli comportamentali ritenuti idonei ad assicurare un grado di concorrenzialità in senso dinamico del mercato»[34].

Si evince, così, che la normativa digitale – probabilmente per le caratteristiche intrinseche di fluidità e mutevolezza che connotano il panorama di riferimento – prediliga come strategia quella di concentrarsi su strumenti improntati alla deterrenza di qualsiasi eventuale danno, piuttosto che sul rimedio in caso di avvenuta lesione. Una "infrastruttura di tutele" configurata unicamente come sanzione *ex post*, volta alla riparazione dei torti subiti, rischierebbe d'altronde di non accordare effettiva protezione al novero di interessi coinvolti nella complessa dinamica negoziale sin qui descritta.

Al contrario, attraverso la responsabilizzazione degli intermediari ed il loro conseguente coinvolgimento attivo e auspicato contributo produttivo alla gestione del fenomeno, si presume che vi potrà essere più chiarezza nelle logiche del mercato digitale e maggiore equilibrio tra i diversi attori digitali coinvolti, eliminando le numerose asimmetrie presenti nel sistema. La dinamicità che connota i portali potrà essere così asservita alla garanzia di una "protezione elastica" degli utenti, ossia di misure sempre attuali a seconda del mutamento delle circostanze.

In virtù di quanto espresso sin d'ora, non appare casuale, pertanto, che il concetto di accountability sia stato assunto nell'architettura del GDPR a «principio dei principi», giacché la sua osservanza, mediante la predisposizione di apposite procedure, garantisce di rimando il rispetto e la tutela delle altre prescrizioni ivi contemplate[35]. Nel Regolamento 2019/1150/UE tale struttura si appura dalla declinazione degli obblighi imposti alle piattaforme, dal momento che la trasparenza viene configurata quale obbligo proattivo *ex ante* di "essere comprensibile" da parte dei fornitori di servizi di intermediazione. Tale *dictat* fungerebbe dunque da regola deontologica generale imposta agli intermediari per la tutela dell'autodeterminazione effettiva dei soggetti più vulnerabili sin dal momento congenito del *contrahere*[36].

Anche nelle nuove proposte di intervento si trova conferma dello stesso schema, in relazione al fatto che anche in tali contesti normativi ci si interfaccia con la previsione espressa dell'obbligo di adozione di numerosi procedimenti organizzativi *ex ante*, volti alla deterrenza di condotte pericolose o illecite da parte dei principali attori digitali per la creazione di un ambiente digitale affidabile.

Il nuovo modello legislativo si caratterizza, pertanto, per la commistione tra principi comuni e disposizioni tecniche specifiche oltre che per la promozione, da parte del legislatore, dei codici di condotta "interni", ritenuti in grado di contribuire positivamente alla corretta applicazione delle prescrizioni previste nei regolamenti, soprattutto per quanto concerne i diversi regimi di responsabilità delle piattaforme nella propria azione negoziale[37]. Ciascuno di tali elementi, in sintonia con gli altri, è inteso a preservare l'ecosistema digitale, affinché all'interno di esso viga una più sicura e vigilata circolazione combinata tra dati personali e beni o servizi, oltre che una maggiore attenzione ai diritti degli individui coinvolti.

La struttura *de quo* intenderebbe risolvere, in sintesi, le numerose lacune normative presenti, divenendo presidio di quelli che sembrano essere i nuovi principi capisaldi del diritto privato europeo digitale, ossia trasparenza, accountability e proporzionalità.

5. Conclusioni: nuove prospettive giuridiche nella transizione digitale

Riportate le caratteristiche salienti della cd. *platform economy* oltre che le possibili strategie "ordinanti" del fenomeno in questione, si possono offrire delle brevi conclusioni. Il *trait d'union* tra le due opposte visioni di *cosmos* e *taxis*, ovvero *private* e *public enforcement*, può realmente essere una via percorribile per la creazione di una governance maggiormente "fluida", in grado di conciliarsi con le peculiari caratteristiche di a-territorialità e di incorporeità del *World Wide Web*.

Gli atti legislativi afferenti al nuovo pacchetto di riforma digitale, sviluppati in logica coordinazione tra loro dalle Istituzioni europee, potrebbero essere, a ben vedere, l'occasione per una efficace transizione verso differenti frontiere normative, con connotati del tutto originali rispetto agli schemi qualificativi prediletti agli albori dell'esperienza *Onlife*. Viene tracciato, difatti, un percorso regolativo formato da principi reciprocamente condivisi tra i diversi atti normativi, uniti allo sviluppo di una normativa *ad hoc* di settore, propria e peculiare per ognuno dei Regolamenti, i quali, tuttavia, seppur nella propria alterità, presentano comunque dei punti di contatto vicendevoli. Come se non bastasse, la scelta di un comune approccio al rischio condiviso, che si sostanzia fondamentalmente in forme di tutela volte alla deterrenza di ogni forma di lesione dei diritti e delle libertà coinvolte nel panorama digitale, pone ancor più in evidenza l'interferenza sostanziale che lega tutta la regolazione digitale.

La strategia prescelta, volta riassuntivamente alla responsabilizzazione delle piattaforme, si innesta nel solco di un vero e proprio processo "educativo" che tenta, da una parte, di rendere gli intermediari più coscienti dei rischi afferenti al proprio modello di business e, dall'altra, di insignirli quali principali incaricati nella risoluzione delle criticità connesse al loro operato attraverso la continua sperimentazione di misure tecniche o organizzative deputate allo scopo.

Un tale approccio responsabilizzante potrebbe costituire, a ben vedere, anche lo strumento in grado di infondere una "cultura dell'affidabilità" all'interno di tutte le strutture che rientrano nell'alveo dell'ecosistema digitale: si pensi, ad esempio, che grazie all'opera di sensibilizzazione collettiva di tutti i soggetti implicati nella catena del trattamento dei dati, che rende limpidi i rischi implicati in tale operazione, la valutazione e prevenzione degli inerenti pericoli dovrebbe avvenire in modo ben più consapevole, comportando un abbassamento ulteriore del rischio di lesione dei diritti fondamentali coinvolti[38]. Così come per i dati, la medesima sensibilizzazione collettiva giova senza dubbio anche per quanto attiene l'ambito di operatività degli *Internet service provider* ovvero la produzione e utilizzo di sistemi di intelligenza artificiale.

Oltre a quanto espresso, non si dimentichi che nel caso di violazione degli obblighi conformativi previsti sia dalle normative digitali già in vigore sia da quelle in corso di approvazione, sono previste sanzioni fortemente pregiudizievoli per l'operato aziendale; l'assunzione di un atteggiamento proattivo e adeguato diviene, di conseguenza, alquanto conveniente anche per i gestori stessi dei portali di intermediazione.

All'adesione a tali obblighi sono sottesi, pertanto, vantaggi di carattere economico in senso ampio: è agevole constatare come l'implementazione di un approccio responsabilizzato sia in grado di apportare numerosi benefici, sia di natura strettamente commerciale, sia altresì per l'ambiente sicuro che la piattaforma contribuisce così a costruire.

Le aziende più "virtuose" nell'essere "*accountable*" saranno in grado di acquisire maggior credito da parte degli utenti e, di conseguenza, un accrescimento della propria competitività sul mercato. Se posto in essere in modo appropriato ed assennato, quindi, tale "approccio al rischio" è in grado di convertire gli obblighi conformativi da puro costo a preziosa risorsa per i soggetti assoggettati alla disciplina[39].

Ulteriore valutazione *a latere*, circa gli obiettivi sottesi all'approccio, risiede nel fatto che la previsione espressa di uno o più professionisti esplicitamente preposti alla gestione dei differenti trattamenti delineati dai regolamenti sia in grado di consentire uno stabile ponte comunicativo tra controllori e controllati; in tal modo viene notevolmente ampliata la possibilità di instaurazione di un dialogo costruttivo e costante tra questi due soggetti, indispensabile per il raggiungimento di un bilanciamento effettivo tra gli interessi coinvolti.

In conclusione, il sistema che si è venuto a delineare in queste brevi considerazioni potrebbe rappresentare, nel quadro regolativo attuale, la chiave di volta per garantire maggiore contemperamento tra le diverse posizioni in gioco nell'ecosistema digitale: la costituzione della governance digitale diverrebbe appannaggio, dunque, di un lavoro congiunto tra le parti sin d'ora poste agli antipodi, plasmando il futuro digitale entro cardini di un vero dialogo volto al progresso non solo digitale ma anche sociale.

Note

[1]A tal proposito, S. Rodotà, *Il mondo nella rete. Quali diritti, quali vincoli*, Laterza, 2014, p. 3 ss., secondo cui «Internet, il più grande spazio pubblico che l'umanità abbia conosciuto, la rete che avvolge l'intero pianeta, non ha sovrano» e per questo lo spazio regolativo senza confini ammette possibilità impensabili in precedenza. Si consideri anche F. Mastrobernardino, *Il patrimonio digitale*, ESI, 2019, p. 13; il quale richiama a sua volta M. Orlandi, voce *Diritto nel mondo virtuale*, in "Enc. Treccani XXI Sec.", 2009, p. 491, a parere del quale «è consueta e diffusa la lezione secondo cui saremmo nell'età telematica. Epoca delle tecnologie informatiche, capaci di conformare il nostro modo di essere e di costruire mondi interamente digitali, che si raggiungono solo attraverso la macchina elaboratrice e sono attingibili uno tempore ovunque; mondi privi di luogo fisico (atopici), e così suscettibili di compresenza istantanea».

[2]Il termine *Onlife* è stato coniato dal noto studioso L. Floridi e il suo gruppo di ricerca finanziato dalla Commissione europea al fine di sottolineare proprio la fusione ormai inscindibile tra vita reale e dimensione online. Per maggiori dettagli si faccia riferimento a L. Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, 2014, *passim*.

[3]Si fa riferimento all'affermazione di modelli economici come, ad esempio, la cd. *sharing economy* o economia collaborativa fondata in sintesi sulla condivisione di beni tra pari grazie all'utilizzo proficuo delle caratteristiche della rete. Relativamente a tale epocale transizione, causata soprattutto dalle recenti crisi socioeconomiche, nonché ai caratteri salienti dell'economia collaborativa si legga J. Rifkin, *L'era dell'accesso. La rivoluzione della new economy* (trad. it.), Mondadori, 2000, *passim*; Id., *La società a costo marginale zero. Internet delle cose, l'ascesa del commons collaborativo e l'eclissi del capitalismo* (trad. it.), Mondadori, 2014, *passim*; Y. Benkler, *Sharing Nicely: On Shereable Goods and the Emergence of Sharing as a Modality of Economic Production*, in "Yale Law Journal", vol. 114, 2004, n. 2, p. 273 ss.; R. Botsman, R. Rogers, *Il consumo collaborativo ovvero quello che è mio è anche tuo* (trad. it.), Franco Angeli, 2017, p. 15 ss.; per quanto riguarda, invece, la dottrina nazionale, trattano del tema D. Pellegrini, *Sharing Economy. Perché l'economia collaborativa è il nostro futuro*, Hoepli, 2017, *passim*; G. Smorto, *Economia della condivisione e antropologia dello scambio*, in "Diritto pubblico comparato ed europeo", 2017, n. 1, p. 119 ss.; Id., *Dall'impresa gerarchica alla comu-*

nità distribuita, in "Orizzonti del Diritto Commerciale", 2014, n. 3, p. 1 ss.; Id., *Verso la disciplina giuridica della Sharing economy*, in "Mercato concorrenza regole", 2015, n. 2, p. 246 ss.; ancora, N. Rampazzo, *Rifkin e Uber. Dall'età dell'accesso all'economia dell'eccesso*, in "Il diritto dell'informazione e dell'informatica", 2015, n. 1, p. 957 ss.

[4]La piattaforma, in estrema sintesi, è un'infrastruttura informatica articolata, composta da un sistema hardware associato ad uno software che ne presiede tutte le funzionalità: tale sistema è in grado di fornire simultaneamente differenti servizi presunti gratuiti o a pagamento. Può essere strutturata secondo uno schema open source oppure commerciale; oltre a ciò, può essere riferita ad un pubblico indeterminato o, al contrario, rivolta ad un certo target di utenti. La presunzione di gratuità viene talvolta superata dal fatto che solo il software o la funzione base del servizio sia completamente gratuita e, al contrario, le funzioni più sofisticate siano a pagamento. In tal caso si parla di remunerazione indiretta o mista, cd. *freemium*. Per una ricostruzione più attenta R. Moro Visconti, *La valutazione delle piattaforme digitali*, in "Diritto industriale", 2020, n. 4, p. 371 ss.

[5]Nel quadro normativo vigente, tali servizi sembrerebbero riconducibili alla disciplina dei "servizi della società dell'informazione", ai sensi della direttiva 2000/31/CE e definiti, oggi, dall'art. 1 lett. b), della direttiva 2015/1535/UE come: «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi». L'intermediazione, difatti, non attiene di per sé alla gestione materiale delle risorse e alla loro allocazione trattandosi, al contrario, di un servizio erogato esclusivamente online. Di conseguenza, il contratto attinente al servizio sottostante viene concluso esclusivamente tra gli utenti secondo uno schema *peer to peer* e le piattaforme tendono a declinare ogni responsabilità in relazione ad esso. L'inquadramento giuridico appena esposto, tuttavia, non rispecchia il ruolo concretamente rivestito, dal momento che le piattaforme tendono spesso a soverchiare la propria funzione formale. Per un'accurata analisi del ruolo svolto dalle piattaforme di intermediazione si osservino A. Quarta, *Il ruolo delle piattaforme digitali nell'economia collaborativa*, in "Contratto e Impresa. Europa", 2017, p. 554 ss.; A. Canepa, *I mercanti nell'era digitale. Un contributo allo studio delle piattaforme*, Giappichelli, 2020, *passim*.

[6]Si fa riferimento soprattutto alla direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»). Essa è stata recepita nell'ordinamento italiano con il d.lgs. 9 aprile 2003, n. 70.

[7]Così fanno eco le parole di N. Irti, *Scambi senza accordo*, in "Rivista trimestrale di diritto e procedura civile", 1998, n. 2, p. 346 ss. Sebbene lo scritto si collochi in un arco temporale in cui nello specifico l'azione degli intermediari digitali fosse lungi dall'essere immaginabile da parte dell'Autore, lo scritto risulta ancora fortemente attuale in termini sostanziali. Questa autorevole voce descrive uno spazio contrattuale spersonalizzato in cui sostanzialmente la tecnica dialogica, fulcro stesso del *contrahere*, diviene pressoché irrilevante, laddove viene prediletto, al contrario, l'imporsi "di un monologo" di una parte in modo tale che «il rapporto guadagna un alto grado di efficienza e calcolabilità» dal momento che «lo schema è ripetibile senza fine, evita sperperi di tempo e di energia, annulla o riduce gli attriti dell'individualità». È evidente, difatti, che «la parte che adotta moduli o formulari, rifiuta e nega il dialogo: non fa e non riceve domande, non dà e non attende risposte o, meglio, fa un'unica domanda e attende un'unica risposta. Essa ha già esaurito la sua risposta comunicativa, ma, appunto, in un'espressione che consuma e annulla il dialogo. L'aderire non è un risultato dialogico, ma – come rivela l'etimo latino – soltanto un rimanere attaccati».

[8]Si consideri, V. Katz, *Regulating the Sharing Economy*, in "Berkeley Technology Law Journal", vol. 30, 2015, n. 4, p. 1067 ss. L'Autrice delinea come le piattaforme, soprattutto nell'ambito della *sharing economy*, esercitino un controllo effettivo sulle modalità di erogazione dei servizi nonché su ogni transazione che si compie al loro interno.

[9]Riguardo alle inedite dinamiche derivanti da questa combinazione tra fornitura di un servizio e utilizzo dei dati, si osservino i contributi di C. Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in "Giustizia civile", 2019, n. 3, p. 499 ss., là dove l'Autrice, nel trattare i contenuti della novella disciplina, evidenzia chiaramente come i modelli contrattuali e di scambio stiano subendo notevoli cambiamenti in ragione del fatto che i dati personali sono divenuti nell'economia delle piattaforme la nuova moneta; sulla stessa linea, C. Camardi, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, in "Jus civile", 2021, n. 4, p. 870 ss. Si veda anche sul punto V. Zeno-Zencovich, *Do 'Data Markets' Exist?*, in "Media Laws", 2019, n. 2, p. 22 ss.; si considerino, infine, i recenti articoli di M.W. Monterossi, *La tutela dell'utente commerciale nei mercati digitali*, in "Contrato e impresa", 2021, n. 3, p. 920 ss.; T. Schrepel, *Platforms or Aggregators: Implications for Digital Antitrust Law*, in "Journal of European Competition Law & Practice", vol. 12, 2021, n. 1, p. 1-3.

[10]Intento principale della direttiva sul commercio elettronico, infatti, era quello di costituire un quadro giuridico in grado di assicurare la libera circolazione dei servizi della società dell'informazione tra gli Stati membri, favorendo lo sviluppo di questo strategico settore. Il progetto comunitario della direttiva si poneva l'obiettivo di incentivare la realizzazione di una società consapevole delle nuove possibilità garantite dall'avvento delle tecnologie e una trasformazione omogenea verso la cd. società dell'informazione. Viene assunto a postulato dell'introduzione della direttiva 2000/31/CE l'obiettivo di armonizzazione delle normative e la creazione di uno spazio senza frontiere, oltre che la creazione di un quadro generale chiaro sugli aspetti giuridici del commercio elettronico nel mercato interno. Per un commento recente e compiuto della direttiva si consideri F. Delfini, *Forma digitale, contratto e commercio elettronico*, UTET, 2020, p. 95 ss. Per cosa si intenda, invece, per società dell'informazione in termini più socio-tecnologici, si consideri M.A. Biasiotti, G. Sartor, F. Turchi, *Tecnologie e abilità informatiche per il diritto*, Giappichelli, 2018, p. 17 ss.

[11]Si faccia riferimento, ad esempio, a M. Orlandi, *Autonomia privata e autorità indipendenti*, in G. Gitti (a cura di), "L'Autonomia privata e le autorità indipendenti", il Mulino, 2006, p. 69 ss.

[12]L'ordine nel mercato viene inteso da autorevole dottrina come «regolarità e prevedibilità dell'agire: chi entra nel mercato – nel mercato di un dato bene – sa che l'agire, proprio e altrui, è governato da regole, e dunque che, entro la misura definita da codeste regole, i comportamenti sono prevedibili». Così, N. Irti, *L'Ordine giuridico del mercato*, Laterza, 1998, p. 5.

[13]Tratta profusamente di questa dicotomia N. Irti, *L'Ordine giuridico del mercato*, cit., p. 6 s.

[14]Il concetto di «autorità private di fatto» richiama immediatamente C.M. Bianca, *Le autorità private*, Jovene, 1977, p. 55 ss. A più di 40 anni dalla sua pubblicazione, questo saggio mostra ancora grande attualità riguardo alla riflessione sull'incidenza del potere privato sia «di diritto» che meramente «di fatto» nei rapporti tra consociati nonché sulle tecniche a disposizione dell'ordinamento giuridico per la tutela di in-

teressi generali, collettivi e individuali. Questa prospettiva d'indagine che invita ad uno sguardo meno rigido rispetto alla classica lettura che sovente contrapponeva nettamente un diritto privato dell'eguaglianza a un diritto pubblico dell'autorità, si intreccia in modo significativo con le più recenti analisi del «diritto della regolazione» e la compenetrazione di tecniche pubbliche e private».

[15]Sul punto si richiama la nota scuola di pensiero *Public Choice* o della scelta pubblica sviluppatasi negli Stati Uniti negli anni '60 del 900, principalmente ad opera di J.M. Buchanam, premio Nobel per l'economia nel 1986, e Gordon Tullock. Il saggio, intitolato "Il calcolo del consenso", pubblicato nel 1962, dimostra come i politici non siano affatto benevoli monarchi illuminati che perseguono prioritariamente il benessere collettivo ma, al contrario, attori razionali guidati soprattutto da interessi egoistici. Si veda a riguardo J.M. Buchanam, G. Tullock, *The Calculus of Consent, Logical Foundations of Constitutional Democracy*, University of Michigan Press, 1962, *passim*; per un commento si consideri anche E. Graziani, *Il mercato tra diritto e economia e politica*, Giappichelli, 2005, p. 77 ss. Di conseguenza, il desiderio che muove i politici nelle proprie campagne elettorali è tutt'altro che improntato verso un sentimento di bene collettivo ma alla soddisfazione di interessi prettamente individuali. In ragione di ciò, si può scorgere da parte del legislatore una maggiore benevolenza verso gli interessi degli attori più forti del mercato, i quali, dunque, sono in grado *de facto* di "catturare il regolatore". La teoria è stata elaborata compiutamente dal premio Nobel per l'economia, George J. Stiegler, aderente anch'egli alla linea di pensiero elaborata dalla *Public Choice*. Si veda a riguardo: G.J. Stiegler, *Mercato, informazione, regolamentazione* (trad. it.), il Mulino, 1994, *passim*.

[16]Il cd. *dilemma di Collingridge* prende dal proprio ideatore, David Collinridge, il quale nel libro *The Social Control of Technology*, demarca proprio l'antitesi tra le due velocità. Questa teoria è collegata strettamente al cd. problema del ritmo, teorizzato dallo studioso Larry Downes nel 2009 nel proprio libro *The Laws of Disruption, Harnessing the New Forces that Govern Life and Business in the Digital Age*, in cui afferma che, mentre la tecnologia si modifica in modo esponenziale, i sistemi giuridici ed economici cambiano progressivamente, evidenziando la differente speditezza a cui tali entità si muovono e la conseguente difficoltà di comunicazione. Così, D. Collinridge, *The Social Control of Technology*, St. Martin's Press, 1980, *passim*; L. Downes, *The Laws of Disruption, Harnessing the New Forces that Govern Life and Business in the Digital Age*, Basic Books, 2009, *passim*.

[17]Cfr. V. Zeno-Zencovich, *Uber: modello economico e implicazioni giuridiche*, in "MediaLaws", 2018, n. 1, pp. 140-143.

[18]Sul punto M. Maugeri, *Funzioni del diritto privato e tecniche di regolazione del mercato*, in M. Maugeri, A. Zoppini, "Funzioni del diritto privato e tecniche di regolazione del mercato", il Mulino, 2009, p. 9 ss.; A. Zoppini, *Una riflessione sul contratto nell'attuale diritto del commercio internazionale*, in "Rivista critica del diritto privato", 2020, n. 1, pp. 291-294.

[19]Sulla cooperazione tra *private* e *public enforcement* nella prospettiva della regolazione del mercato concorrenziale si considerino M. Maugeri, A. Zoppini, *op. cit.*; A. Zoppini, *Una riflessione sul contratto nell'attuale diritto del commercio internazionale*, cit.; G. Muscolo, *Il nuovo assetto istituzionale del private antitrust enforcement in Italia e nell'Unione europea: la cooperazione tra public e private enforcement*, in G.A. Benacchio, M. Carpagnano (a cura di), "Assetti istituzionali e prospettive del private antitrust enforcement nell'Unione europea", Editoriale Scientifica, 2018, p. 11 ss.

[20]Per un'analisi approfondita dei contenuti del GDPR, si faccia riferimento, *ex multis*, a R. Caterina, *Novità e continuità nel Regolamento generale sulla protezione dei dati*, in "Giurisprudenza italiana", 2019, n. 12, p. 2777; G. Finocchiaro, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in "Quaderni costituzionali", 2018, n. 4, pp. 895-898; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016, *passim*; Id., *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Giappichelli, 2016, passim; E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in "Contratto e impresa", 2018, n. 1, pp. 106-125.

[21]Così, M.G. Stanzione, *Consenso e trattamento di dati personali nella dimensione europea*, in P. Stanzione (a cura di), "I poteri privati delle piattaforme e le nuove frontiere della privacy", Giappichelli, 2022, p. 77 ss.

[22]Sul punto C. Camardi, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in "Jus Civile", 2020, n. 3, pp. 786-811; G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in "Le nuove leggi civili commentate", 2017, n. 1, pp. 1-18; sul concetto di accountability nel GDPR si osservi anche G. Amore, *Fairness, Transparency e Accountability, nella protezione dei dati personali*, in "Studium Iuris", 2020, n. 4, pp. 414-429. Spetta, dunque, al titolare valutare la portata del pericolo e prevenirne i possibili effetti pregiudizievoli mediante puntuali accorgimenti in via cautelativa di cui deve poter dare costantemente prova.

[23]Si riprende E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, 2019, p. 34 ss.; si veda anche Id., *La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR)*, in "Studium Iuris", 2020, n. 7-8, pp. 840-845. Così, anche, G. Busia, L. Liguori, O. Pollicino, *Nota introduttiva*, in Id. (a cura di), "Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive", Aracne, 2016, p. 12 ss.

[24]Per una trattazione circa la disciplina del consenso e annesse questioni si rimanda a E. Lucchini Guastalla, *Privacy e Data Protection: principi generali*, in E. Tosi (a cura di), "Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo codice privacy", Giuffrè, 2019, p. 71 ss.; L. Aulino, *Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come un rimedio ex ante*, in "Il Diritto dell'informazione e dell'informatica", 2020, n. 2, pp. 303-312.

[25]La nuova fattispecie evidenzia, da una parte, le caratteristiche attinenti alla struttura e, dall'altra, sottolinea quali siano le modalità di conduzione del business. Nello specifico, ai sensi dell'art. 2 n. 2) del Regolamento, si definiscono servizi di intermediazione online quelli che soddisfano i tre seguenti requisiti: «a) sono servizi della società dell'informazione ai sensi dell'art. 1, par. 1, lett. b della direttiva 2015/1535/UE del Parlamento europeo e del Consiglio; b) consentono agli utenti commerciali di offrire beni o servizi ai consumatori, con l'obiettivo di facilitare l'avvio di transazioni dirette tra tali utenti commerciali e i consumatori, a prescindere da dove sono concluse dette transazioni; c) sono forniti agli utenti commerciali in base a rapporti contrattuali tra il fornitore di tale servizi, da un lato, e gli utenti commerciali e i consumatori a cui gli utenti commerciali offrono beni o servizi, dall'altro». Per un commento approfondito al nuovo regolamento A. Palmieri, *Profili giuridici delle piattaforme digitali*, Giappichelli, 2019, p. 32 ss.

[26]Alla luce di ciò, l'art. 3 del Regolamento 2019/1150/UE – dedicato in modo esplicito proprio a "Termini e Condizioni" unilateralmente predisposte dai gestori di piattaforme di intermediazione – indica in modo puntuale le misure a cui tali soggetti sono tenuti a conformarsi al fine di assicurare traspa-

renza in ogni fase della contrattazione con gli utenti che si interfacciano nel portale.

[27]Per un primo commento sui contenuti della riforma si considerino, G.M. Ruotolo, *Digital Service Act e Digital Market Act: tra responsabilità dei fornitori e rischi di bis in idem*, in "SIDIblog", 29 marzo 2021; Id., *Le proposte di disciplina di digital service e digital markets della Commissione del 15 dicembre 2020*, in "DPCE online", 2020, n. 4, pp. 5419-5421. Si segnalano nelle due proposte i seguenti macro-profili di intervento: «- norme specifiche per le grandi piattaforme digitali che svolgono una funzione sistemica di controllo di accesso al mercato; - rafforzamento della protezione per i consumatori dai prodotti illegali, contraffatti e non sicuri; - regole più incisive per pubblicità mirata e controlli su contenuti online; - obbligatorietà delle norme introdotte anche per i prestatori stranieri di servizi» Così, E. Tosi, *Diritto privato delle nuove tecnologie digitali*, Giuffrè, 2021, p. 39.

[28]Per un'analisi delle prospettive di riforma si osservi C. Camardi, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, cit., p. 907 ss.; si consideri, inoltre, M. Eifert, A. Metzger, W. Schweitzer, G. Wagner, *Taming the giants: the DMA/DSA package*, in "Common Market Law Review", vol. 58, 2021, n. 4, p. 987-1028; O. Pollicino, G. De Gregorio, *Verso il Digital Service Act: problemi e prospettive. Presentazione del simposio*, in "MediaLaws", 23 novembre 2020; M. Donateo, A. Polimeni, *Digital Service Act, verso un nuovo modello di responsabilità per i social: i primi passi Ue*, in "Agenda digitale EU", 22 giugno 2020; N. Pisanu, *Ecco il Digital Service Act: perché è rivoluzionaria la proposta della Commissione UE*, in "Cibersecurity360", 15 dicembre 2020; F. Paoluci, *Il Digital Service Act: verso una nuova governance di Internet?*, in "Ius in Itinere", 23 dicembre 2020. Rispetto alla sua approvazione, F. Meta, *Digital Service Act, ok del Parlamento Ue: stretta su contenuti e algoritmi*, in "Corcom", 20 gennaio 2022.

[29]Gli *Internet service provider* tradizionalmente venivano configurati all'interno della direttiva 2000/31/CE come "servizi della società dell'informazione" il cui operato si limitava alla garanzia di accesso ad una rete di comunicazione ed erano ritenuti privi di responsabilità alcuna circa i contenuti pubblicati nei propri canali da parte degli utenti. Così, ai sensi degli artt. 13, 14, 15 della suddetta Direttiva, qualora l'attività del *provider* sia definibile in termini di *access*, *cache* o *host*, e dunque connotata da mero tecnicismo, automatismo nonché passività, viene disposta l'assenza di un obbligo specifico di sorveglianza a carico di questi soggetti in ragione del fatto che essi vengono ritenuti inidonei ad un controllo effettivo dei contenuti pubblicati, data la loro natura formalmente "passiva". Lo sviluppo della cd. *platform economy* ha determinato, tuttavia, un'evoluzione significativa anche nell'attività di *hosting* rispetto a come inizialmente concepita che ha sollevato negli anni numerose contese giudiziali, all'interno delle quali si è fatta spazio una debita distinzione nella formulazione interpretativa soggettiva del *provider* ossia tra cd. *hosting* passivo e attivo. I cd. *host* attivi non presentano di certo le caratteristiche di passività e neutralità delineate dalla normativa comunitaria, non potendosi considerare, di conseguenza, scevri da qualsivoglia responsabilità ma, al contrario, co-responsabili. In particolare, si vedano le seguenti sentenze della Corte di Giustizia europea che hanno delineato la differenza tra hosting passivo e attivo, CGUE, C-236/08, 23 marzo 2010, *Google v. Luis Vuitton*; nello stesso senso CGUE, C-324/09, 12 luglio 2011, *L'Oreal v. eBay*. Il dibattito in dottrina sul punto è molto vivace, per maggiori dettagli sulla questione si considerino, *ex multis*, A.G. Parisi, *Privacy e mercato digitale*, Pacini Giuridica, 2020, p. 155 ss.; R. Petruso, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, Giappichelli, 2019, *passim*; E. Tosi, *L'evoluzione della responsabilità civile dell'Internet service provider passivo e attivo*, in "Diritto industriale", 2019, pp. 590-613; Id., *Obblighi di filtraggio ex post di contenuti digitali illeciti equivalenti e responsabilità civile degli hosting provider*, in "Diritto industriale", 2020, pp. 284-298; Id., *Diritto privato*, cit., p. 447 ss.

[30]Per maggiori dettagli si veda il documento informativo della Commissione europea intitolato *Legge sui mercati digitali: garantire mercati digitali equi e aperti*. Per un breve commento alla proposta M.R. Carbone, *Digital Market Act: così l'Europa limita il potere delle Big Tech*, in "Agenda digitale EU", 15 dicembre 2020.

[31]Si fa riferimento alla nuova proposta legata alla normazione dell'AI recante titolo *Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale e che modifica alcuni atti legislativi dell'Unione*, pubblicato il 21 aprile 2021.

[32]Per un primo breve commento alla proposta, L. Tosoni, *Intelligenza artificiale, i punti chiave del regolamento europeo*, in "Agenda digitale EU", 21 aprile 2021; F. Giordanelli, A. Chiarini, *Il regolamento sull'intelligenza artificiale: "essere o non essere" intelligenza artificiale*, in "Media Laws", 3 marzo 2022.

[33]Così, in relazione alla disciplina della privacy, C. Camardi, *Note critiche*, cit., p. 796.

[34]Si riprende A. Zoppini, *Il diritto privato e i suoi confini*, il Mulino, 2020, p. 193 ss., al quale si rinvia per più ampie riflessioni sistemiche.

[35]Si tenga presente quanto riportato in particolare da R. Celella, *Il principio di responsabilizzazione: la vera novità del GDPR*, in "Ciberspazio e diritto", 2018, n. 1-2, pp. 211-224; C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in "Federalismi.it", 2018, n. 22, p. 26 ss.; L. Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. Califano, C. Colapietro (a cura di), "Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679", Editoriale Scientifica, 2017, p. 35; L. Califano, *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, in L. Scaffardi (a cura di), "I profili del diritto. Regole, rischi e opportunità nell'era digitale", Giappichelli, 2018, p. 1 ss.

[36]L'imperativo della trasparenza contrattuale, obiettivo centrale anche del Codice del consumo, impone chiaramente una contribuzione attiva da parte di coloro che si trovano in una situazione di vantaggio nel mercato. Per maggiori dettagli sulla sua funzione nei rapporti asimmetrici si considerino, ad esempio, M. De Poli, *Asimmetrie informative e rapporti contrattuali*, Cedam, 2002, *passim*; F. Rende, *Informazione e consenso nella costruzione del regolamento contrattuale*, Giuffrè, 2012, *passim*.

[37]Così, ad esempio, l'art. 24, co. 3, del GDPR individua nell'«applicazione dei codici di condotta approvati ai sensi dell'art. 40» un ulteriore strumento funzionale all'incentivo dell'autodisciplina dei soggetti preposti al trattamento, come pure un irrobustimento delle fonti legislative interconnesse preposte a tale scopo. Anche nelle nuove proposte, inoltre, viene sponsorizzata la loro adozione; così, l'art. 35, co. 1, del DSA recita «La Commissione e il comitato incoraggiano e agevolano l'elaborazione di codici di condotta a livello di Unione per contribuire alla corretta applicazione del presente regolamento, tenendo conto in particolare delle sfide specifiche connesse alla lotta di diversi tipi di contenuti illegali e ai rischi sistematici, conformemente al diritto dell'Unione, in particolare in materia di concorrenza e protezione dei dati personali».

[38]Cfr. L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, 2016, p. 82 ss.

[39]Sul punto Id., *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, cit., p. 10; R. Celella, *op. cit.*, p. 223. Sul concetto di privacy da "costo a risorsa", ben prima del Regolamento attualmente vigente si vedano i diversi contributi contenuti in G. Rasi (a cura di), *Da costo a risorsa. La tutela dei dati personali nelle attività produttive*, p. 7 ss.

* * *

The regulatory evolution of digital intermediation: new profiles of accountability

Abstract: This article aims to investigate the development of digital intermediation platforms and their remarkable impact on the governance of the digital ecosystem; secondly, the paper aims to identify new legal protection tools for users in a *de iure condito - de iure condendo* perspective. Intermediation platforms proved to be complex to be qualified in legal terms, due to their "fluid" nature, both in structure and services. They play an important role in the borderless digital market: platforms, indeed, have been gaining a position of strength in negotiation relationships with users. Such a situation is cause of substantial asymmetry between parties to the prejudice of the user's rights involved. The EU legislation of the sector is a contributing factor in the current situation as it often regarded as outdated and so unable of governing such a phenomenon, which give raise to many doubts about the reasonableness of a new regulatory intervention of the European Institutions on the matter. Considering this, the paper will consider how new regulatory techniques, such as accountability, provided for by the new European regulatory text and proposals about the technological issue, might or not contribute to build a more transparent and secure governance of the digital ecosystem.

Keywords: Platforms – Intermediation – Governance – Accountability

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0075
Articolo sottoposto a peer review

Il paradosso di Nakamoto: utilità attese e pericoli potenziali di un impiego istituzionale della tecnologia *blockchain*

Marco Rhao

Il contributo, eleggendo la rosa di sperimentazioni amministrative italiane in ambito *blockchain* quale proprio laboratorio euristico, proverà a rappresentare (in prospettiva giuspubblicistica) le principali ricadute dell'impiego pubblico di questa tecnologia sulla vita del cittadino, come dello Stato apparato, sempre più investiti dal portato trasformativo della quarta rivoluzione industriale. Ci si propone, in tal senso, di evidenziare tanto le possibili utilità connesse ad un utilizzo istituzionale della *blockchain*, quanto i pericoli di cui la stessa parrebbe essere foriera.

Blockchain – Pubbliche amministrazioni – Stato – Anarcocapitalismo – Amministrazione digitale

Sommario: *1.* Blockchain *e comunità* Cypherpunk*: storia di un binomio – 2. Alcune note di contesto – 3. Le sperimentazioni italiane – 4.* Blockchain*: utilità attese di una tecnologia – 5.* Blockchain*: i pericoli potenziali di un impiego istituzionale di questa tecnologia – 6. Alcune riflessioni conclusive*

1. *Blockchain* e comunità *Cypherpunk*: storia di un binomio

La quarta rivoluzione industriale, teorizzata da Klaus Schwab nell'omonimo volume del 2016[1], sta rapidamente inducendo istituzioni, imprese e individui a ridefinire il proprio modo di interagire con gli altri attori sociali, nonché a rideterminare la propria collocazione in seno alla società stessa.

In un simile scenario, la ricerca di strumenti tecnologici e telematici sempre più performanti si dimostra fattore condizionante e, al contempo, variabile condizionata di questo processo trasformativo. L'uomo, inteso quale pubblico decisore, pubblico funzionario, imprenditore o cittadino è messo dinnanzi ad una scelta: affrontare simili tecnologie (tentando di comprendere pro e contro derivanti dal loro utilizzo) o rifuggire da simili manifestazioni del presente (restando ai margini della "tela relazionale" di cui si compone il "ritratto della realtà sociale").

Questo lavoro trova nel dilemma appena rappresentato la propria ragion d'essere. In particolare, lo spettro d'indagine si attesterà lungo il perimetro giuridico dell'impiego istituzionale della tecnologia *blockchain* «sulla quale, da più parti, si scommette per realizzare un significativo salto di livello nell'efficienza organizzativa di molte parti del settore pubblico e privato»[2].

Le *blockchain*, o catene di blocchi, si configurano quali registri distribuiti (o *distributed ledger* "DLT") che, attraverso specifici protocolli crittografici, mirano allo scambio di informazioni e contestuale archiviazione delle prefate operazioni, attraverso la rete dei registri, la cui peculiarità risiede nella loro in-

M. Rhao è dottorando di ricerca in Economia e finanza delle amministrazioni pubbliche; cultore della materia in Diritto pubblico presso l'Università degli Studi di Bari "Aldo Moro".

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

trinseca capacità di autenticazione dell'effettiva sussistenza di un dato trasferimento di informazioni, pur operando in assenza di un "soggetto certificatore istituzionale"[3]. Le informazioni, al momento del loro caricamento in una *blockchain*, sono allocate, a seguito di un processo crittografico asimmetrico, in blocchi «accompagnati dal meccanismo di *hashing* e della marcatura temporale»[4]. Quanto al primo, con meccanismo di *hash* ci si riferisce ad una specifica categoria di «algoritmi per la traduzione matematica di dati di lunghezza arbitraria in un codice alfanumerico fisso. Elementi essenziali per la sicurezza informatica, le funzioni di *hash* devono avere, da un lato, la caratteristica di produrre in uscita il medesimo codice al ricorrere della medesima stringa di dati, ma, dall'altro, quella di non offrire la possibilità di risalire dalla stringa in uscita ai dati di partenza»[5]. Grazie a questa equazione è possibile «collegare ciascun blocco a quello precedente, per mezzo del richiamo all'*hash* del blocco precedente in quello successivo, mentre la marcatura temporale (c.d. *timestamping*) associa data e ora certe e legalmente valide ad un documento informatico, permettendo una validazione temporale del documento opponibile a terzi»[6].

La prima catena di blocchi fu presentata al grande pubblico da Satoshi Nakamoto il 31 ottobre 2008. Nakamoto formulò, attraverso il *white paper* "*Bitcoin*: un sistema di moneta elettronica *peer-to-peer*", la sua idea di *blockchain*, immaginando un utilizzo della stessa per la creazione di una "cryptovaluta" nonché del mercato funzionale al suo scambio. Questa idea si poneva in continuità con tutta una serie di precedenti iniziative in materia di software crittografico opensource, maturate (nell'ultimo decennio del XX secolo) in seno agli orizzonti tecnologici offerti dalla *new economy*[7]. Un fermento, tanto di natura industriale quanto accademica, divenuto il terreno di coltura privilegiato di un controverso fenomeno sociale: la comunità "cypherpunk".

Cypherpunk è un'espressione nata all'inizio degli anni Novanta, atta a definire una specifica subcultura «che intendeva richiamarsi, con un pizzico di ironia, al più conosciuto movimento *cyberpunk*. Se i *cyberpunk* si proponevano come eredi dell'antagonismo radicale (*punk*) potenziati da un uso critico quanto massiccio delle nuove tecnologie (*cyber*), i *cypherpunk* sono portatori di una visione più specifica»[8]. Le tecnologie in uso a questa "generazione *punk* 3.0" sono quelle inerenti alla dimensione crittografica: *cypher* in inglese significa cifrario, mentre il verbo *to cypher* sta ad indicare l'atto del crittografare. La visione *cypherpunk*, efficacemente rappresentata da alcuni celebri manifesti ancora oggi presenti sul Web[9], «non si limita a reclamare un minore controllo statale sugli strumenti crittografici, ma ne programma esplicitamente la completa eliminazione»[10]. I *cypherpunk* propongono la fine dei sistemi fiscali nazionali attraverso la migrazione di tutte le transazioni economiche sulla rete, che risulta in grado di garantire l'anonimato degli attori economici. Va da sé che al collasso del controllo statale sui flussi di ricchezza consegue l'intrinseca incapacità delle istituzioni di garantire la copertura del fabbisogno economico della propria "macchina amministrativa" (*rectius* della propria sussistenza in seno alle comunità umane da esse governate).

Questo movimento, anche definito come *cryptoanarchism*, pur condividendo parzialmente i fini dell'azione militante dei propri "ascendenti *cyberpunk*", risulta discostarsi dal patrimonio culturale "antagonista" di questi ultimi. Nonostante il loro dichiararsi anarchici, la variegata compagine *cypherpunk* assunse, ed assume tutt'ora, quale *humus* culturale di riferimento il liberismo economico assoluto, qualificandosi come proiezione cybernetica del movimento anarcocapitalista.

Oggi, entro questa subcultura, sono fatti rientrare tanto il gruppo di accademici e professionisti dell'industria tecnologica che animano il tessuto economico-culturale della Silicon Valley, quanto un movimento più generale che, eleggendo quale privilegiato campo d'azione il World Wide Web, condivide e sostiene l'uso degli strumenti di crittografia per sottrarsi al controllo statale.

Il movimento *cypherpunk* si presenta fortemente caratterizzato da una fiducia nelle potenzialità della ricerca in ambito tecnologico, declinata entro una prospettiva euristica antistatalista. L'ambiente *cypher* fonda la propria esistenza sulla «vasta collaborazione internazionale per lo sviluppo di nuovo software crittografico libero e gratuito» e si fa portavoce di un «conflitto che, mettendo in discussione l'autorità dello Stato, investe la struttura del sistema in cui prende forma»[11].

Entro questo perimetro politico-informatico emerge il lavoro di Satoshi Nakamoto. Tuttavia, da quel 31 ottobre 2008, molta strada è stata percorsa dal bitcoin, ed ancor più dalle catene di blocchi su cui lo stesso fonda il proprio funzionamento. Queste ultime, infatti, nate come un mero precipitato fattuale di un modello matematico, in grado di affascinare uno sparuto drappello di specialisti dell'ICT o gli affiliati di poche "comuni cybernetiche", hanno rappresentato un "silicon swan"[12] per buona parte del tessuto industriale globale, generando (financo in sede istituzionale) un crescente e diffuso interesse per i possibili impieghi pubblici della *blockchain*.

2. Alcune note di contesto

La ricerca di margini di applicabilità politica delle catene di blocchi ha portato alcuni legislatori ad attivarsi in prospettiva nomopoietica nel governo di tali nuove risorse informatiche. Nel solco di questo interesse istituzionale per la *blockchain*, il contributo (identificando quale proprio laboratorio concettuale il caso italiano) affronterà alcune di queste "catene di Stato" (tanto in prospettiva teorico-giuridica quanto in termini politico-organizzativi), i margini di loro successo e le criticità ad esse associate.

A tal fine, pare opportuno approfondire l'iter con cui la *blockchain* è progressivamente entrata a far parte dell'agenda politica delle istituzioni eurounitarie e nazionali. Giova, in tal senso, ricordare come il Servizio di ricerca del Parlamento europeo, nel febbraio 2017, attraverso il report *How blockchain technology could change our lives* evidenziò la potenziale applicazione delle catene di blocchi nella tenuta della documentazione amministrativa, riferendosi specificatamente ai registri pubblici deputati alla conservazione dei certificati catastali, di nascita e delle licenze commerciali. Gli autori rimarcarono la capacità di questa tecnologia di creare e verificare dei record, con un maggiore livello di velocità, sicurezza e trasparenza rispetto ad ogni altra tecnologia in uso alle amministrazioni. In virtù di questi possibili vantaggi applicativi, il 1° febbraio 2018, fu istituito l'*EU blockchain Observatory and Forum*: uno strumento di promozione della ricerca e del confronto, volto al monitoraggio delle opportunità e delle criticità offerte dalla *blockchain*, in grado di sollecitare un dibattito di respiro continentale sull'effettiva compatibilità delle catene di blocchi con il quadro giuridico eurounitario. A questo primo intervento seguì, il 10 aprile 2018, l'istituzione dell'European blockchain Partnership (EBP). Questa ulteriore iniziativa si pose l'obiettivo di creare un'infrastruttura europea dei servizi blockchain, al fine di cooperare nella fornitura di servizi pubblici digitali transfrontalieri secondo i più alti standard di sicurezza e privacy[13]. Questa partnership ha, ben presto, visto un ruolo attivo del nostro Paese, entrato a par parte del progetto il 27 settembre 2018.

L'impegno eurounitario in materia, tuttavia, non si è limitato alle precedenti due iniziative.

Il 3 ottobre 2018, attraverso lo strumento della Risoluzione, il Parlamento europeo ha riconosciuto le potenzialità delle *blockchain*, affermando (in quell'occasione) che le predette sono potenzialmente in grado di costituire uno strumento di garanzia delle prerogative del cittadino. Le catene di blocchi, incentivando la disintermediazione e la decentralizzazione di alcune attività e di alcuni settori delle amministrazioni pubbliche, permetterebbero un efficace controllo dei propri dati da parte del cittadino-utente, nonché una trasformazione migliorativa di taluni procedimenti amministrativi.

Ulteriori profili d'interesse, in prospettiva eurounitaria, sono stati, poi, offerti dalla *Risoluzione sulla blockchain: una politica commerciale lungimirante*, del Parlamento europeo del 13 dicembre 2018. In questa occasione è stato sottolineato come (ove concepita adeguatamente) «la tecnologia *blockchain* dovrebbe essere in linea con il principio della "protezione dei dati fin dalla progettazione"». Una GDPR-*security by design*, che appare necessaria nell'ottica di una effettiva garanzia dei dati nell'intero loro ciclo di vita in seno alle catene di blocchi.

Il Parlamento europeo, sulla base di quanto appena rappresentato, ha ritenuto opportuno sollecitare gli attori interessati allo sviluppo di registri distribuiti ad adottare particolare cautela, con riferimento al management dei dati, costitutivi i blocchi di ciascuna catena. Una cautela ancor più necessaria, quando ad essere elaborati sono "dati personali", i quali non dovrebbero concorrere alla costruzione delle *blockchain*.

Un simile fermento istituzionale ha condotto, sul piano tecnico-regolamentare, alla pubblicazione del Libro Bianco sulla *blockchain*, a cura del Comitato europeo per la standardizzazione (CEN) e del Comitato europeo per la standardizzazione elettronica (Cenelec). Tra i molteplici intenti, posti a fondamento di questa iniziativa, ve n'è uno di estremo interesse per l'analisi che occupa: gettare le basi per una valutazione dell'impatto di questi nuovi strumenti tecnologici sul rapporto tra pubblica amministrazione e comunità dei consociati. Inoltre, sempre attraverso il predetto libro bianco, gli autori hanno tentato di definire un possibile modello organizzativo, tale da permettere il superamento di quei limiti al funzionamento della tecnologia *de qua* posti dall'assetto giuridico eurounitario in materia di protezione dei dati personali.

Questo quadro di iniziative continentali ha stimolato l'intervento dei legislatori nazionali ed in particolare (per quanto qui rileva) quello italiano.

Il primo intervento nazionale in materia risale al 2018, quando con il d.l. 14 dicembre 2018, n. 135[14], poi convertito con la l. 11 febbraio 2019, n. 12, si è giunti alla formulazione di una prima definizione di *blockchain*[15]. A seguito di questo intervento, l'ordinamento giuridico italiano ha riconosciuto gli effetti giuridici della validazione temporale elettronica, di cui al Reg. UE 910/2014, in materia di identificazione elettronica, alla memorizzazione di un documento informatico in seno ad una catena di blocchi.

Una simile iniziativa ha certamente concorso alla creazione di un panorama di maggiore certezza giuridica in materia, che si rende necessaria, stante il crescente interesse della pubblica amministrazione italiana per i margini di sua introduzione nei meccanismi di funzionamento della macchina amministrativa. Tale normativa di carattere nazionale dovrà necessariamente confrontarsi, nel medio termine, con un panorama giuridico più ampio e «potrebbe essere soggetta a future modifiche o integrazioni, così come avvenuto nel passato per la regolamentazione del documento informatico e delle firme elettroniche»[16].

Il contributo italiano in materia, tuttavia, risulta ben lungi dai soli interventi normativi di cui sopra. Sul punto, infatti, giova qui richiamare l'attenzione dimostrata dal Ministero per lo Sviluppo Economico (MISE) e dall'Agenzia per l'Italia Digitale (AGID).

Quanto al MISE, pare opportuno spendere alcune parole circa il *position paper* "Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e *blockchain*"[17], redatto da una squadra di trenta esperti del mondo DLT e sottoposto a consultazione pubblica dal 18 giugno al 20 luglio 2020 (i cui risultati sono ancora in fase di elaborazione al momento in cui si scrive).

Il documento in questione mette a sistema distinti piani del sapere, formulando un'articolata serie di raccomandazioni che spaziano dai profili giuridici connessi all'impiego dei registri distribuiti, ai possibili loro concreti utilizzi, tanto in ambito pubblico quanto in quello privato. Un ulteriore aspetto, affrontato dagli esperti ministeriali, è poi la governance dell'ecosistema digitale nazionale, per come configurabile a seguito del diffuso impiego di queste tecnologie, nonché le politiche pubbliche in materia di ricerca, formazione e divulgazione in ambito *distributed ledger*, che si rendono necessarie per un loro impiego su larga scala.

Il MISE, inoltre, con questo studio affronta l'impatto di queste tecnologie in seno alla vita della "macchina amministrativa", unitamente al margine di utilità delle predette nel processo trasformativo del Paese all'insegna della sostenibilità. Una connessione tra differenti transizioni, che ha trovato ulteriore spazio nelle case delle tecnologie emergenti. Attraverso questi "laboratori civici", il MISE intende promuovere la realizzazione, sul territorio nazionale, di centri di trasferimento tecnologico, volti al sostegno di progetti di ricerca e sperimentazione sui temi della *blockchain*, delle IoT e dell'intelligenza artificiale[18].

Un interesse, quello dimostrato dal ministero per le cd. tecnologie di frontiera, che ha portato, il 31 gennaio 2022, all'istituzione di un fondo[19] volto al sostegno economico di progetti di amministrazioni pubbliche ed imprese, in materia di intelligenza artificiale, Internet delle cose e *blockchain*. L'iniziativa si propone di perseguire, attraverso l'investimento di quarantacinque milioni di euro, gli obiettivi di politica economica e industriale nazionale, connessi agli ambiti di ricerca, sviluppo e innovazione tecnologica del Piano Transizione 4.0 (già programma Impresa 4.0). In tal senso, il Ministero intende «accrescere la competitività e la produttività del sistema economico affinché i processi di innovazione digitale possano generare crescita intelligente, sostenibile e inclusiva, in raccordo con gli obiettivi di sviluppo fissati dall'Unione europea»[20].

Inoltre, ciascuno di questi stanziamenti del MISE potrà essere combinato con ulteriori risorse nazionali, anche di fonte regionale, ed eurounitarie. Una ricerca di partnership continentali, quella messa in atto dal MISE, che nel decreto ministeriale di attivazione del fondo viene sottolineata dalla disponibilità dell'ente a supportare i progetti italiani, selezionati nel quadro di bandi emanati da istituzioni unionali, purché inerenti alle tecnologie di cui sopra.

Quanto poi ai profili organizzativi di questa iniziativa, il Ministero (oltre ad attivare gli interventi di cui in discussione) opererà in qualità di amministrazione vigilante, mentre la gestione in concreto sarà affidata a Infratel Italia s.p.a.[21]

Gli interventi a valere sul fondo *de quo* consisteranno in agevolazioni[22], partecipazioni al capitale di rischio (cd. *venture capital*) e, ove la natura degli obiettivi generali perseguiti lo richieda, in appalti pre-commerciali o appalti pubblici di soluzioni innovative.

Infine, il ministero ha inteso promuovere, attraverso questo strumento finanziario, una crescita tecnologica del mezzogiorno, prevedendo (all'insegna del principio di riequilibrio territoriale[23]) una quota di riserva destinata ai progetti localizzati in una delle regioni del sud-Italia[24], proporzionale alla popolazione ivi residente. Tuttavia, decorsi sei mesi dall'apertura dei termini per la presentazione delle domande, le risorse non impegnate nell'ambito di detta riserva saranno rese disponibili per soddisfare il fabbisogno manifestato nei restanti territori.

Proseguendo con l'analisi, giova poi richiamare le iniziative attivate, in materia, dall'Agenzia per l'Italia Digitale (AGID). Più nel dettaglio, nel 2021 essa ha formulato una prima "Strategia nazionale per le competenze digitali (*Release 1.0*)"[25], con la quale ha sostenuto la necessità di un maggior impegno circa lo sviluppo e l'integrazione di tecnologie emergenti (tra le quali spiccano le catene di blocchi) nella vita delle amministrazioni pubbliche, come del tessuto industriale nazionale. Questo processo (auspicato

dall'Agenzia) mira non già alla mera implementazione di nuovi ritrovati tecnologici nel quotidiano di cittadini, imprese ed istituzioni, ma anche alla «realizzazione di nuovi sistemi di produzione più sostenibili e inclusivi»[26]. Inoltre, sempre nel medesimo *white paper*, l'AGID pone l'accento sulla rilevanza della domanda pubblica di innovazione nello "stimolo" della crescita di un'omologa domanda da parte del comparto privato[27].

Queste riflessioni si collocano nel solco di un più ampio ed articolato programma di implementazione delle competenze digitali del personale della pubblica amministrazione, ritenuta funzionale ad un effettivo sviluppo dell'*e-government* italiano, al quale l'Agenzia accosta la necessità di una più incisiva lotta al *digital divide*[28].

Tuttavia, l'impegno dell'AGID è ben lungi dal circoscriversi alla sola formulazione della "strategia" di cui sopra. In prospettiva internazionale, infatti, essa è stata coordinatrice del gruppo tematico OCSE sulle tecnologie emergenti nel settore pubblico, impegnato nell'elaborazione di linee guida per l'utilizzo della *blockchain* e degli strumenti di intelligenza artificiale nei servizi pubblici dei 35 Paesi Ocse[29]. L'AGID, inoltre, rientra nella rosa dei promotori del progetto IBSI (*Italian Blockchain Service Infrastructure*), tra i quali figurano CIMEA, CSI Piemonte, ENEA, INAIL, Infratel Italia, INPS, Politecnico di Milano, Poste Italiane, RSE, GSE, SOGEI e Università di Cagliari. L'iniziativa mira allo sviluppo di un «ecosistema basato su tecnologie di tipo Registri Distribuiti (DLT), in linea con la Strategia europea che sta realizzando, anche con il contributo italiano, un'infrastruttura analoga nell'ambito della *European Blockchain Partnership*»[30].

3. Le sperimentazioni italiane

Volendo poi spostare il *focus* dell'analisi dalla dimensione "pianificatoria" ai profili applicativo-istituzionali di questa tecnologia, è possibile rilevare un discreto numero di sperimentazioni, portate avanti da svariate amministrazioni pubbliche (tra loro differenti tanto in ordine alla rispettiva collocazione geografica quanto al livello di prossimità al cittadino).

Esempi di questi "possibili impieghi" sono offerti, ad esempio, dalla Regione Lombardia, che vede sul proprio territorio ben tre progetti, ormai pienamente operativi. In particolare, «nel 2019 il Comune di Cinisello Balsamo fu scelto, da Regione Lombardia, come ente pilota a livello europeo per la sperimentazione della tecnologia *blockchain*, da utilizzarsi per l'iscrizione alla Misura regionale Nidi Gratis. A distanza di poco più di un anno fu possibile costatare come l'introduzione di questa tecnologia di frontiera avesse portato grandi benefici nel lavoro della pubblica amministrazione e nella fruizione dei servizi da questa offerti»[31].

Nello specifico, è stato sostenuto (in sede istituzionale) come, a seguito di tale sperimentazione, sia stato possibile assistere all'eliminazione di «più del 70% dei passaggi amministrativi»[32] necessari all'espletamento della procedura interessata dal progetto. Inoltre, grazie a questo ecosistema *blockchain*, delle 219 domande inviate in Regione dai potenziali beneficiari, ben «156 sono state approvate in tempo reale»[33].

Sempre al 2019 risale l'avvio di un'ulteriore iniziativa in ambito *blockchain*, portata avanti dalla Regione Lombardia. In questo caso, l'ente ha inteso declinare le potenzialità dei registri distribuiti alla governance di specifiche filiere agroalimentari[34]. La Regione, attraverso questa piattaforma *blockchain*, ha inteso tutelare il consumatore da frodi e contraffazioni; contestualmente, detta infrastruttura informatica si è posta l'obiettivo di garantire tanto la qualità dei prodotti quanto il benessere animale (nonché la sostenibilità dell'intera *supply chain*).

Risulta, inoltre, di grande interesse il progetto avviato dall'Università di Milano Bicocca che, in collaborazione con Cineca, ha introdotto «un sistema digitale basato su *blockchain* per garantire agli studenti la validità e l'integrità di documenti e certificati ufficiali sul web»[35]. La piattaforma in questione si offre di «emettere documenti digitali certificati, assicurando che non siano manipolabili o falsificabili. Uno strumento moderno, sicuro e sempre accessibile, utilizzabile ovunque nel mondo, grazie al quale gli studenti possono garantire l'autenticità e l'integrità del loro titolo di laurea a potenziali datori di lavoro e ad altre istituzioni»[36].

L'iniziativa dell'ateneo milanese mira ad offrire una risposta a quel processo trasformativo delle istituzioni accademiche, sempre più orientate alla costruzione di «percorsi di apprendimento flessibili, *life-long*, basati sull'accumulo di apprendimenti attraverso esperienze diverse, modulari, supportate da istituzioni e piattaforme diverse, e quindi certificati da diverse istituzioni e piattaforme»[37]. In questo caso, la *blockchain* parrebbe offrire al mondo dell'istruzione, un efficace strumento di *digital academic credentialing*, in grado di «facilitare la mobilità professionale di studenti e laureati»[38]. Circostanza, quella ivi rappresentata, da cui sembrerebbe potersi desumere l'intrinseca capacità di questa tecnologia di supportare le istituzioni (accademiche e non solo) nella promozione di quelle condizioni (*ex* art. 4,

comma 1, Cost.) strumentali all'effettivo esercizio, da parte di ciascun *civis*, del diritto al lavoro.

Volendo proseguire la ricognizione delle più rilevanti sperimentazioni pubbliche in ambito *blockchain*, riconducibili al panorama amministrativo italiano, giova sottolineare come le pubbliche amministrazioni del sud Italia sembrerebbero non aver inteso giocare un ruolo di secondo piano. È, infatti, possibile ritrovare nella rosa di amministrazioni attive in materia il Comune di Bari che, dopo una prima fase dedicata all'analisi dei possibili impieghi delle criptovalute nell'ambito di alcuni processi pubblici, ha incentrato i propri sforzi sui margini di applicabilità dei registri distribuiti al funzionamento della propria macchina amministrativa. Tale fermento, lungi dall'essere una mera ricerca di maggiori livelli di digitalizzazione della pubblica amministrazione, sembrerebbe orientato ad una strutturale implementazione dell'approccio *bottom up* nel funzionamento dell'ente. Alcuni rappresentanti istituzionali dell'amministrazione, inoltre, hanno avuto modo di sostenere, con riferimento a queste sperimentazioni, che esse rappresentino una concreta «componente enzimatica nella generazione di valore pubblico»[39]. Attraverso il supporto offerto da una rete di partner provenienti dal tessuto economico-sociale, l'ente locale ha approfondito, in prima battuta, il margine di applicabilità delle catene di blocchi alla governance dell'identità digitale, nonché alla costruzione di un possibile sistema di *e-voting* (da circoscriversi all'elezione dei soli rappresentanti dei municipi di cui si compone la città metropolitana di Bari). Tuttavia, questo progetto non ha, ad oggi, ancora avuto una concreta fase di test, limitandosi a rappresentare un mero esercizio teorico.

L'interesse del Comune di Bari per la *blockchain* si è, poi, tradotto nell'avvio di una partnership con Fincons Group, con la quale è stato realizzato un modello di gestione dello smart working, attraverso *smart contract* su *blockchain permissionless*. Un intervento strutturato nell'ottica di una piena garanzia dei lavoratori coinvolti, nonché dei diritti di cui costoro sono portatori. Rispetto al preliminare progetto pilota, però sembrerebbero permanere alcuni profili problematici in merito «alla *compliance* al GDPR»[40] di questa piattaforma.

Alle iniziative sin qui rappresentate, si è poi sommata un'ulteriore piattaforma, realizzata grazie al supporto tecnico di SIA s.p.a. L'infrastruttura *de qua* è stata immaginata come funzionale alla gestione delle polizze fideiussorie, poste a garanzia di quelle imprese con cui l'ente locale intrattiene rapporti, nel quadro dei suoi processi di *public procurement*.

Il progetto prevede che i documenti attestanti il rapporto fideiussorio tra impresa appaltatrice e soggetto garante (es. istituti di credito o società assicurative), una volta sottoscritta la polizza, vengano resi disponibili per l'ente pubblico interessato, a seguito di un processo di notarizzazione, attraverso un'infrastruttura *blockchain permissioned*.

In relazione a questa infrastruttura, giova sottolineare come la stessa sia stata predisposta sulla base di *Solidity*, «il linguaggio di programmazione della principale *blockchain* pubblica per la gestione di *smart contract*»[41]: circostanza che rende questa piattaforma un concreto ecosistema digitale.

Per le pubbliche amministrazioni, infatti, «nonostante il ricorso al mercato elettronico, a centrali di committenza, a procedure informatiche di gestione delle varie fasi della gara, la conformità del documento presentato, la legittimità del garante a poter operare, la possibilità che la polizza possa essere all'occorrenza escussa, rappresentano ancora delle incognite non facilmente gestibili»[42]. Nel solco di tali profili problematici si colloca questo ecosistema *blockchain*, il quale trova la propria ragion d'essere nella contestuale ricerca di una maggiore efficienza della macchina amministrativa, unitamente alla dematerializzazione delle procedure ad essa imputabili. Un ecosistema che mira ad assorbire al suo interno, con il tempo, una «serie di oracoli, già impegnati nel supporto alle amministrazioni, agli operatori economici e alle aziende del settore bancario ed assicurativo»[43] (Es. ANAC, Banca d'Italia, IVASS, camere di commercio). Tale integrazione, a detta dei promotori potrebbe impedire *ab origine* la stipulazione di «contratti inefficaci rispetto alla manifestazione di effetti giuridici» e bloccare «operatori che hanno perso i requisiti per poter operare sul mercato nazionale»[44]. Questa infrastruttura, infine, sembrerebbe poter integrare un «sistema di *rating* degli operatori coinvolti, sistema tanto più efficace quanto più detta soluzione diventasse universale approdando ad essere una componente del Mercato Elettronico della Pubblica Amministrazione (MEPA) e dei Mercati Elettronici decentrati»[45].

Pare, infine, opportuno fare menzione anche di alcune iniziative che, negli ultimi anni, hanno interessato le amministrazioni centrali.

Ci si riferisce, in tal senso, ai due progetti che hanno coinvolto, sin dal 2014, il Ministero dell'economia e delle finanze "MEF": *SUNFISH* e *Poseid-on*.

Quanto al primo, la Direzione dei Sistemi informativi e dell'innovazione del MEF, posta a capo di un consorzio internazionale composto da 11 organizzazioni (facenti capo a sei distinti Stati), ha sviluppato (nel triennio 2015-2017) una piattaforma

funzionale alla condivisione di informazioni riservate tra cloud privati ed all'impiego di cloud pubblici, all'insegna di elevati standard di sicurezza cybernetica.

SUNFISH (*SecUre iNFormatIon SHaring in federated heterogeneous private clouds*), «integralmente finanziato nell'ambito di Horizon 2020 per un importo pari a 4,5 milioni di euro»[46], si è articolato in tre distinti scenari d'uso. In particolare, sulla base di specifiche esigenze del MEF e del Ministero dell'Interno italiani, del Ministero delle Finanze maltese e della *South East Regional Cyber Crime Unit* della polizia britannica, l'iniziativa è stata orientata all'utilizzo in sicurezza di cloud pubblici in ambito amministrativo, al compimento di interrogazioni sicure e riservate, senza rivelazione della chiave di ricerca, di database distribuiti su una serie di cloud privati ed alla garanzia della condivisione sicura di informazioni riservate tra questi ultimi (quando in uso alla pubblica amministrazione).

Quest'ultimo caso d'uso (particolarmente rilevante ai fini di questo lavoro) ha visto i due citati ministeri italiani impegnati nella realizzazione di una piattaforma in grado di garantire, attraverso il ricorso a *smart contract* fondati su tecnologia *blockchain*, la correttezza, l'integrità e la riservatezza delle informazioni inerenti al personale della polizia di Stato, archiviati entro i sistemi informativi del Ministero degli Interni, quando trasmesse al MEF per il calcolo della busta paga.

La seconda iniziativa, che prende il nome di progetto *Poseid-on*, vede il MEF a capo di un consorzio di dieci partner europei, tra i quali figurano università, soggetti pubblici ed imprese provenienti da sette diversi Paesi. L'iniziativa, selezionata dalla Commissione europea nell'ambito della call "Cybersecurity PPP: Privacy, Data Protection, Digital Identities", parzialmente finanziata dalla Commissione europea tramite il programma Horizon 2020, è finalizzata alla realizzazione di una piattaforma innovativa per la gestione e protezione dei dati personali dei cittadini in possesso delle pubbliche amministrazioni. A seguito dell'implementazione di Poseid-on nel sistema NoiPA, il Ministero sostiene di poter offrire al cittadino, sempre attraverso *smart contract* fondati su tecnologia *blockchain*, «la possibilità di prendere decisioni consapevoli su chi potrà elaborare i propri dati, abilitando o revocando le autorizzazioni e chiedere eventualmente di rimuovere definitivamente i propri dati personali in base all'attendibilità del responsabile del trattamento»[47].

Al netto delle prefate sperimentazioni, l'interesse del MEF per la tecnologia *blockchain* si è spinto ben al di là della creazione di strumenti DLT al servizio delle pubbliche amministrazioni. Giova, infatti, richiamare il decreto ministeriale del 17 febbraio 2022, con il quale è stato attivato il registro degli operatori in valute virtuali. Un intervento grazie al quale il Ministero sembrerebbe mirare alla governance pubblica di una parte di quelle iniziative economiche private fondate sulla tecnologia *blockchain*.

Nello specifico, il decreto istituisce (presso l'Organismo degli Agenti e dei Mediatori creditizi "OAM") una sezione speciale del registro dei cambiavalute, ove ciascun soggetto, italiano o straniero, qualora voglia esercitare l'attività di *exchanger*[48] o *wallet provider*[49] in Italia, dovrà necessariamente iscriversi. In caso di inosservanza di questo obbligo, ovvero in caso di assenza di un proprio domicilio o di una stabile organizzazione in Italia, l'iniziativa economica in questione sarà vietata e si potrebbe incorrere nell'oscuramento del sito Internet connesso all'attività d'impresa.

Inoltre, con cadenza trimestrale, gli iscritti al registro dovranno comunicare all'OAM i dati identificativi dei propri utenti, unitamente alle informazioni inerenti alle operazioni da costoro poste in essere. La qualcosa sembrerebbe poter favorire un agevole monitoraggio di una parte delle "proiezioni economicamente rilevanti del protocollo di Nakamoto" da parte delle forze dell'ordine e, più in generale, dello Stato apparato nel suo insieme.

4. *Blockchain*: utilità attese di una tecnologia

Considerato l'interesse della pubblica amministrazione italiana per questa tecnologia, pare opportuno tentare di definire tanto le utilità attese, quanto i pericoli potenziali, riconducibili ad un impiego pubblico di quello che (non senza un certo grado di "hýbris") è stato definito il «Protocollo di Dio»[50].

In prima battuta, risulta agevole comprendere come le già citate *Distributed Ledger Technologies* possano (grazie ai loro caratteri di «certezza, trasparenza e immodificabilità»[51]) rappresentare, nel quotidiano funzionamento delle istituzioni pubbliche, un'utile risorsa. Si pensi ai margini di applicabilità della *blockchain* nell'attività certificativa, di cui un esempio può essere il citato progetto dell'Università di Milano Bicocca, o a quella di controllo, con riferimento alla quale è stato possibile trovare traccia nel passaggio dedicato alla piattaforma per il monitoraggio delle polizze fideiussorie del Comune di Bari.

Inoltre, secondo parte della dottrina, le catene di blocchi rivestirebbero un ruolo strategico nella transizione digitale di alcuni «processi di tipo autenticamente decisionale e, segnatamente, di quelli soggettivamente complessi, che vedano il coinvolgimen-

to di più attori, privati o pubblici»[52]. In tal senso, ci si riferisce a «procedure selettive (quali, ad esempio, i concorsi e l'evidenza pubblica) e dei procedimenti pluristrutturati (tra tutti quelli che prevedono il ricorso al modulo della conferenza di servizi)»[53], nella sua forma semplificata ed in modalità asincrona. Quest'ultima, «per espressa previsione del comma 1 dell'art. 14-*bis* deve, infatti, avere luogo attraverso comunicazioni telematiche»[54], circostanza che apre ad un possibile sviluppo delle interazioni tra soggetti interessati dalla procedura da svilupparsi in ambiente *blockchain*.

Un ulteriore profilo degno di nota è, poi, quello connesso alla governance di grandi moli di dati (come sostenuto dal MEF con riferimento alle sperimentazioni *SUNFISH* e *Poseid-on*). L'impiego di questa tecnologia, secondo i rispettivi consorzi promotori, potrebbe garantire l'eliminazione degli eventuali casi di alterazione accidentale o volontaria dei dati elaborati, ipotesi più che possibile in caso di utilizzo di database tradizionali. Circostanza da cui discende l'elevata compliance del trattamento posto in essere dalle pubbliche amministrazioni competenti, senza che sia intaccata l'efficienza dell'amministrazione nel suo insieme.

Giova poi richiamare, in questa sede, il legame che sembrerebbe intercorrere tra l'impiego pubblico delle catene di blocchi e la lotta ai fenomeni di *digital divide* infrastrutturale che interessa alcune articolazioni dell'amministrazione. Infatti, non pare fuori luogo sottolineare come, in presenza di una solida infrastruttura *blockchain* (in cui gli attori sono dotati in larga misura di strumentazione hardware e software idonea allo scopo) anche un nodo, se pur compromesso da elevati livelli di obsolescenza delle proprie risorse informatiche, possa comunque godere delle potenzialità dell'infrastruttura. Tale potenziale inclusivo pare potersi riflettere positivamente su quel principio d'unità a cui si ispira la Repubblica, in ragione dell'intrinseca capacità di garantire, sul piano teorico, a ciascun cittadino le medesime opportunità, al di là del territorio ove egli si trovi o della tipologia di amministrazione interessata.

Un ulteriore aspetto meritevole di attenzione è, poi, l'agevole navigabilità dei dati stoccati in un DLT, in grado di permettere a ciascuno dei partecipanti la loro consultazione ed analisi[55].

Un esempio di simili impieghi è stato offerto da Regione Lombardia che, come evidenziato in precedenza, ha inteso rendere tracciabili alcune filiere agroalimentari. Quanto ai profili di utilità di questa iniziativa, pare opportuno evidenziare, in prima battuta, come una simile piattaforma abbia determinato «l'accountability degli attori della filiera», da cui consegue la rimozione di quelle asimmetrie informative in grado di compromettere l'adozione, da parte del consumatore, di scelte libere e consapevoli (*rectius*: l'effettività del principio concorrenziale stesso). In secondo luogo, parrebbe potersi scorgere (all'ombra di una simile scelta della Regione) la volontà di promuovere, attraverso i DLT, quella funzione sociale dell'iniziativa economica privata (*ex* art. 41 Cost.). Una promozione portata innanzi attraverso una politica di *nudging*[56] indiretto, fondato sulla capacità di condizionamento dei processi produttivi sottesi all'offerta, attraverso una campagna di sensibilizzazione della "domanda" (portata avanti da Regione Lombardia sui temi della sostenibilità), resa ancor più incisiva dal livello di informazione del cittadino-consumatore imputabile all'avvio di una simile piattaforma.

Tuttavia, il valore del patrimonio di dati in possesso della pubblica amministrazione (e precipuamente della sua conoscibilità da parte del cittadino) va ben al di là della tutela del singolo nella sua veste di consumatore ovvero della garanzia di elevati standard concorrenziali in seno al mercato. A partire dall'ultimo decennio del "secolo breve", infatti, «le informazioni rivestono per le amministrazioni un ruolo sempre più decisivo, nel perseguimento di politiche di sostenibilità. Alla loro originaria e intrinseca finalità di aumentare le possibilità di apprendimento circa lo stato di compromissione degli ecosistemi, si aggiunge quella di favorire la più ampia partecipazione dei cittadini ai processi decisionali in tema di tutela dell'ambiente»[57].

La conoscibilità delle informazioni ambientali ha, con il tempo, acquistato crescente rilievo nella vita delle nostre istituzioni. un percorso evolutivo che, muovendo i suoi primi passi in occasione della Conferenza ONU di Rio de Janeiro del 1992, ha portato (con la Convenzione di Aarhus del 1998) all'introduzione di un obbligo per gli Stati sottoscrittori di raccogliere (attraverso le proprie amministrazioni pubbliche) ogni informazione rilevante ai fini dell'espletamento delle proprie funzioni amministrative, nonché il periodico aggiornamento dei dataset in loro possesso. Tale obbligo mira alla garanzia di una «*total disclosure* in caso di minacce per la salute umana o per l'ambiente»[58]. Inoltre, la comunità internazionale ha previsto, nella medesima occasione, che ai cittadini sia garantito un accesso trasparente alle informazioni ambientali di cui sopra, nonché la loro digitalizzazione (al fine di massimizzare le occasioni di detto accesso).

Tale diritto non pare essere riconducibile, in prospettiva costituzionale, al mero esercizio della libertà di informarsi, di informare o di essere informato; sembra, piuttosto, profilarsi quale presupposto per la

conquista, da parte del *civis*, di un ruolo attivo nella progettazione e conseguente realizzazione di politiche pubbliche in materia di sostenibilità ambientale.

Nel solco di quanto appena rappresentato, la *blockchain* pare poter essere un utile supporto alla predetta attività di *disclosure*, potendo garantire un ecosistema digitale caratterizzato da elevate prestazioni in termini di trasparenza ed integrità del dato, che, se messe a sistema con l'eterogeneità dei possibili impieghi dell'*Internet of things* (IoT), potrebbe permettere un diffuso ed effettivo monitoraggio di ciascuna delle facce semantiche di quel polisenso prisma che è il concetto di "ambiente".

Secondo alcuni, poi, ciò che renderebbe unico l'impiego pubblico della *blockchain* sarebbe «la sua capacità di mutare il volto dell'amministrazione»[59]. Questo impiego, infatti, aprirebbe (in taluni casi) alla cogestione del procedimento amministrativo, rendendo ciascun operatore della rete (attivo all'interno dell'infrastruttura in qualità di nodo) protagonista e non semplice destinatario dell'azione amministrativa. Saremmo dinnanzi ad un «terreno inedito di realizzazione del principio costituzionale di sussidiarietà»[60], inteso nella sua accezione orizzontale. Se però volessimo porre tali suggestioni in relazione con la citata capacità della tecnologia *blockchain* di ridurre i divari infrastrutturali tra distinte articolazioni della macchina amministrativa (attraverso la creazione di ecosistemi digitali in grado di favorire reciproche interazioni), allora non sembrerà inopportuno tentare un'interpretazione del rapporto tra DLT e principio di sussidiarietà ben più estensiva.

Degli spazi di applicabilità del prefato principio, alla luce dei quali «il dialogo con e tra le pubbliche amministrazioni diviene lo scenario obbligato di verifica dell'effettività del diritto costituzionale e delle tutele sue proprie»[61], stante quella "missione costituzionale" di cui sarebbero custodi (secondo parte della dottrina) le pubbliche amministrazioni[62].

Inoltre, appare doveroso spendere alcune parole circa i possibili impieghi delle catene di blocchi nell'attività di *public procurement*.

Il primo aspetto degno di nota attiene alla presunta assenza di opportunità di modifica fraudolenta delle informazioni contrattuali immesse in una DLT, come la tracciabilità delle operazioni realizzate dagli attori del rapporto. Ogni singolo frangente della vita del contratto, dalla stipula alla sua compiuta attuazione, è censito; i relativi dati sono inseriti nel registro condiviso, non sono alterabili *a posteriori* ed hanno (grazie ad un marcatore temporale loro apposto al momento dell'immissione nel registro) una data ed un ora di riferimento giuridicamente certa. Il tema della certezza temporale, difatti, è stato oggetto di attenzione da parte del legislatore italiano, che ha chiarito come «la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produca gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014»[63]. Ciò rende opponibile anche al terzo il momento esatto del compimento del singolo atto di esecuzione del contratto, «dando vita ad un inedito sistema di pubblicità contrattuale di tipo dichiarativo»[64]. L'impiego della tecnologia *blockchain*, inoltre, garantendo la codetenzione *ab origine* di ogni dato immesso, permette a tutti i partecipanti alla rete di possedere una copia del registro distribuito su cui sono annotate non già le sole proprie operazioni bensì anche quelle poste in essere dagli altri operatori dell'infrastruttura.

Si è, dunque, ben oltre la trasparenza intesa quale accessibilità totale al dato[65], perché quest'ultimo è sin dal principio nella disponibilità come dell'amministrazione così del cittadino coinvolto (a vario titolo) dalla vicenda contrattuale[66]. Pertanto, con l'impiego dei registri distribuiti nell'attività di *public procurement*, si assisterebbe ad un'apertura del rapporto contrattuale ad una serie di soggetti estranei al rapporto pattizio in senso stretto, tra i quali figurano tutti coloro che (pur avendo presentato la propria proposta economica) non si siano utilmente classificati.

Con specifico riferimento alla conoscibilità (da parte degli operatori economici non aggiudicatari) delle informazioni riconducibili agli atti della fase di esecuzione, la giurisprudenza ha assunto (secondo parte della dottrina) un atteggiamento piuttosto ondivago[67]. In alcuni casi, infatti, le pronunce del giudice amministrativo hanno riconosciuto la piena praticabilità dell'accesso *ex* d.lgs. n. 33/2013[68]; in altre circostanze, invece, sono state tratteggiati confini ben più stringenti all'esercizio del rimedio *de quo*[69]. Le pronunce hanno inteso definire una netta cesura tra gli atti della fase pubblicistica, in riferimento ai quali può riconoscersi l'esperibilità dell'accesso civico, e quelle informazioni inerenti alla fase di esecuzione, per la cui conoscibilità si rende necessario il ricorso all'accesso *ex* art. 22 l. 7 agosto 1990, n. 241[70]. Al netto di questo approccio dicotomico del giudice amministrativo (poi *reductio ad unum* con la sent. Cons. St., Ad. plen., n. 10 del 2 aprile 2020), l'impiego della tecnologia *blockchain* sembrerebbe poter offrire ai soggetti non aggiudicatari un ruolo di primo piano nel presidio dell'efficace ed efficiente funzionamento della macchina amministrativa. Questa tecnologia, infatti, permetterebbe il tempestivo esercizio del diritto di interpello per il subentro nel rapporto, ove vi sia stato lo scioglimento anticipato

del contratto concluso con l'originario aggiudicatario[71]. Inoltre, questo accesso ad una serie di informazioni relative all'esecuzione del contratto da parte dell'operatore economico non aggiudicatario (avente interessi intrinsecamente antagonisti a quelli del soggetto utilmente classificato) potrebbe rappresentare il presupposto per un controllo diffuso e costante sul contegno tenuto dalle "parti" (tanto pubbliche quanto private). In un simile scenario, la pletora di operatori terzi, al fine di garantire i propri legittimi interessi (aspettativa di per sé degna di tutela), scoraggerebbe lungo l'intero iter del rapporto contrattuale eventuali inadempienze, quanto non concrete condotte corruttive. Con specifico riferimento a quest'ultimo *genus* di pratiche, «ben può dirsi che la corruzione è funzione inversa della capacità di controllo che il principale – pubblica amministrazione è in grado di esercitare»[72] sull'agente-aggiudicatario. Da ciò consegue che l'impiego del registro distribuito in ogni fase del rapporto tra pubblica amministrazione e soggetto utilmente classificato, incrementando i livelli di "trasparenza del rapporto" possa rappresentare, al contempo, una concreta difesa da pratiche di *maladministration*, nonché un presidio avverso fenomeni di "cattura del controllore"[73].

Emerge a più riprese, quale convitato di pietra delle riflessioni sin qui svolte, il tema della concorrenza, nonché il rilievo costituzionale che essa riveste attualmente nella vita dello Stato apparato, come di quello comunità. Così, la trasparenza, principio cardine dell'azione amministrativa, che trova nella tecnologia *blockchain* nuovi orizzonti di effettività, diviene (con riferimento all'impiego delle catene di blocchi nell'attività di *public procurement*) *conditio sine qua non* per generare un ecosistema istituzionale in grado di essere vettore di effettività del principio di concorrenza in seno al tessuto economico-sociale.

Un ulteriore aspetto, riconducibile all'impiego di questa tecnologia nel "funzionamento della macchina amministrativa" è poi l'automatica raccolta di enormi moli di dati, a seguito della sistematica registrazione (attraverso DLT) delle relazioni attuate dalle pubbliche amministrazioni con i differenti operatori presenti sul mercato. Un patrimonio informativo che, secondo avvertita dottrina, potrebbe essere impiegato «nell'ambito delle successive procedure di affidamento, per il *rating* degli operatori economici ed il vaglio di ammissibilità delle offerte formulate»[74].

A quanto sin qui rappresentato, giova poi accostare la disamina di alcuni margini di utilità derivanti da tecnologie che della logica *blockchain* sono dirette derivazioni: quali, ad esempio, gli *smart contract* (o contratti intelligenti), costituiti da «un protocollo di transazione computerizzato che esegue automaticamente prestazioni corrispondenti ad adempimenti negoziali»[75].

Sul punto, la dottrina ha avuto modo di ipotizzare come, a seguito dell'impiego di questo strumento in seno alla vicenda contrattuale, consegua la riduzione dei margini di incertezza applicativa delle clausole negoziali e, con essa, delle già citate occasioni di *maladministration*.

Da ciò parrebbe conseguire l'intrinseca attitudine delle catene di blocchi e dei loro precipitati algoritmici a circoscrivere (seppur parzialmente) i margini di conflitto in seno a questo specifico *genus* di vicenda contrattuale. Un'attitudine, in forza della quale sembrerebbe potersi ascrivere all'impiego pubblico delle DLT una capacità deflattiva della mole di contenziosi che, ad oggi, interessano la pubblica amministrazione.

Circostanza, a seguito della quale discenderebbe, presumibilmente, un abbattimento del "bisogno di assistenza forense" delle pubbliche amministrazioni, a cui si potrebbe riconnettere tanto una riduzione del carico di lavoro dell'Avvocatura di Stato e, dunque, del fabbisogno di organico in essa incardinato, quanto del ricorso ai professionisti del libero foro. Quest'ultimo aspetto, poi, comporterebbe una riduzione dei margini di spesa che, per quanto esigua rispetto alla complessiva entità dei cespiti di cui si compone il bilancio dello Stato, parrebbe concorrere positivamente al rispetto di quel dovere che l'ordinamento riconosce in capo alle amministrazioni, in forza del quale le stesse sono tenute ad assicurare «la sostenibilità del debito pubblico» (*ex* art. 97, co. 1, Cost.). Un ulteriore aspetto degno di nota inerisce all'efficientamento della "macchina della giustizia", che la riduzione dei conflitti tra aggiudicatario e pubblica amministrazione comporterebbe, con contestuale redistribuzione di quella quota parte delle risorse che (in assenza dell'impiego pubblico della *blockchain* e degli strumenti ad essa riconducibili) sarebbero impegnate per la composizione di quei contenziosi scaturenti dalle attività di *public procurement*.

Vi è poi uno specifico fronte di quest'ultima attività che apre a spazi di "ibridazione delle transizioni" oggi in atto. Ci si riferisce all'impiego della *blockchain* per la stipulazione di contratti pubblici all'insegna della sostenibilità. In particolare, in dottrina è stato affermato come il *Building Information Modeling* (BIM)[76], se combinato con ecosistemi *blockchain*, possa rappresentare un concreto giro di boa per la transizione sostenibile degli appalti pubblici. Vi è stato chi, nello specifico, abbia parlato di "Circular BIM"[77] che, se messo a sistema con un oculato impiego dei già citati *smart contract* e dei controlli tramite IoT, aprirebbe nuovi orizzonti di operatività

alle clausole ecologiche in grado di offrire, alle pubbliche amministrazioni, l'opportunità di una metamorfosi delle commesse pubbliche all'insegna del cd. *green public procurement*[78].

5. *Blockchain*: i pericoli potenziali di un impiego istituzionale di questa tecnologia

Alla pervicace fiducia di una parte della dottrina circa le potenzialità delle nuove tecnologie nella ricerca di innovativi itinerari di sviluppo sociale ed istituzionale, si sono opposte, però, letture di senso contrario. Quanto al "lato oscuro della trasparenza", nonché agli interrogativi «che si celano dietro la dismissione di ogni diaframma rispetto alla conoscibilità del dato»[79], giova richiamare il contributo di Shoshana Zuboff, che in un suo volume del 2018 ha tentato di rappresentare (in prospettiva sociologica) i caratteri costitutivi di una società senza filtri[80].

Volendo limitare i molteplici profili di critica (emersi in dottrina) solo a quelli che interessano il ricorso a questa tecnologia da parte della pubblica amministrazione, innanzitutto, riveste un ruolo cruciale quello della protezione dati, in ragione del fatto che il dato si configura quale "atomo" di cui si compone ogni ecosistema digitale. In tal senso, un primo aspetto degno di nota è certamente la difficile individuazione del titolare del trattamento, «ossia dell'entità che da sola o congiuntamente con altri determina le finalità e le modalità del trattamento dei dati personali»[81]. Essa risulta problematica, infatti, «dal momento che, come si è visto, nelle *blockchain* di tipo *permissionless* l'adesione a una *blockchain* è aperta, e tutti i partecipanti hanno uguali ruoli e poteri»[82]. Pur rilevandosi differenti tipologie di partecipanti osservabili in una *blockchain permissioned*, tuttavia, non risulta praticabile «l'assimilazione delle caratteristiche del ruolo di titolare a quelle di un *miner*, essendo nella maggior parte dei casi quest'ultimo soggetto un mero esecutore di una funzione tecnica»[83]. Tuttalpiù, i "nodi" potrebbero essere qualificati come responsabili del trattamento (o *processor*) «qualora essi ricevano opportune istruzioni dal titolare del trattamento su come eseguire la loro funzione tecnica di creazione del consenso»[84].

A tali profili problematici, appare utile accostare l'approfondimento del margine di effettività di due "diritti", propri del quadro giuridico nazionale ed unionale, che sembrerebbero collidere «con un registro caratterizzato per sua natura da immutabilità»[85]. Ci si riferisce al difficile esercizio del diritto di modifica del dato, nonché all'assoluta ineffettività di quello di cancellazione del medesimo. Quest'ultimo profilo appare di particolare interesse, in ragione del suo essere causa dell'endemica incompatibilità delle DLT con il diritto all'oblio[86] (di cui all'art. 17 del Regolamento n. 679/2016 GDPR). Diritto, in forza del quale, è riconosciuta all'interessato la facoltà di pretendere la cancellazione dei propri dati personali, esercitabile anche a seguito della revoca del consenso al trattamento[87]. Proprio il tema del consenso si dimostra essere strettamente connesso all'esercizio di questo diritto ai sensi dell'art. 4 del GDPR. Il primo può infatti dirsi validamente espresso quando vi sia stata una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso abbia espresso il proprio assenso alla partecipazione ad uno specifico trattamento (*rectius*, ad una elaborazione in ambiente *blockchain*). Tuttavia, l'effettiva pienezza di una simile manifestazione di volontà riposa sulla capacità dell'interessato «di rifiutare o revocare il consenso senza subire pregiudizio»[88], ottenendo in questo caso la cancellazione del dato.

Giova, poi, osservare come «se da una parte è vero che non tutti i dati trattati sono qualificabili come personali, dall'altra la natura personale dei dati non è legata alla loro intelligibilità»[89]. Un dato anonimizzato[90], infatti, può essere un dato personale stante l'ampiezza della definizione di quest'ultimo data dal GDPR. In presenza di un «dato composto (ad esempio, un record di un database in cui sono presenti molti attributi di una persona) qualsiasi elemento, intellegibile o meno, è idoneo a identificare un interessato. Basta, infatti che quell'elemento sia noto a un terzo e riconosciuto da questi come un attributo di una specifica persona»[91]. Pertanto, l'identificabilità dipende dal contesto in cui il dato è utilizzato, e l'anonimizzazione di un dato, ossia l'eliminazione del collegamento tra un dato e un'identità, non consiste unicamente nella rimozione di attributi facilmente identificativi (il nome e cognome, il domicilio, ecc.) o nella non intellegibilità di quelli impiegati. Pertanto, appare problematica, in una prospettiva di *data privacy*, la coodetenzione (da parte di tutti i nodi della catena) di ciascun dato di cui si compongono le catene di blocchi. Questa imprescindibile coodetenzione rappresenta, al contempo, un punto di forza in caso di informazioni sottoposte ad obbligo di pubblicità obbligatoria, come di debolezza in presenza di dati personali.

Inoltre, con riferimento alla modalità ad accumulo "add-only" (propria del processo di immissione dei dati in un'infrastruttura *blockchain*) vi è stato chi ha sostenuto la sua capacità di «generare conflitti con il principio di minimizzazione, messo alla prova dal

fatto che, in presenza di uno schema a transazioni disintermediate, ciascuna delle operazioni svolte in seno all'infrastruttura è necessaria per l'abilitazione dell'ultima transazione in ordine di tempo»[92].

Infine, nell'ottica di un'effettiva garanzia della compliance della piattaforma *blockchain* rispetto al quadro giuridico in materia di protezione dati, è il caso di ricordare come il titolare debba essere in grado di dimostrare la necessità del ricorso ad una specifica tecnologia, nonché l'assenza di eventuali opzioni ad essa alternative, che possano ragionevolmente essere adottate per il raggiungimento del medesimo scopo. Circostanza, a margine della quale, pare utile interrogarsi sull'attuale sviluppo delle *data science*, altresì sulla pluralità di strumenti offerti alle amministrazioni pubbliche dalle tecnologie dell'informazione e della comunicazione.

Nonostante un orizzonte d'azione così denso di opportunità e strumenti, pare dunque opportuno domandarsi in che modo le catene di blocchi potrebbero dimostrarsi maggiormente efficaci ed efficienti rispetto ad altri approcci di governance del dato.

Proprio la *data governance* risulta foriera di utili spunti di riflessione, circa ulteriori profili problematici ascrivibili alla tecnologia di Satoshi Nakamoto.

Un preliminare distinguo, funzionale ad una piena comprensione delle prefate criticità, si attesta lungo il discrimine che distingue le *blockchain* aperte (o *permissionless*) da quelle private (*permissioned*). La prima tipologia non appare impiegabile nella vita delle pubbliche amministrazioni in ragione dell'assenza di qualsivoglia barriera all'accesso, da cui consegue che ciascun operatore (disponendo liberamente delle chiavi crittografiche) può godere di un pieno anonimato. Una simile infrastruttura, composta da un numero indeterminato di nodi disseminati per il globo terracqueo, rischia di sfuggire ad un qualsiasi sindacato giurisdizionale. «Si tratta insomma di una tecnologia che si presta a sfuggire al controllo statale, a sottrarsi alla legge, più che a promuovere l'efficace attuazione del diritto»[93]. Essa si dimostra, piuttosto, come «un'arena le cui regole non sono prodotte da organismi statuali o sovranazionali, certamente imperfetti ma sottoposti in varie forme al pubblico scrutinio, ma sono dettate da un'*élite* di neonotabili dall'incerto *pedigree*»[94].

Secondo avvertita dottrina, tuttavia, anche con riferimento alla seconda tipologia di *blockchain* sussisterebbero alcuni aspetti critici. Ad esempio, una simile infrastruttura potrebbe comunque essere definita "insostenibile", perché caratterizzata da «un'architettura complessa, definita "energivora" in quanto fonte di un consumo particolarmente elevato di energia e per questa ragione dispendiosa e ad elevato impatto ambientale»[95]. Pertanto, l'impiego di database centralizzati sarebbe da preferire in via generale (nonostante la loro superiore fragilità infrastrutturale) sulla base della loro maggiore efficienza e rapidità di calcolo. La *blockchain*, pur essendo «più robusta»[96], sarebbe caratterizzata da maggiori tempi di elaborazione, nonché da elevati costi[97] (tanto ecosistemici quanto strettamente economici), conseguenza dell'elevato numero di calcolatori, necessari al suo funzionamento. Il ricorso alle catene di blocchi, dunque, dovrebbe necessariamente fondarsi sulla base di specifiche ragioni per l'assunzione dei predetti costi, la più evidente delle quali «è la mancanza di un'autorità riconosciuta da parte di tutti i soggetti interessati»[98] dall'infrastruttura.

È il caso di sottolineare come, nonostante siano stati rilevati taluni benefici ambientali[99], pur essendo stato possibile scorgere "un certo margine di ottimizzazione della spesa pubblica", a seguito dell'impiego di questa tecnologia nella vita delle amministrazioni, si assisterebbe alla produzione di esternalità negative, probabilmente in grado di attenuare i margini di utilità attesi dai promotori di un simile impiego della *blockchain*.

Una simile analisi, poi, potrebbe essere svolta con riguardo agli *smart contract* che, come già evidenziato, rappresentano la proiezione dinamica delle potenzialità delle DLT.

«Per quanto la *blockchain* rappresenti una struttura affidabile, quella della sicurezza è una delle principali problematiche inerenti agli *smart contract*»[100], come dimostrato, a più riprese, dai furti plurimilionari perpetrati sulle piattaforme *blockchain* (prima tra tutte quella "Ethereum"), sfruttando i *bug* presenti negli algoritmi di una larga fetta dei "contratti intelligenti" presenti nell'infrastrutture[101]. Tuttavia, margini di vulnerabilità degli *smart contract* devono anche essere ricercati all'esterno dell'algoritmo. Si pensi, in tal senso, all'impiego dei già citati *oracle* ed alla loro potenziale manomissione (a seguito della quale si potrebbe indurre in errore il calcolatore)[102]. Ulteriori criticità sono, poi, ascrivibili alla performance e, specificatamente, alla «limitata scalabilità e latenza proprie della struttura *blockchain*»[103], a cui si somma l'irreversibilità degli errori, da cui consegue (salvo eccezioni) la stipulazione di un nuovo *smart contract*.

L'impiego su larga scala dello *smart contract*, inoltre, pone interrogativi in ordine agli effetti dell'eventuale illegittimità dell'output di un contratto intelligente.

Infine, è stato segnalato come «qualunque previsione contrattuale, demandata in teoria al giudi-

ce, semplicemente potrebbe non essere prevista dall'algoritmo» e, in tal caso, «nessuna autorità può intervenire per contrastare gli effetti dell'automatismo, quantomeno alla stessa velocità dello *smart contract*»[104].

6. Alcune riflessioni conclusive

«Se la *blockchain* è stata originariamente creata per eliminare il bisogno di terze parti, il paradosso è che gli attori economicamente rilevanti oggi coinvolti nella *blockchain governance* giocano il classico ruolo del *tertius gaudens*»[105], che ottiene benefici economici nel sostituire lo Stato in alcune o tutte le sue funzioni. Cosa anche peggiore, questi soggetti potrebbero intenzionalmente condurre strategie finalizzate «a compromettere l'attuale ordine democratico, modificarne i rapporti di forza e ottenere una posizione dominante nella società»[106].

In un simile orizzonte si colloca la tecnologia di Satoshi Nakamoto. Nel medesimo contesto occorre calare un'attenta riflessione circa le ragioni di un crescente interesse (da parte delle pubbliche amministrazioni) per i possibili impieghi istituzionali delle DLT; interrogativo a cui si riconnette il secondo paradosso della vicenda *blockchain* o, piuttosto, il volto pubblicistico del paradosso di cui sopra.

Le catene di blocchi, nate per erodere definitivamente il rapporto tra cittadino e Stato, appaiono (agli occhi di quest'ultimo) quali formidabili strumenti di rivalsa, perché in grado di ricostituire un rapporto di fiducia tra Stato apparato e Stato comunità, da tempo compromesso. Allora, in un simile scenario, riflettere sull'*an* e sul *quomodo* dell'introduzione della *blockchain* in seno alla vita delle amministrazioni significa interrogarsi sul futuro dello Stato, sulla sua collocazione nella vita del tessuto economico-sociale, nonché sul futuro stesso dell'essere umano (sempre più individuo e sempre meno persona). Nel solco di un simile interrogativo, se non si intende cedere alla distopia *cypherpunk*, non resta che difendere lo Stato nella sua accezione olistica (apparato e comunità). Una difesa che, come sostenuto in dottrina, passa dalla decisa riaffermazione del «primato della politica sull'economia» e, in un certo senso, del comma sul *byte*; riconoscendo la necessità di un coordinamento sociale (da conseguirsi anche per il tramite di un oculato impiego delle DLT), attraverso il quale «le tensioni tra interessi centrali e periferici siano elaborate nel segno di un adeguato compromesso politico»[107].

Ciò non implica accogliere in *bonam partem* l'ingresso delle DLT nella vita delle amministrazioni, né ritenere tollerabile lo *status quo ante blockchain*, bensì ritornare, come suggerito in dottrina, «allo spirito originario delle nostre Costituzioni»[108] e, in funzione della loro garanzia, introdurre quegli strumenti informatici e telematici capaci di garantire un saldo sociale, economico e politico di segno positivo, avendo cura di non cedere (nel processo di loro implementazione) al distruttivo "fascino della zampa di scimmia"[109].

Note

[1] K. Schwab, *La quarta rivoluzione industriale*, Franco Angeli, 2016.

[2] C. Sarra, *Il mondo dato. Saggi su datificazione e diritto*, Cleup, 2019, p. 104.

[3] Per approfondimenti, si v. sul punto A.M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain: Unlocking Digital Cryprocurrencies*, Oreilly & Associates, 2017.

[4] A. Saporito, *L'intelligenza artificiale nel procedimento amministrativo: il sistema della tecnologica Blockchain*, in "Ambientediritto", 2021, n. 4, p. 6.

[5] C. Sarra, *op. cit.*, p. 110.

[6] A. Saporito, *op. cit.*, p. 6; per ulteriori dettagli circa i profili tecnici della *blockchain*, la cui conoscenza si rende necessaria per giungere ad una piena comprensione delle implicazioni giuridiche del suo funzionamento, si v. C. Sarra, *op. cit.*, pp. 107-112.

[7] Si pensi al contributo offerto in materia da Philip Zimmerman e da Daniel Bernstein. Per approfondimenti, si v. L. Paccagnella, *Il potere dei codici: crittografia, cypherpunk e movimenti sociali*, in "Quaderni di sociologia", 2000, n. 23, pp. 48-63, a pp. 53-54.

[8] *Ivi*, p. 55.

[9] Ci si riferisce a E. Hughes, *A Cypherpunk's Manifesto*, 1993. Ulteriori spunti sono poi offerti da T. May, *The Crypto Anarchist Manifesto*, 1988.

[10] L. Paccagnella, *op. cit.*, p. 56.

[11] *Ibidem*.

[12] Con l'espressione *silicon swan* ci si riferisce al modello economico del cigno nero, identificando nel lemma *silicon* un chiaro riferimento alla Silicon Valley, dimensione geografica in cui la comunità *cypherpunk* ha mosso i suoi primi passi.

[13] M. Ippolito, *La disintermediazione dei processi nella Pubblica Amministrazione: l'impatto della tecnologia blockchain*, in "AmbienteDiritto", 2021, n. 2, p. 41 ss.

[14] Con riferimento alle DLT, *rectius* alla tecnologia *blockchain*, l'articolo 8-*ter* co. 1 recita: «Si definiscono tecnologie basate su registri distribuiti le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».

[15] Si v. per approfondimenti: Associazione Italiana per la Sicurezza Informatica, *Blockchain & Distributed Ledger: aspetti di governance, security e compliance*, 2019, p. 35 p.

[16] *Ivi*, p. 36.

[17] Ministero dello sviluppo economico, *Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain Sintesi per la consultazione pubblica*, 2020.

[18] Id., *Case delle tecnologie emergenti, finanziati 5 nuovi progetti*, 2020.

[19] Istituito nello stato di previsione del Ministero dello sviluppo economico dall'art. 1, co. 226, della l. 30 dicembre 2018, n. 145, come modificato dall'art. 39-*ter*, co. 1, del d.l. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla l. 11 settembre 2020, n. 12, per interventi volti a favorire lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, *blockchain* e *Internet of things*.

[20] Decreto interministeriale 6 dicembre 2021 - *Fondo per interventi volti a favorire lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, blockchain e Internet of things*, art. 3.

[21] Infratel Italia (Infrastrutture e Telecomunicazioni per l'Italia s.p.a.) è una società in-house del Ministero dello Sviluppo Economico, attiva dal 2005, afferente al Gruppo Invitalia.

[22] Nelle forme del finanziamento agevolato, del contributo in conto impianti, del contributo in conto capitale, del contributo diretto alla spesa e del contributo in conto interessi.

[23] *Ex* art. 7-*bis*, co. 2, del d.l. 29 dicembre 2016, n. 243, convertito, con modificazioni, dalla l. 27 febbraio 2017.

[24] In dettaglio, le regioni coinvolte sono: Abruzzo, Molise, Campania, Basilicata, Calabria, Puglia, Sicilia e Sardegna.

[25] Ministro per l'innovazione tecnologica e la digitalizzazione, *Strategia Nazionale per le Competenze Digitali (Release 1.0)*, 2020.

[26] *Ivi*, p. 25.

[27] *Ivi*, p. 28.

[28] *Ivi*, p. 12.

[29] AGID, *Task force IA*, 2020

[30] Id., *Blockchain: AgID promotrice dell'infrastruttura italiana IBSI*, 2021. Cfr. C.P. Guarini, *Pubblica amministrazione e cittadinanza digitale. Prime riflessioni tra evoluzione normativa e questioni di sistema*, in "I Battelli del Reno", 24 ottobre 2021, p. 3 ss.

[31] Comune di Cinisello Balsamo, *La sfida della tecnologia blockchain continua anche quest'anno*, 25 settembre 2020.

[32] *Ibidem*.

[33] *Ibidem*.

[34] *Ibidem*.

[35] Università degli Studi di Milano Bicocca, *Bicocca rilascia le prime certificazioni di laurea Blockcerts*, 2019.

[36] *Ibidem*.

[37] *Ibidem*.

[38] *Ibidem*.

[39] Comune di Bari, *La blockchain per una gestione distribuita e condivisa dei servizi pubblici: il contributo del Comune di Bari alla 30ª edizione del Forum P.A.*, 17 maggio 2019.

[40] *Ibidem*.

[41] *Ibidem*.

[42] *Ibidem*.

[43] *Ibidem*.

[44] *Ibidem*.

[45] *Ibidem*.

[46] Ministero dell'Economia e delle Finanze, *Con il progetto SUNFISH il MEF all'avanguardia in Europa sui servizi cloud e la cybersecurity*, 9 novembre 2017.

[47] Id., *Identità digitale, con Poseidon il MEF sperimenta nuovi servizi per 2 milioni di dipendenti pubblici*, Comunicato stampa n. 167, 25 ottobre 2018.

[48] È possibile definire *exchanger*, quel soggetto che presta servizi relativi all'utilizzo di valuta virtuale.

[49] Si qualifica come *wallet provider*, quel soggetto che offre servizi connessi alla gestione di un portafoglio digitale.

[50] Espressione coniata da M.J. Casey, P. Vigna, *La macchina della verità. La blockchain e il futuro di ogni cosa*, Franco Angeli, 2018.

[51] C. Sarra, *op. cit.*, p. 114.

[52] G. Gallone, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in "Il diritto dell'economia", 2019, n. 3, p. 192.

[53] *Ivi*, p. 193.

[54] *Ibidem*.

[55] Utili spunti sono offerti dalla dottrina italiana. Si v. diffusamente V. Berlingò, *Il fenomeno della datafication e la sua giuridicizzazione*, in "Rivista Trimestrale Diritto Pubblico", 2017, n. 3, p. 641 ss.; F. Costantino, *Lampi. Nuove frontiere delle decisioni amministrative tra open e biga data*, in "Diritto Amministrativo", 2017, n. 4, p. 799 ss.; V. Zeno-Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in "MediaLaws", 2018, n. 2.

[56] L'espressione *nudging* è da ricondursi a C.R. Sunstein, R.H. Thaler, *Nudge. La spinta gentile* (trad. it. A. Oliveri), Feltrinelli, 2019.

[57] A. Micello, *La tecnologia blockchain al servizio della gestione delle informazioni ambientali: verso un "Blockchained Green Public Procurement?"*, in "Rivista Quadrimestrale di Diritto dell'ambiente", 2018, n. 3.

[58] *Convenzione sull'accesso alle informazioni, la partecipazione del pubblico ai processi decisionali e l'accesso alla giustizia in materia ambientale*, Århus, 25 giugno 1998.

[59] G. Gallone, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, cit., p. 194.

[60] *Ibidem*.

[61] A. Micello, *op. cit.*, p. 83.

[62] G. Arena, *Introduzione all'amministrazione condivisa*, in "Studi parlamentari e di politica costituzionale", 1997, n. 117/118, p. 30 ss., a p. 46.

[63] D.l. 14 dicembre 2018, n. 135, art. 8-*ter*, co. 3.

[64] G. Gallone, *La Pubblica Amministrazione alla prova dell'automazione contrattuale. Note in tema di* smart contracts, in "Federalismi.it", 2020, n. 20, p. 149.

[65] Si v. sul punto: A.G. Orofino, *Profili giuridici della trasparenza amministrativa*, Cacucci, 2013; F. Manganaro, *Evoluzione del principio di trasparenza amministrativa*, in "Astrid", 21 dicembre 2009; A. Natalini, G. Vesperini, *Il big bang della trasparenza*, Editoriale Scientifica, 2015.

[66] Cfr. G. Gallone, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, cit., p. 210.

[67] Cfr. G. Gallone, *La Pubblica Amministrazione alla prova dell'automazione contrattuale*, cit., p. 150.

[68] T.A.R. Sicilia, Palermo sez. II, 6 settembre 2018, n. 1905.

[69] T.A.R. Toscana, sez. III, 17 aprile 2019, n. 577.

[70] Cfr. L. Minervini, *Accesso agli atti e procedure di affidamento ed esecuzione di contratti pubblici*, in "Foro Amministrativo", 2019, n. 5, p. 949.

[71] D.lgs. 18 aprile 2016, n. 50, art. 110.

[72] G. Gallone, *La Pubblica Amministrazione alla prova dell'automazione contrattuale*, cit., p. 152, che riprende le considerazioni già espresse da L. Mundula, *La corruzione: dalle determinanti alle modalità di contrasto*, in M. D'Alberti (a cura di), "Corruzione e pubblica amministrazione", Jovene, 2017; S. Rose-Ackerman, *Corruption: Greed, Culture and the State*, in "The Yale Law Journal Online", vol. 120, 2010, p. 125-140.

[73] Cfr. J.D. Carrillo, *Corruption in Hiérarchies*, in "Annales d'Économie et de Statistique", 2000, n. 59, pp. 37-61.

[74] G. Gallone, *La Pubblica Amministrazione alla prova dell'automazione contrattuale*, cit., p. 151.

[75] C. Sarra, *op. cit.*, p. 115.

[76] Il *Building Information Modeling* (BIM) è un insieme di tecnologie, processi e politiche che consentono a più parti interessate di progettare, costruire e gestire in modo collaborativo una struttura nello spazio virtuale.

[77] C. Kinnaird, M. Geipel, M. Bew MBE, *Blockchain Technology. How the Inventions Behind Bitcoin are Enabling a Network of Trust for the Built Environment*, ARUP, 2014, p. 46.

[78] A. Micello, *op. cit.*, p. 105.

[79] G. Gallone, *La Pubblica Amministrazione alla prova dell'automazione contrattuale*, cit., p. 150.

[80] Cfr. S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (trad. it. P. Bassotti), LUISS University Press, 2019.

[81] G. D'Acquisto, *Blockchain e GDPR: verso un approccio basato sul rischio*, in "Federalismi.it", 2021, n. 2, p. 56.

[82] *Ibidem*.

[83] *Ibidem*.

[84] *Ibidem*.

[85] S. Ciucciovino, M. Faioli, A. Toscano et al., *La* blockchain *nel mercato del lavoro italiano: una struttura non relazionale*, in "Federalismi.it", 2021, n. 2, 35 p.

[86] Sul punto, A.M. Gambino, C. Bomprezzi, *Blockchain e protezione dei dati personali*, in "Il Diritto dell'informazione e dell'informatica", 2019, n. 3, pp. 619-646.

[87] M. Macchia, *Blockchain e pubblica amministrazione*, in "Federalismi.it", 2021, n. 2, pp. 117-129.

[88] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, art. 42.

[89] G. D'Acquisto, *op. cit.*, p. 57.

[90] In tema di anonimizzazione, si v. G. D'Acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, 2017.

[91] G. D'Acquisto, *op. cit.*, p. 57.

[92] *Ivi*, p. 54.

[93] M. Macchia, *op. cit.*, p. 119.

[94] U. Bechini, *Da Berlino a Dublino e Pechino: sulle tracce della Blockchain*, in "Rivista del Notariato", 2018, n. 6, pp. 1181-1190.

[95] M. Macchia, *op. cit.*, p. 119.

[96] *Ibidem*.

[97] Alcune stime a riguardo sono offerte da Labella, che sottolinea come «tutta la tecnologia delle varie *blockchain* sparse nel mondo ha comportato l'utilizzazione di un quantitativo di energia nell'anno 2017 pari a circa 35 terawatt (cioè 35 milioni di megawatt, 7 in più di quelli consumati da tutta l'Irlanda nello stesso anno) mentre per l'anno 2019 si stima che il consumo sia arrivato a 48 tW». Si v. E. Labella, *Gli smart contract: riflessioni sulle prestazioni "autoesecutive" nel sistema di blockchain*, in "MediaLaws", 2020, n. 3. Per ulteriori approfondimenti, diffusamente L. Parola, P. Merati, G. Gavotti, *Blockchain e smart contract*, in "I Contratti", 2018, n. 6, pp. 681-688.

[98] Si pensi all'esempio avanzato da Bechini, con riferimento ad una possibile piattaforma funzionale al monitoraggio del traffico commerciale marittimo su scala planetaria, che abbia tra i propri partner UE, USA e Cina. U. Bechini, *op. cit.*, p. 1189.

[99] Cfr. A. Micello, *op. cit.*

[100] S. Ciucciovino, M. Faioli, A. Toscano et al., *op. cit.*, p. 34.

[101] Si pensi, ad esempio, al furto, del 2022, di 320 milioni di dollari in criptovaluta Ethereum dalla piattaforma Wormhole, a quello del 2021, (pari a più 600 milioni di dollari) dalla piattaforma DeFi Poly Network, nonché a quello del 2016 perpetrato ai danni di una *Decentralize Autonomous Organizations* (DAO) di Ethereum, stimato in 55 milioni di dollari. Quanto a quest'ultimo, si rinvia per approfondimenti a C. Sarra, *op. cit.*, pp. 119-123.

[102] Per approfondimenti, cfr. V. Gatteschi, F. Lamberti, C. Demartini et al., *Blockchain and smart contracts for insurance: Is the technology mature enough?*, in "Future Internet", 20 febbraio 2018.

[103] S. Ciucciovino, M. Faioli, A. Toscano et al., *op. cit.*, p. 34.

[104] E. Labella, *op. cit.*, p. 42.

[105] G. Simmel, *Die quantitative Bestimmheit der Gruppe*, in Id., "Soziologie, Untersuchungen über die Formen der Vergesellschaftung" (1a ed.), Duncker & Humblot, 1908; P. Portinaro, *Il terzo. Una figura del politico*, Franco Angeli, 1986.

[106] M. Atzori, *Tecnologia blockchain e governance decentralizzata: lo Stato è ancora necessario?*, disponibile in SSRN, 2015, p. 36.

[107] *Ibidem*.

[108] *Ibidem*.

[109] Con questa espressione ci si riferisce alle riflessioni di Claudio Sarra che, nel suo "Il mondo-dato" del 2019, affronta, in prospettiva filosofico giuridica, i margini di criticità della tecnologia *blockchain*, richiamando quanto sostenuto da Norbert Wiener (nel volume "Dio & Golem S.P.A." del 1991) circa la responsabilità morale e la consapevolezza critica che dovrebbe accompagnare l'affidamento alla "magia" dell'automazione. L'Autore, in tal senso, ricorda come «l'aumento della potenza che essa consente, lungi dal semplificare la vita dell'uomo, la grava, invece, di ben più difficili compiti».

* * *

Nakamoto's paradox: expected utilities and potential dangers of an institutional use of blockchain technology

Abstract: The contribution, electing the shortlist of Italian administrative experiments in the blockchain field as its heuristic laboratory, will try to present (in a public law perspective) the main repercussions of this technology public use on the citizen life, as well as of the State apparatus, increasingly invested by the transformative effect of the fourth industrial revolution. In this sense, the aim of this article is highlight both the possible utilities with an institutional use of the blockchain, and the dangers of which it would seem to be a harbinger.

Keywords: Blockchain – Public Administrations – State – Anarchocapitalism – Digital Administration

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0071
Articolo sottoposto a peer review

Una governance dei dati genetici per lo sviluppo della ricerca scientifica

Dimitri Martignago

Per la prima volta nel panorama normativo europeo, il GDPR ha introdotto il concetto di "dati genetici" che ha fra i principali campi di impiego quello della ricerca scientifica. Con l'obiettivo di contribuire ad un più ampio dibattito in materia, l'articolo intende affrontare la disciplina prevista dal dettato normativo per il trattamento dei dati genetici a fini di ricerca scientifica. Nello specifico, lo scopo dell'articolo è quello di esaminare ed approfondire l'insieme delle misure tecniche ed organizzative individuate dal legislatore europeo al fine di conciliare il rispetto dei diritti e delle libertà fondamentali degli individui con le necessità di sviluppo della ricerca scientifica e dunque le possibili deroghe ai diritti individuali. In particolare, partendo dalla disciplina introdotta dall'articolo 89 del Regolamento verranno fra l'altro presentate le tecniche di anonimizzazione e quelle di pseudonimizzazione per il trattamento dei dati genetici; il possibile spazio applicativo delle *distributed ledger technologies* e della *blockchain*, nonché quella parte di misure tecniche ed organizzative indicate dalle varie linee guida delle autorità nazionali per la protezione dei dati personali, oltre ai principi della *privacy by design* e *by default*. Un ultimo approfondimento sarà infine rivolto alle certificazioni e alla necessità di un impiego su scala internazionale di codici di condotta settoriali condivisi tra più Stati per superare le barriere nazionali che ad oggi rappresentano un freno alla ricerca genetica.

GDPR – Governance dei dati – Dati genetici – Ricerca scientifica

Sommario: *1. Introduzione – 2. L'anonimizzazione – 3. Misure tecniche e organizzative – 3.1. La pseudonimizzazione – 3.2. La protezione dei dati* by design *e* by default *– 3.3. Le misure di sicurezza e la valutazione del rischio – 3.4. La co-regolamentazione, tra codici di condotta e certificazioni – 4. Conclusione*

1. Introduzione

Gli sviluppi tecnologi e scientifici dell'ultimo decennio hanno consentito un'accelerazione improvvisa del progresso della ricerca genetica. La quantità di informazioni potenzialmente estraibili dai dati genetici li rende di estrema rilevanza tanto per ragioni sanitarie quanto per i risvolti nel contesto della ricerca scientifica. Per queste ragioni la tutela normativa dei dati genetici ha recentemente raccolto l'interesse di legislatori ed opinione pubblica con particolare riguardo alle questioni di carattere etico e pratico da risolvere, soprattutto a fronte del vertiginoso aumento dei test genetici diretti al consumatore (DTC) nonché dei potenziali rischi legati allo sviluppo della medicina personalizzata. La complessità e la sensibilità delle informazioni genetiche comportano un elevato rischio di abuso da parte di chi dispone dei dati e dei soggetti terzi in grado di identificare in maniera univoca i singoli interessati[1]. La quantità di informazioni potenzialmente estraibili da essi li rende di

D. Martignago si occupa di sviluppo dell'Innovazione nell'ambito della compliance e della responsabilità d'impresa in ReD OPEN S.r.l., spin-off partecipato dell'Università degli Studi Milano-Bicocca.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

estrema rilevanza, soprattutto in virtù del fatto che buona parte del genoma di un individuo è condivisa anche dai suoi parenti. Questi rischi riguardano tanto le informazioni genetiche già estratte, quanto quelle potenzialmente estraibili da ogni genere di campione biologico. Ciononostante, il COVID-19 ed il rischio di nuove pandemie su scala globale ha evidenziato l'imperatività di una maggiore condivisione dei dati non solo per il progresso della ricerca scientifica, ma anche per favorire la proposta di nuovi trial clinici[2].

Nonostante il DNA di per sé non sia altro che un insieme di nucleotidi incatenati tra loro, le interpretazioni che vengono adottate e le informazioni da esso estratte possono determinare l'insorgere di discriminazioni o di violazioni di molteplice natura.

In considerazione della sostanziale riduzione dei costi di sequenziamento avvenuta negli ultimi anni, secondo recenti stime il mercato dei test genomici potrebbe subire una crescita repentina nei prossimi quattro o cinque anni, arrivando a toccare la soglia di 35,7 miliardi di euro. La conseguenza diretta di queste stime è che con il passare degli anni saranno sempre di più i soggetti coinvolti in maniera diretta o indiretta dal trattamento dei dati genetici, anche alla luce del fatto che i dati genetici riguardano tanto il soggetto da cui provengono quanto la sua parentela.

Dal 2016, con il GDPR, i dati genetici sono stati inclusi tra quelle categorie di dati particolari che, in virtù dell'articolo 9, non possono essere trattate a meno del ricorrere di una delle ipotesi previste al secondo paragrafo dello stesso. Ad esempio, laddove il trattamento sia condotto per finalità di ricerca scientifica questo dovrà avvenire, oltre che nel rispetto del principio di proporzionalità e dell'essenza del diritto alla protezione dei dati personali, adottando «delle misure adeguate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato»[3] e in conformità con l'articolo 89, paragrafo 1 del GDPR. Quest'ultimo stabilisce dei generici standard di riferimento il cui rispetto è necessario non solo laddove ci si desideri avvalere della possibilità *ex* articolo 89(2) del GDPR di derogare ai diritti individuali per finalità di ricerca scientifica, ma, ancor prima, nei casi in cui per la stessa finalità, si vogliano trattare dati genetici in deroga al divieto imposto all'articolo 9 del GDPR.

Riconoscendo il trattamento per finalità di ricerca scientifica come una possibile eccezione al divieto di trattare i dati particolari, il Regolamento demanda ai singoli Stati membri, alle organizzazioni, alle associazioni e ai titolari del trattamento l'individuazione di una disciplina più specifica per quel che concerne sia le deroghe ai diritti individuali *ex* articolo 89(2), sia le misure con cui garantire il rispetto del Regolamento e la tutela dei diritti individuali. Per poter portare a termine un trattamento a fini di ricerca scientifica è dunque necessario tener presente che questo deve essere «soggetto a garanzie adeguate per i diritti e le libertà dell'interessato»[4], in conformità con il GDPR. Pur non precisando in maniera esaustiva in che cosa consistano dette garanzie[5], l'articolo 89(1) continua affermando che queste «assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati»[6]. Se però la finalità di ricerca scientifica può essere conseguita «attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato»[7], ossia con un dato anonimo o anonimizzato, la norma impone che venga conseguita in tal modo. In virtù di ciò, per poter trattare i dati a fini di ricerca scientifica la prima opzione da prendere in considerazione è l'anonimizzazione o comunque l'uso di dati anonimi. Solo una volta scartata questa ipotesi si potrà quindi valutare l'adozione delle altre misure tecniche e organizzative disponibili.

2. L'anonimizzazione

Non esiste un'interpretazione dei termini *anonimia*, *anonimizzazione* e *identificazione* che sia condivisa dalla comunità internazionale. Nella stessa Unione europea il concetto di "dato anonimo" può essere inteso in maniera differente[8].

Nel GDPR viene innanzitutto stabilito che il «regolamento non si applica [...] al trattamento di [...] informazioni anonime, anche per finalità statistiche o di ricerca»[9]. Per poter anonimizzare dei dati personali però il sistema deve anzitutto essere alimentato con dei dati personali che potranno esser considerati anonimi solo a seguito dell'applicazione delle tecniche di anonimizzazione più adeguate[10]. Per questa ragione, il trattamento con cui si procede a privare i dati personali di tutti gli elementi identificativi, ossia l'anonimizzazione, è da considerarsi senza alcun dubbio un trattamento ulteriore dei dati personali e in quanto tale sottostà alle regole imposte dal Regolamento e all'obbligo del previo consenso, salve le eventuali eccezioni.

Esistono due generi di tecniche di anonimizzazione: la randomizzazione, che consiste nell'attenuare il legame tra la persona e i dati che lo riguardano così che, noti i dati randomizzati, non si possa risalire all'individuo[11], e la generalizzazione «che consiste nel rendere meno dettagliati o diluire gli attributi delle persone interessate presenti in una tabella modificando la rispettiva scala o ordine di grandezza in modo che più righe di quella tabella presentino la stessa combinazione di attributi generalizzati»[12].

In ambito genetico le tecniche che hanno generato maggior interesse da parte della comunità scientifica sono ad ora la *differential privacy*, tra i metodi di randomizzazione, la *k-anonimity* e la *l-diversity*, tra quelli di generalizzazione[13]. In ogni caso le rilevanti problematiche connesse all'anonimizzazione, laddove applicata al contesto dei dati genetici, sembrerebbero non renderla mai preferibile da un punto di vista scientifico[14]. Dal momento che i dati genetici sono la rappresentazione biologica di un singolo individuo, anche laddove il loro collegamento con l'identità civile dovesse essere cancellato, rimarrebbero estremamente personali e questo renderebbe difficile, se non impossibile, pensare che possano essere anonimizzati come avviene con altri dati[15].

Le conseguenze riguardano tanto i ricercatori quanto gli interessati. Nell'ambito delle ricerche svolte dalle biobanche, ad esempio, l'efficacia degli studi sui tessuti dipende dalle cosiddette informazioni di follow-up e quindi dalla storia clinica aggiornata dei soggetti da cui sono stati prelevati[16]. In questo settore un dato anonimizzato rischierebbe quindi di vanificare gli sforzi fatti, non permettendo di risalire al soggetto originario.

Sulla base dell'opinione rilasciata dal WP29, sono stati delineati tre fattori da tenere in considerazione laddove si desideri fare affidamento sulle tecniche di anonimizzazione dei dati[17].

In primo luogo, il titolare deve tenere conto dei mezzi necessari affinché un dato possa essere reso anonimo, valutando costantemente le tecnologie disponibili in termini di capacità di calcolo, nonché gli algoritmi sviluppati in grado di invertire il processo e quindi rendere identificabile la persona, de-anonimizzando i dati.

Bisogna poi sempre considerare il fatto che molti dataset disponibili al pubblico, nonostante vengano definiti anonimi, in realtà non rispondono agli standard di sicurezza richiesti. La portata di questo requisito è di particolare importanza, soprattutto considerato che impone in capo al titolare l'obbligo di considerare non solo la propria capacità nel de-anonimizzare i dati, ma anche quella di altri soggetti, conosciuti o meno, che, considerato lo sviluppo tecnologico e le altre fonti di dati pubblicamente disponibili, potrebbero risalire al soggetto interessato.

Già nel 2013 Yaniv Erlich dimostrò che, utilizzando informazioni pubbliche, era possibile risalire ad alcuni partecipanti che avevano contribuito con il proprio DNA ad un progetto di ricerca scientifica[18]. Lo stesso Erlich, in uno studio condotto nel 2018[19], arrivò a dimostrare che, da un dataset di 1,28 milioni di campioni prelevati ad individui anonimi, era possibile risalire al 60% della popolazione statunitense con origini europee. Lo studio documentò inoltre come, laddove un database genetico arrivi a contenere i dati del 2% degli adulti appartenenti ad una determinata etnia, nonostante l'anonimizzazione, sarebbe quasi certa la possibilità di individuare una corrispondenza tra ognuno di questi individui e un cugino di terzo grado o più prossimo. In aggiunta, ulteriori ricerche condotte nella comunità scientifica hanno dimostrato come, anche in mezzo ai dati di molti individui, sia possibile recuperare i dati personali di un singolo soggetto risalendo ad essi da aggregati di polimorfismi a singolo nucleotide, anche laddove si faccia uso di soli 25 loci selezionati in maniera casuale[20].

Tornando ai fattori da considerare nel caso in cui si desideri anonimizzare un dato, il terzo, ed essenziale, elemento aggiuntivo individuato corrisponde all'obbligo per il titolare del trattamento di non fare affidamento sulle proprie intenzioni, dovendo piuttosto valutare la propria disponibilità di altri dati il cui riferimento incrociato con il dataset potenzialmente anonimizzato potrebbe identificare i soggetti a cui i dati fanno riferimento. Molti progetti di ricerca, infatti, non trattano solo dati genetici, ma ne fanno un uso combinato ad altri dati riguardanti fattori non genetici come le variabili legate allo stile di vita o dati socioeconomici[21]. Lo stesso concetto è infatti ribadito al considerando 26 del GDPR in base al quale, se le informazioni anonime sono da considerarsi come quelle che non si riferiscono ad una persona fisica identificata o identificabile, «[p]er stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi [...] di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente»[22].

Pur non potendo affermare che i dati genetici non possano essere anonimizzati in generale[23], è comunque importante sottolineare che, in questo settore, nessuno scienziato responsabile potrebbe garantire un rispetto assoluto della privacy, ed infatti le linee guida internazionali per la ricerca stanno prendendo le distanze dall'anonimizzazione per ragioni legate alla qualità dei dati, al ritiro dei partecipanti alle ricerche e per la necessità di divulgare le scoperte oltre che di collegare in maniera continuativa questi dati con quelli clinici o altri ancora[24].

Alla luce di ciò, della scarsa utilità derivabile dall'anonimizzazione genetica e dei costi che simili tecniche potrebbero comportare, sembrerebbe necessario andare oltre, interrogandosi in merito a quelle misure tecniche e organizzative che il GDPR impone di predisporre in generale al fine di «garantire il rispetto delle disposizioni del [...] regolamento»[25], dei diritti e delle libertà degli individui e, più nello specifico, così da «attuare in modo efficace i prin-

cipi di protezione dei dati, quali la minimizzazione»[26], e soddisfare «i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default»[27].

3. Misure tecniche e organizzative

L'obiettivo di garantire il rispetto delle disposizioni del GDPR e di assicurare le adeguate garanzie ai diritti e alle libertà individuali tramite l'adozione di misure tecniche e organizzative appropriate non trae origine dall'articolo 89 del Regolamento, ma costituisce piuttosto un tassello essenziale di quel concetto espresso tramite il principio di accountability[28], su cui si sviluppa buona parte del testo legislativo.

Se infatti la precedente normativa era «focalizzata sui diritti dell'interessato»[29] il testo del GDPR «si sviluppa essenzialmente su processi, attività, misure tecniche ed organizzative, sanzioni e obblighi rivolti a[l] titolare e [al] responsabile del trattamento»[30]. E sulla base della formulazione adottata dal legislatore europeo, si può poi notare come, lì dove la norma tratta con maggior riguardo il principio di minimizzazione dei dati rispetto agli altri principi della protezione dei dati, nel caso delle singole misure da implementare, è la pseudonimizzazione ad esser stata posta come punto di riferimento in svariati articoli[31], nonostante le molte questioni aperte in merito al suo utilizzo.

3.1. La pseudonimizzazione

Tra i metodi di de-identificazione, il termine pseudonimizzazione normalmente raggruppa quelle tecniche volte a sostituire con uno pseudonimo gli identificatori diretti, quali ad esempio il nome, il cognome e il numero di telefono, conservando però quelli che vengono definiti come quasi-identificatori o identificatori indiretti[32]. La possibilità che un identificatore sia in grado di condurre all'identificazione di un soggetto dipende sempre dal contesto. In certi casi, infatti, un nome e un cognome potrebbero rivelarsi poco utili a fronte dell'assenza di altri riferimenti in grado di fornire ulteriori informazioni. In ogni caso, se è vero che un collegamento tra gli identificatori diretti e gli pseudonimi deve sempre essere mantenuto per consentire una re-identificazione; al fine di poter considerare la pseudonimizzazione una scelta utile a garantire un alto livello di sicurezza dei dati, l'associazione tra identificatore e pseudonimo non deve essere tanto palese da consentire a chiunque abbia accesso ai soli dati de-identificati di risalire al soggetto.

Seppur vero che la pseudonimizzazione, come definita dal GDPR[33], può fornire il giusto supporto alla tutela dei dati personali, è d'altronde necessario tenere in considerazione che non tutte le tecniche utilizzabili sono ugualmente efficaci e valide, potendo alcune comportare un rischio perfino maggiore, in virtù della falsa sensazione di sicurezza che si verrebbe a generare negli individui.

In molti casi lo pseudonimo è generato da un terzo fidato spesso autorizzato a re-identificare lo pseudonimo per ricollegarlo al soggetto originario[34]. Per queste ragioni l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) ha contribuito a definire degli obiettivi generali di progettazione che ogni titolare del trattamento farebbe meglio a tenere in considerazione nella valutazione delle migliori tecniche di pseudonimizzazione[35]. Il primo consiste nel far sì che gli pseudonimi non consentano una facile re-identificazione da parte di terzi in uno specifico contesto di trattamento. Una volta sinceratosi di ciò, il titolare deve evitare di rendere troppo semplice per un terzo la riproduzione degli stessi pseudonimi[36].

Il WP29 ha individuato due categorie di risultati che possono derivare dalla pseudonimizzazione: gli pseudonimi che possono essere derivati dai valori originali di un attributo o di una serie di attributi[37] e quelli indipendenti dal valore iniziale, come un numero generato casualmente o un identificativo scelto dall'interessato. Più nello specifico ENISA ha poi contribuito a circoscrivere le 5 tecniche attualmente più utilizzate per pseudonimizzare un singolo identificatore[38].

Nella tecnica del *Counter* l'identificatore viene sostituito con dei numeri individuati da un contatore monotono. Il problema di questo metodo è però rappresentato dalle difficoltà nell'implementazione e nella scalabilità laddove applicato a dataset avanzati e di grandi dimensioni. Allo stesso modo la tecnica del *Random Number Generator* (RNG) e quella della *Cryptographic Hash Function* hanno un'utilità limitata dalle circostanze in cui vengono adottate. Nel primo, infatti, sono frequenti i casi in cui si verificano delle *collisioni*, ossia situazioni in cui ad un unico pseudonimo vengono associati due identificatori. Nel caso della funzione di hash invece, nonostante questa sia in grado di assicurare un alto livello di integrità dei dati, allo stesso tempo è spesso soggetta ad attacchi di forza bruta quali la *dictionary search* che possono metterne in mostra le vulnerabilità. La quarta categoria è rappresentata dalla tecnica del *Message Authentication Code* (MAC), che utilizza sempre una funzione hash, ma che differisce da quella precedentemente vista per l'impiego di una chiave segreta nella generazione dello pseudonimo, senza la quale non è possibile mappare gli identificativi e gli pseudonimi. Il MAC è tuttora considerato una valida

tecnica di pseudonimizzazione nel settore della tutela dei dati personali e presenta diverse varianti che possono essere adottate in base ai requisiti di scalabilità e funzionalità richiesti. Ultima delle cinque è infine la crittografia che può essere utilizzata come tecnica di pseudonimizzazione[39] e si distingue in simmetrica e asimmetrica. Un esempio di cifratura simmetrica applicata nel settore della genetica è quello che prevede l'uso dell'algoritmo di cifratura a blocchi, *TwoFish*[40]. per convertire il numero di previdenza sociale (SSN) in un'"alphabet-derived string". La cifratura asimmetrica è stata spesso impiegata per processi di pseudonimizzazione, soprattutto nel settore della salute. In un caso ad esempio, partendo da un'analisi di «previously published privacy concepts regarding a streamlined de-pseudonymization process and a patient-based pseudonym as applicable to research with genomic data [...] approaches»[41], si è riusciti a ricostruire una tecnica di pseudonimizzazione apposita per progetti di ricerca transnazionali, in grado di generare pseudonimi univoci, così da evitare collisioni, e facendo in modo che l'addetto alla de-pseudonimizzazione non corrispondesse al soggetto incaricato della pseudonimizzazione[42]. In un altro contesto invece, la crittografia asimmetrica è stata applicata per sviluppare un nuovo approccio per la gestione dei dati particolari, denominato *Polymorphic Encryption and Pseudonymisation*. Pensato appositamente per risolvere problematiche recenti che sorgono dal sempre più diffuso utilizzo dei big data tramite una struttura di pseudonimizzazione polimorfica, garantisce che ogni individuo abbia in automatico «different pseudonyms at different parties»[43] e che questi possano essere de-pseudonimizzati solo da partecipanti, che conoscono l'identità originale.

La scelta rispetto a quale tecnica di pseudonimizzazione utilizzare dipende in ogni caso da diversi parametri, tra cui ovviamente il livello di protezione desiderato e il vantaggio che si vuole ottenere dal dataset. Per di più, come visto nel caso delle tecniche di anonimizzazione applicate ai dati genetici e come anche affermato dall'ENISA, è bene tener presente che ci sarà sempre il rischio di una re-identificazione degli individui[44]. Può infatti darsi che un individuo, inizialmente non identificabile, lo divenga successivamente per via dell'aggiunta di ulteriori informazioni, collegate allo pseudonimo. Proprio per questa ragione il titolare deve avere ben chiaro lo scopo della pseudonimizzazione e deve selezionare la tecnica appropriata ad esso, in quanto un livello di protezione non adeguato sarà certamente in contrasto con i requisiti *ex* articolo 5 del GDPR.

Lo status dei dati pseudonimizzati resta una delle incertezze che più impattano sull'uso dei dati genetici[45] e, se la pseudonimizzazione può rappresentare una misura utile a garantire il rispetto del principio di minimizzazione, bisogna però tener presente che i vantaggi che possono derivare dal suo impiego sono legati al singolo contesto e che dunque potrebbero esserci soluzioni più adeguate.

Nel GDPR la pseudonimizzazione viene menzionata oltre che nell'articolo 89, anche negli articoli 25 e 32. In entrambi viene inclusa all'interno di quel macro insieme di misure tecniche e organizzative che, a seconda della situazione, possono rivelarsi più o meno adatte a «soddisfare i requisiti del [...] regolamento e a tutelare i diritti degli interessati»[46] in generale, e nello specifico a garantire «un livello di sicurezza adeguato al rischio»[47]. La loro utilità è quindi legata al contesto, e per questo è sempre bene tener presente il quadro generale dei requisiti imposti dal GDPR piuttosto che concentrarsi su una sola delle possibili misure.

3.2. La protezione dei dati *by design* e *by default*

L'inserimento della protezione dei dati *by design* e *by default* tra le misure tecniche e organizzative del GDPR ha rappresentato un passo enorme che per poter esser compreso richiede innanzitutto di prendere le mosse dai tre paragrafi dell'articolo 25 in materia di protezione dei dati *by design* e *by default*. Quest'ultimo, infatti, parte dal presupposto per cui le tecnologie digitali e i sistemi possono essere progettati in maniera tale da garantire la privacy e la protezione dei dati degli individui. Con un incipit che ricalca in buona parte quello dell'articolo 24 sul principio di accountability, il primo paragrafo individua i parametri che il titolare del trattamento deve tenere in considerazione nel valutare l'adeguatezza delle misure da mettere in atto per «attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione» e di «integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del [...] Regolamento e tutelare i diritti degli interessati»[48]. L'elenco dei parametri non è da considerarsi esaustivo, ma consente comunque di condurre un'analisi di sostenibilità, utile ad orientare il titolare verso scelte adeguate, per assicurare la conformità del trattamento alla legge[49] e non solo ai principi di minimizzazione dei dati o di sicurezza[50].

In virtù del principio di *data protection by design*, la valutazione sull'adeguatezza delle misure tecniche e organizzative deve avvenire già in fase di progettazione ovvero «sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso»[51], in maniera dinamica e costante nel tempo. Il titolare del trattamento deve quindi rimanere

aggiornato sui più recenti sviluppi tecnologici e su come questi possano comportare dei rischi per la protezione dei dati nelle operazioni di trattamento. Il tutto deve essere tenuto in considerazione sin dalle fasi di organizzazione del trattamento, pianificando e spendendo sulla base dei costi necessari a far fronte ai rischi per i diritti e le libertà degli interessati, implementando ogni principio del Regolamento nel trattamento.

Il secondo paragrafo dell'articolo 25 è dedicato al principio della protezione dei dati *by default*. Se nel caso della tutela dei dati *by design* le misure tecniche e organizzative adottate devono essere volte all'implementazione di tutti i principi *ex* articolo 5 del Regolamento, nel caso della protezione *by default* il legislatore si è concentrato nello specifico su quei principi maggiormente correlati al concetto di necessità, ovvero la minimizzazione, la limitazione delle finalità e della conservazione, con l'intento di limitare il trattamento solo a ciò che è strettamente necessario.

Con una formulazione che riprende il testo dell'articolo 5(1)(c), il principio in questione persegue l'obiettivo di tutelare gli interessati proteggendo direttamente i loro dati e il modo in cui questi vengono trattati[52]. Per questa ragione in capo al titolare del trattamento spetta quindi l'obbligo di mettere «in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento»[53].

Se è vero che la struttura dei principi di protezione dei dati *by design* e *by default* potrebbe sembrare all'apparenza identica, in realtà così non è. Mentre il primo principio è più orientato ai processi, il secondo è invece più incentrato sui risultati[54]. L'obbligo sancito al secondo paragrafo dell'articolo 25 è formulato in termini assoluti: il trattamento deve avere ad oggetto, per impostazione predefinita, solo quei dati necessari alla specifica finalità perseguita. Per questo, in tutti i casi in cui venga fatto uso di impostazioni di default, queste devono rispettare i requisiti di necessità correlati allo scopo prefissato.

Nel caso della protezione dei dati *by design* invece, l'imperatività dell'obbligo sancito dal legislatore è affievolita dall'insieme dei fattori che il titolare deve tenere in considerazione e bilanciare durante il processo decisionale relativo alle misure tecniche e organizzative da adottare[55]. Il tono adottato in questo caso dal legislatore sembrerebbe conferire all'obbligo normativo un carattere meno assoluto rispetto a quello visto sopra. In effetti la maggiore attenzione generalmente dedicata nel GDPR al principio di accountability e alla gestione del rischio[56] trova qui un contemperamento nello stato dell'arte e nei costi di implementazione, da valutare nella scelta delle misure adeguate con cui attuare in modo efficace i principi di protezione dei dati e integrare le garanzie necessarie per la tutela degli interessati e il rispetto del Regolamento.

Un approccio simile lo si ritrova poi nell'articolo 32 del GDPR, specificamente dedicato alla sicurezza del trattamento. Nonostante la formulazione, più congrua con il principio della protezione dei dati *by design*, è però bene precisare fin da ora che la norma in questione è collegata tanto alla protezione dei dati *by design* quanto a quella *by default*[57].

3.3. Le misure di sicurezza e la valutazione del rischio

Sulla base dell'articolo 32 del GDPR, il titolare del trattamento è oggi tenuto a mettere in atto «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio»[58] tenendo in considerazione lo stato dell'arte, i costi di attuazione e tutti i restanti fattori poc'anzi analizzati in merito alla protezione dei dati *by design*. L'adeguatezza del livello di sicurezza è rapportata ai potenziali rischi del trattamento e detti rischi sono stati suddivisi in tre diverse categorie, potendo essi comportare: la violazione della disponibilità, dell'integrità o della riservatezza dei dati[59].

Con riferimento alle modalità di valutazione del rischio[60] il Regolamento ha preferito affidarsi ad un disegno basato su tre moduli scalari piuttosto che su un unico procedimento valutativo di carattere generale. Il primo è rappresentato dalla generica analisi, svolta dal titolare o dai suoi responsabili sull'entità e la probabilità del rischio. Laddove questa non dovesse rivelarsi sufficiente, considerato l'elevato grado di rischio potenziale per i diritti e le libertà dell'interessato, l'articolo 35 prevede che il titolare debba portare a termine una valutazione d'impatto sulla protezione dei dati (DPIA). In ultima istanza, l'articolo 36 prevede l'obbligo di consultazione preventiva dell'autorità di controllo qualora dalla DPIA condotta dal titolare risulti un grado di rischio elevato in assenza di misure adottate per attenuarlo. Più alto è il rischio per il diritto dell'interessato, più rigorose devono essere le misure adottate dal titolare o dal responsabile del trattamento.

Anche l'articolo 32 distingue le misure di sicurezza adeguate al rischio tra tecniche e organizzative. Le prime consistono in quelle soluzioni demandate al lavoro di una macchina, un elaboratore, mentre le seconde sono affidate alle persone, che devono adottare comportamenti conformi a standard operativi. È poi lo stesso articolo a fornire un elenco esemplificativo

delle altre possibili misure di sicurezza da adottare[61]. Detta elencazione necessita però di essere sdoppiata per ciascun punto in: una regola tecnica e una regola organizzativa[62]. Quindi, nel caso della pseudonimizzazione o della cifratura, la loro implementazione dovrà avvenire sia con tecniche apposite, sia tramite «policies che impongono a funzioni aziendali di ricorrere a tali strumenti e di monitorare il ricorso a tali strumenti»[63]. Proprio per questa ragione, al fine di mettere in atto un sistema di sicurezza adeguato, è sempre essenziale procedere preventivamente a formare gli addetti al trattamento dei dati.

Ad oggi sono molte le autorità nazionali intente a fornire il proprio contributo nel tracciare una serie di linee guida generali per consentire alle organizzazioni e alle aziende di individuare il mezzo più adatto al proprio contesto, opponendosi all'illusione di una soluzione *one size fits all*.

Nel campo della ricerca genetica, ad esempio, è innanzitutto essenziale limitare l'accesso ai dati alle sole persone autorizzate, fino a quando questo si riveli necessario ai fini della ricerca stessa. È quindi essenziale prevedere dapprima una procedura di autorizzazione all'uso dei dati, definendo i differenti profili di autorizzazione ai sistemi e separandoli sulla base delle attività e delle responsabilità. Scaduto il contratto o conclusosi il periodo prestabilito, l'autorizzazione dovrà essere prontamente rimossa, così da garantire la riservatezza in maniera continuativa. Per questa ragione è bene effettuare una revisione annuale delle autorizzazioni, riallineando i diritti dell'utente alle sue funzioni. Una garanzia ulteriore sarebbe inoltre offerta, secondo il CNIL, da una politica di controllo degli accessi che sia specifica per i trattamenti messi in atto dall'organizzazione. Registrando parte delle azioni avvenute sui sistemi informatici si potrebbero infatti gestire gli incidenti o gli abusi, verificando l'origine degli accessi illeciti con *file* di registro o *log*, tramite il tracciamento.

Considerati i rischi di uso improprio dei dati è poi necessario integrare le normali misure per la deidentificazione e per l'acquisizione del consenso con ulteriori misure per una governance efficace, che solitamente si concretizzano in sistemi di controllo ulteriori per limitare l'accesso ai dati ai soli utenti autorizzati[64] e che coinvolgono tanto gli aspetti tecnici, quanto quelli manageriali, o organizzativi. Proprio in virtù di ciò, oggi per buona parte dei repository di dati genetici è previsto uno step preliminare, in base al quale un comitato apposito può acconsentire o meno a fornire l'accesso ai dati, ma solo dopo aver determinato se il progetto di ricerca presentato dal ricercatore rientri nell'ambito del consenso informato fornito dagli interessati. Purtroppo, un simile processo richiede spesso molti mesi per essere portato a termine e, pur garantendo agli interessati e alle biobanche di esercitare un controllo più preciso sui dati, ne limita la condivisione, non contribuendo a risolvere le preoccupazioni legate ad eventuali violazioni da parte dei ricercatori stessi[65].

Per far fronte a simili problematiche un insieme di nuove tecnologie tra cui la *blockchain*, dette *Distributed Ledger Technologies* (DLT), ha recentemente raccolto l'interesse di parte della comunità scientifica. Se infatti i metodi finora utilizzati sono stati contraddistinti da una particolare lentezza e in certi casi da uno scarso controllo effettivo sui dati stessi, la tecnologia sviluppata nel 2008 dal soggetto conosciuto con lo pseudonimo di Satoshi Nakamoto presenta delle caratteristiche che, nonostante i limiti ancora irrisolti, la rendono una valida soluzione per contribuire al progresso scientifico.

Le evidenti potenzialità alla base della *blockchain*, tra cui la decentralizzazione ed il controllo degli utenti sui propri dati[66], vanno però ponderate con alcune problematiche. Innanzitutto, il relativo panorama normativo è contrassegnato da una forte incertezza e frammentazione e mettere dei dati su una *blockchain* sarebbe una decisione difficile da revocare, che potrebbe richiedere sforzi particolarmente intensi, andando quindi in contrasto con il diritto all'oblio[67]. Per di più le DLT non sono state progettate per avere a che fare con «omics-sized data sets»[68] o con i dati derivanti dal sequenziamento di un intero genoma che possono arrivare ad occupare 0,5 terabyte per genoma, escludendo le immagini. Non per ultimo, nonostante aziende tra cui *Nebula Genomics* e *Encrypgen* facciano già uso della *blockchain* per acquisire e trasferire dati genetici, le strategie di monetizzazione alla base di simili modelli di business fanno sorgere nuove questioni etiche tuttora inesplorate.

Date le attuali incognite una certa cautela è quindi d'obbligo, senza però dimenticare che l'obiettivo da perseguire nel contesto europeo dovrebbe risiedere non nella creazione dell'ennesimo mercato europeo di test diretti al consumatore, ma piuttosto nell'applicazione delle DLT come uno strumento per i ricercatori che permetta agli individui di contribuire alla ricerca genomica[69], tenendo presente che i ricercatori europei si distinguono da sempre per gli sforzi compiuti nella sensibilizzazione rispetto ai pericoli e alle implicazioni etiche dell'uso dei dati genetici e del loro accesso su larga scala[70].

In conclusione, è poi da tenere a mente che sia l'articolo 32 che l'articolo 24, in tema di responsabilità del titolare del trattamento, affermano che, per dimostrare il rispetto degli obblighi sanciti in capo al titolare e la conformità ai requisiti *ex* articolo

32(1) poc'anzi analizzati, è possibile fare affidamento all'«adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42».

3.4. La co-regolamentazione, tra codici di condotta e certificazioni

I codici di condotta nel settore della tutela dei dati personali non rappresentano una novità. Ancor prima del GDPR, la Direttiva 95/46/CE, all'articolo 27, prevedeva una formulazione secondo cui era compito degli Stati membri e della Commissione incoraggiare «l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della presente direttiva, adottate dagli Stati membri»[71].

Se nel caso della Direttiva i codici avevano una funzione limitata, dovendo semplicemente facilitare l'applicazione della normativa e non integrarla o sostituirla, nel GDPR si assiste ad un importante cambio di direzione, proprio in virtù del fatto che tali codici sono oggi considerati degli strumenti di co-regolazione[72]. Stando alla definizione offerta dal Comitato europeo per la protezione dei dati personali (EDPB), i codici di condotta servono a dimostrare il rispetto del principio di accountability da parte di alcune categorie di titolari e di responsabili del trattamento, tramite la messa in pratica delle regole qui previste per la tutela dei dati personali[73]. Il contenuto è quindi costituito da norme che descrivono in maniera dettagliata i comportamenti più appropriati ed etici in un determinato settore[74].

Ormai da tempo si è avuto modo di evidenziare come la legislazione nazionale si sia rivelata inidonea a fronteggiare le sfide poste dal progresso tecnologico e dalla tutela dei dati personali[75]. Per queste ragioni è stata da più parti avanzata la possibilità di adottare dei codici di condotta settoriali approvati anche a livello internazionale. Una simile opportunità avrebbe il potenziale vantaggio di ridurre non solo l'incertezza legislativa ma anche i problemi connessi allo scambio di dati tra Stati, con particolare riguardo a temi quali il consenso informato, la giustificazione del trattamento dei dati senza il consenso dell'interessato o del trattamento di informazioni genetiche[76]. Ad oggi però i tentativi messi in atto per adottare un codice di condotta internazionale si sono rivelati inconcludenti, essendo stati tutt'al più pubblicati sotto forma di dichiarazioni non vincolanti[77]. Ciononostante, soprattutto in ambito genetico, questi sono visti come lo strumento in grado di apportare benefici concreti tanto nell'immediato quanto nel lungo periodo, potendo essere utilizzati per promuovere un vero ecosistema europeo per la ricerca biomedica congiunta e una più facile condivisione dei dati a livello internazionale[78].

Gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati personali (EDPB) e la Commissione sono oggi esortate a incoraggiare le associazioni e gli altri organismi rappresentanti determinate categorie di titolari del trattamento o di responsabili, a elaborare codici di condotta, modificandoli e, nel caso, prorogandoli, per precisare l'applicazione del GDPR in funzione delle specificità del settore. Questo è il caso del Codice di condotta polacco approvato recentemente dalla *General Assembly of Biobanking and BioMolecular Resources Research Infrastructure* in Polonia[79].

Tra gli elementi che il Regolamento enumera a titolo esemplificativo come meritevoli di una particolare disciplina all'interno dei codici di condotta, meritano particolare attenzione «d) la pseudonimizzazione dei dati personali; e) l'informazione fornita al pubblico e agli interessati; f) l'esercizio dei diritti degli interessati» nonché «h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32»[80]. Una disciplina apposita per ognuno di questi elementi all'interno di un codice di condotta adottato su larga scala, pur non costituendo una panacea di fronte ad eventuali conflitti tra normative nazionali, sarebbe comunque in grado di contribuire a tracciare delle valide linee guida vincolanti per l'armonizzazione della disciplina del trattamento dei dati genetici per finalità di ricerca scientifica. L'adozione di ulteriori codici deontologici promossi dalle autorità di controllo sarebbe inoltre un'alternativa valida tanto nelle circostanze «in cui il GDPR riserva agli Stati membri la libertà di mantenere o introdurre disposizioni più specifiche»[81], quanto nel caso dell'articolo 9, dove il testo del Regolamento rinvia «ai legislatori nazionali l'individuazione di garanzie apposite»[82].

Le disposizioni relative ai codici di condotta «si correlano a quelle sulla certificazione e sugli organismi privati a ciò abilitati»[83]. Anche le certificazioni, infatti, servono a dimostrare l'ottemperanza volontaria da parte del titolare e del responsabile alle norme e ai principi del regolamento. Il GDPR prevede che gli Stati membri, le autorità di controllo, il comitato e la Commissione sono tenuti a incoraggiare l'istituzione di simili meccanismi, oltre che di sigilli e marchi, relativamente alla protezione dei dati personali per dimostrare la conformità al Regolamento[84]. In questo caso il focus normativo è incentrato sulla dimostrazione della conformità piuttosto che sulla conformità in sé[85], ragion per cui l'articolo 42 e le

certificazioni sono da ritenersi una diretta conseguenza del principio di accountability[86], servendo a «dimostrare che un titolare del trattamento ha rispettato la disposizione e che quindi ha definito e attuato misure appropriate che sono state periodicamente sottoposte a revisione»[87].

Entrambe le normative, sia quella sui codici di condotta, sia quella relativa alle certificazioni, sono da ritenersi di estrema importanza soprattutto a fronte delle affermazioni della *Global Alliance for Genomics and Health* (*GA4GH*), secondo cui, già nel 2017, si riteneva plausibile che entro il 2025 sarebbe stato sequenziato il genoma di almeno 60 milioni di persone[88]. Recenti stime affermano infatti che ad oggi esistono 800 terabyte di dati genomici nel mondo[89]. Con l'obiettivo di massimizzarne l'utilità le istituzioni hanno però il bisogno di scambiare i propri dati al di fuori dei confini nazionali, una prassi rivelatasi evolutiva tanto per la ricerca contro le malattie rare quanto contro il cancro[90]. Lo scopo ultimo dei codici di condotta è di rispondere a delle problematiche in maniera accettabile e comprensibile tanto per il ricercatore quanto per il soggetto interessato dal trattamento. Benché la BBMRI-ERIC (Infrastruttura di Ricerca Europea delle Biobanche e delle Risorse BioMolecolari), ad esempio, nel 2017 abbia annunciato che avrebbe sviluppato un codice di condotta per l'intera Unione europea al fine di facilitare le dinamiche per il trattamento di dati legati alla salute[91] ad oggi questo non è ancora stato pubblicato.

Una circostanza in cui l'adozione di un codice di condotta o una certificazione possono rivelarsi utili è data dal caso in cui a un'istituzione che aggreghi i dati personali ricevuti da altre istituzioni venga richiesto di dimostrare l'esistenza e la validità del consenso al trattamento raccolto da un'altra istituzione. In questo caso appunto l'adozione di un codice di condotta sarebbe sufficiente a dimostrare che «the providing data controller follows the approved code of conduct and is certified under Article 42 of the GDPR»[92]. La mancanza di un organismo o di un'associazione che rappresenti davvero tutte le istituzioni di ricerca, la frammentazione e il contrasto tra gli interessi delle singole branche scientifiche e, infine, la sovrapposizione tra la ricerca scientifica e altri settori che possono richiedere il loro codice di condotta personale rappresentano però ad oggi un grosso freno all'adozione di un codice di condotta condiviso[93].

Alla luce di simili difficoltà, è quindi legittimo domandarsi se anche ora, nonostante i recenti traguardi conseguiti grazie al GDPR, la richiesta dei ricercatori di adottare delle linee guida uniformi per il trattamento di dati genetici continuerà a rimanere una questione irrisolta.

4. Conclusione

Per la prosecuzione e lo sviluppo della ricerca scientifica risulta oggi sempre più essenziale l'implementazione da parte dei titolari del trattamento delle misure tecniche e organizzative necessarie per attuare i principi di protezione dei dati e garantire il rispetto dei diritti e delle libertà degli individui. Questo risulta ancor più rilevante laddove si consideri che, a fronte dell'attuale e futuro progresso tecnologico, l'anonimizzazione dei dati genetici, oltre a rivelarsi poco utile per i ricercatori, sarà a dir poco irraggiungibile.

In attesa dell'adozione di strumenti di *soft law* flessibili e specifici per il settore della ricerca scientifica in grado di integrare le norme europee e nazionali, i titolari dovranno dunque tenere a mente che le tecniche efficaci oggi, un domani potrebbero non esserlo più, richiedendo ad essi un'opera di costante aggiornamento e un dispiegamento di forze non indifferente nel nome della privacy e della sicurezza.

Note

[1] C. Ziegenhain, R. Sandberg, *BAMboozle removes genetic variation from human sequence data for open data sharing*, in "Nature Communications", 2021, n. 12.

[2] J. Scheibner, J.L. Raisaro, J.R. Troncoso-Pastoriza et al., *Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis*, in "Journal of Medical Internet Research", vol. 23, 2021, n. 2.

[3] Art. 9, co. 2, lett. j), Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[4] *Ivi*, art. 89, co. 1.

[5] C. Staunton, S. Slokenberga, D. Mascalzoni, *The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks*, in "European Journal of Human Genetics", vol. 27, 2019, p. 1159-1167.

[6] Art. 89, co. 1, Regolamento (UE) 2016/679.

[7] *Ibidem*.

[8] T. Finnegan, A. Hall, *Identification and genomic data*, 2017, p. 20.

[9] Considerando 26, co. 1, Regolamento (UE) 2016/679.

[10] K. El Emam, C. Álvarez, *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, in "International Data Privacy Law", vol. 5, 2015, n. 1, p. 79.

[11] G. D'Acquisto, M. Naldi, *Big Data e Privacy by Design: Anonimizzazione Pseudonimizzazione Sicurezza*, Giappichelli, 2017, p. 67.

[12] *Ivi*, p. 81.

[13] S.S. Samani, *Assessing Disclosure Risks with Genomic Data*, A thesis submitted to The University of Manchester for the degree of Doctor of Philosophy in the Faculty of Humanities, 2018, p. 53-54; per ulteriori studi: J. Scheibner, J.L. Raisaro, J.R. Troncoso-Pastoriza et al., *op. cit.*; D. Froelicher, J.R. Troncoso-Pastoriza, J.L. Raisaro

et al., *Truly privacy-preserving federated analytics for precision medicine with multiparty homomorphic encryption*, in "Nature Communications", 2021, n. 12.

[14] R. Cippitani, *Il trattamento di dati genetici a fini di ricerca scientifica*, in "Diritto e Processo", 2018, pp. 95-134, a p. 118.

[15] D. Hallinan, M. Friedewald, P. De Hert, *Genetic Data and the Data Protection Regulation: Anonymity, multiple subjects, sensitivity and a prohibitionary logic regarding genetic data?*, in "Computer Law & Security Review", vol. 29, 2013, n. 4, p. 317-329, a p. 322.

[16] M. Macilotti, U. Izzo, G. Pascuzzi, M. Barbareschi, *La disciplina giuridica delle biobanche*, in "Pathologica", 2008, n. 100, pp. 86-108, a p. 87.

[17] P. Quinn, L. Quinn, *Big genetic data and its big data protection challenges*, in "Computer Law & Security Review", vol. 34, 2018, n. 5, pp. 1000-1018, a p. 1003.

[18] E.C. Hayden, *The genome hacker*, in "Nature", vol. 497, 2013, p. 172-174.

[19] Y. Erlich, T. Shor, I. Pe'er, S. Carmi, *Identity inference of genomic data using long-range familial searches*, in "Science", vol. 362, 2018, n. 6415, pp. 690-694.

[20] M. Philips, *Can Genomic Data Be Anonymised?*, Global Alliance for Genomic Health, 10 October 2018.

[21] P. Quinn, L. Quinn, *op. cit.*, p. 1003.

[22] Considerando 26, Regolamento (UE) 2016/679.

[23] P. Quinn, L. Quinn, *op. cit.*, p. 1003.

[24] M. Phillips, B. Knoppers, *The discombobulation of de-identification*, in "Nature Biotechnology", vol. 34, 2016, n. 11, p. 1102-1103, a p. 1102

[25] Considerando 78, Regolamento (UE) 2016/679.

[26] *Ivi*, art. 25, co. 1.

[27] *Ivi*, considerando 78.

[28] *Ivi*, art. 5, co. 2 e art. 24.

[29] M. Siano, *Art. 24*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), "GDPR e Normativa Privacy Commentario", Wolters Kluwer, 2018, p. 237.

[30] *Ibidem*.

[31] V. artt. 25, 32 e 89 Regolamento (UE) 2016/679.

[32] M. Hintze, K. El Emam, *Comparing the Benefits of Pseudonymization and Anonymization Under the GDPR*, Privacy Analytics, 17 August 2017, p. 3.

[33] Art. 4, co. 1, n. 5, Regolamento (UE) 2016/679.

[34] A. Gabel, I. Schiering, *Privacy Patterns for Pseudonymity*, in E. Kosta, J. Pierson, D. Slamanig (eds.), "Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data", Springer, 2018, pp. 155-172, a p. 159.

[35] ENISA, *Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation*, November 2018.

[36] *Ivi*, p. 19.

[37] Article 29 Data Protection Working Party, *Opinion 5/2014 on Anonymisation Techniques*, 10 April 2014, p. 20.

[38] ENISA, *op. cit.*, p. 21-23.

[39] *Ibidem*.

[40] F.K. Dankar, A. Ptitsyn, S.K. Dankar, *The development of large-scale de-identified biomedical databases in the age of genomics – principles and challenges*, in "Human Genomics", 2018, n. 12, p. 16.

[41] H. Aamot, C.D. Kohl, D. Richter, P. Knaup-Gregori, *Pseudonymization of patient identifiers for translational research*, in "BMC Medical Informatics and Decision Making", vol. 13, 2013, n. 75, p. 1.

[42] *Ivi*, p. 10.

[43] E. Verheul, B. Jacobs, C. Meijer et al., *Polymorphic Encryption and Pseudonymisation for Personalised Healthcare. A Whitepaper*, Institute for Computing and Information Sciences Radboud University Nijmegen, 2016, p. 1.

[44] ENISA, *op. cit.*, p. 11.

[45] C. Mitchell, J. Ordish, E. Johnson et al., *The GDPR and Genomic Data. The impact of the GDPR and DPA 2018 on genomic healthcare and research*, PHG Foundation, 2020, p. 50.

[46] Art. 25, co. 1, Regolamento (UE) 2016/679.

[47] *Ivi*, art. 32, co. 1.

[48] *Ivi*, art. 25, co. 1.

[49] G. D'Acquisto, *Art. 25*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), "op. cit.", p. 247.

[50] A. Ciccia Messina, N. Bernardi, *Privacy e Regolamento Europeo*, 2017, Wolters Kluwer, p. 112.

[51] Art. 25, co. 1, Regolamento (UE) 2016/679.

[52] European Data Protection Supervisor (EDPS), *Opinion 5/2018. Preliminary Opinion on privacy by design*, 31 May 2018, p. 7.

[53] Art. 25, co. 2, Regolamento (UE) 2016/679.

[54] L.A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in "Oslo Law Review", vol. 4, 2017, n. 2, p. 105-120, a p. 116.

[55] Art. 25, co. 1, Regolamento (UE) 2016/679.

[56] A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017, p. 306.

[57] ENISA, *op. cit.*, p. 7.

[58] Art. 32, co. 1, Regolamento (UE) 2016/679.

[59] Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 3/2014 sulla notifica delle violazioni dei dati personali*, 25 marzo 2014, p. 5.

[60] A. Mantelero, *op. cit.*, p. 307.

[61] Art. 32, co. 1, Regolamento (UE) 2016/679.

[62] A. Ciccia Messina, N. Bernardi, *op. cit.*, p. 113.

[63] *Ibidem*.

[64] Nuffield Council on Bioethics, *The collection, linking and use of data in biological research and health care: ethical issues*, 2015, p. 78.

[65] B. Berger, H. Cho, *Emerging technologies towards enhancing privacy in genomic data sharing*, in "Genome Biology", vol. 20, 2019, n. 128.

[66] M. Alghazwi, F. Turkmen, K.J. van der Velde, D. Karastoyanova, *Blockchain for Genomics: A Systematic Literature Review*, arXiv, 2021.

[67] S. Thiebes, M. Schlesner, B. Brors, A. Sunyaev, *Distributed Ledger Technology in genomics: A call for Europe*, in "European Journal of Human Genetics", vol. 28, 2020, p. 139.

[68] *Ibidem*.

[69] *Ivi*, p. 140.

[70] European Society of Human Genetics, *Statement of the ESHG on direct-to-consumer genetic testing for health-related purposes*, in "European Journal of Human Genetics", vol. 18, 2010, p. 1271-1273.

[71] Art. 27, co. 1, Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[72] A.R. Popoli, *Codici di Condotta e Certificazioni*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017, cit., pp. 394-395

[73] European Data Protection Board (EDPB), *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, 12 February 2019, p. 6.

[74] Art. 40, co. 1, Regolamento (UE) 2016/679.

[75] D.D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, in "Ohio State Law Journal", vol. 74, 2013, n. 6, pp. 1030-1069.

[76] M. Koščík, M. Myška, *Data protection and codes of conduct in collaborative research*, in "International Review of Law, Computers & Technology", vol. 32, 2018, n. 1, p. 141-154, a p. 143.

[77] *Ibidem*.

[78] F. Molnár-Gábor, J.O. Korbel, *Genomic data sharing in Europe is stumbling. Could a code of conduct prevent its fall?*, in "EMBO Molecular Medicine", vol. 12, 2020, n. 3, p. 1-7, a p. 1.

[79] D. Krekora-Zając, B. Marciniak, J. Pawlikowski, *Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on the GDPR art. 40*, in "Frontiers in Genetics", vol. 12, 2021, n. 12, p. 2189.

[80] Art. 40, co. 2, Regolamento (UE) 2016/679.

[81] R. D'Orazio, *Art. 40*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), "op. cit.", pp. 357-358.

[82] *Ibidem*.

[83] *Ivi*, p. 359.

[84] Art. 42, co. 1, Regolamento (UE) 2016/679.

[85] I. Kamara, R. Leenes, E. Lachaud et al., *Study on Certification Mechanisms under Articles 42 and 43 of the General Data Protection Regulation (GDPR) (EU) 2016/679*, 2019, p. 19.

[86] Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 3/2010 sul principio di responsabilità*, 12 luglio 2010, p. 18.

[87] *Ibidem*.

[88] E. Birney, J. Vamathevan, P. Goodhand, *Genomics in healthcare: GA4GH looks to 2022*, in "bioRxiv", 2017, p. 1.

[89] M. Phillips, F. Molnár-Gábor, H.O. Korbel et al., *Genomics: data sharing needs an international code of conduct*, in "Nature", vol. 578, 2020, p. 31-33, a p. 31.

[90] F. Molnár-Gábor, J.O. Korbel, *op. cit.*, p. 1.

[91] BBMRI-ERIC, *Code of conduct for using personal data in health research*, 2017.

[92] M. Koščík, M. Myška, *op. cit.*, p. 149.

[93] *Ivi*, p. 151.

* * *

Genetic data governance for the development of the scientific research

Abstract: For the first time in the European regulatory landscape, the GDPR has introduced the concept of "genetic data". A concept that is especially relevant in the context of scientific research. With the aim of contributing to a broader debate on the subject, this article aims to address the legal framework for the processing of genetic data for scientific research purposes. In particular, the article aims to examine and deepen the set of technical and organisational measures identified by the European legislator to reconcile the respect for the fundamental rights and freedoms of individuals with the needs of the development of scientific research and therefore the possible derogations to individual rights. Starting from the discipline introduced by Article 89 of the Regulation, the anonymisation and pseudonymisation techniques for the processing of genetic data will be presented, as well as the possible application of distributed ledger technologies (DLT) and blockchain This will be accompanied by a presentation of the technical and organisational measures set out in the various guidelines of national data protection authorities, as well as the principles of privacy by design and by default. A final in-depth analysis will be devoted to certification and to the need for international use of sectoral codes of conduct to overcome the national barriers that currently hinder genetic research.

Keywords: GDPR – Data governance – Genetic data – Scientific research

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0068
Articolo sottoposto a peer review

Internet governance: una questione di digital trust

Igor Marcolongo • Lorenzo Piatti • Alessandra Bossi

Ci sono due pilastri fondamentali che oggi garantiscono una rete Internet forte basata su una governance affidabile e utilizzabile a livello globale: regolamentazione e identità digitale. L'evoluzione di Internet sarà descritta partendo da questi due strumenti abilitanti del trust digitale. Sotto il primo aspetto, inizialmente si analizzerà il significato e l'impatto che la Internet governance ha avuto a livello teorico-filosofico, investigando il rapporto tra legge e codice, e in seguito sarà esaminato in concreto ciò che è stato portato avanti dai legislatori italiano ed europeo, che hanno da tempo cercato la migliore formula normativa per garantire un ecosistema in grado di bilanciare gli interessi dei cittadini e del mercato. Il secondo aspetto della governance di un ecosistema complesso come Internet è l'identità degli utenti. Saranno ripercorsi i tentativi di approcciare il tema dell'identità online: iniziali soluzioni centralizzate hanno lasciato spazio a proposte federate e le tendenze di democratizzazione e digital sovereignty hanno successivamente permesso il fiorire di un nuovo approccio, quello della *Self Sovereign Identity*. Partendo da una disamina della normativa in vigore in Europa, con alcuni richiami agli interventi regolatori previsti a livello eurounionale, si cercherà di esporre quali strumenti – tecnici e organizzativi – sono più idonei per il raggiungimento di un mercato digitale sicuro e affidabile.

Digital trust – Digital identity – eIDAS

Sommario: *1. Il significato dell'Internet governance – 2. Il ruolo della regolamentazione – 3. Identità digitale e presenza degli utenti in rete – 4. Conclusioni*

To be, or not to be (a part of the networked society):
that is no longer a question but an issue we have to deal with.
C. Costa, R. Torres[1]

1. Il significato dell'Internet governance

L'interazione tra diritto e Internet[2] ha attraversato, sin dalla fine del secolo scorso, diverse fasi: l'oggetto tecnologico, per costituzione indipendente dalla normativa, ha acquisito con il passare del tempo un livello tale di compenetrazione, affidabilità ed essenzialità da chiedersi se una governance specifica non fosse possibile, o perfino necessaria e indispensabile.

In "A Declaration of the Independence of Cyberspace" (1996) John Perry Barlow illustra come il ciberspazio sia un'area senza sovranità, dove una governance non solo non sia auspicabile, ma nemmeno realizzabile. La partecipazione del legislatore nel ciberspazio non è prevista, specialmente in tematiche quali la libertà di espressione, né tantomeno viene riconosciuto il potere esecutivo dello Stato. Il concetto di identità è interpretato come distaccato dalla

I. Marcolongo Head of Business Solutions Compliance, InfoCert – Gruppo Tinexta; L. Piatti, Head of Trust Specialists, Business & Solutions Compliance, InfoCert – Gruppo Tinexta; A. Bossi, Analyst, Business & Solutions Compliance, InfoCert – Gruppo Tinexta

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

persona fisica, e inteso solo come entità generica che opera in rete.

La proprietà intellettuale, le implicazioni penalistiche e civilistiche delle azioni svolte online, tuttavia, non possono coesistere con l'ideologia di Barlow. I numerosi reati che possono essere commessi in rete, quali hacking, phishing, violazione di copyright, cyberbullismo, distribuzione di materiale pedopornografico, non lasciano dubbi sulla necessità di una regolamentazione *ad hoc*. Anche da un punto di vista civilistico l'ascesa degli e-commerce, la contrattazione telematica, l'erogazione di servizi da remoto e il ruolo dei service provider hanno reso necessario l'intervento del legislatore per garantire un'adozione estesa – e sicura – della nuova tecnologia.

Una visione dell'Internet governance differente rispetto a Barlow è presentata da Lawrence Lessig che con l'espressione "Code is Law" tratta dal libro *Code and Other Laws of Cyberspace* (1999), riprende il concetto di "Lex informatica" coniato da Joel Reidenberg ed esprime la progressiva affermazione del codice come *rule-maker*. Il codice stesso infatti assume un ruolo primario nel regolamentare le interazioni e il comportamento degli utenti di Internet, e della rete stessa[3]. Si assiste, riferendosi a un processo spontaneo e inevitabile che avviene nel ciberspazio, al confluire di un nuovo tassello nella gerarchia delle norme. Nello stesso lavoro, Lessig ammonisce che la libertà nel ciberspazio non sarà data dall'assenza dello Stato, ma da uno Stato che garantisca il controllo di un certo tipo, che favorisca un luogo dove la libertà possa fiorire: si passa dalla visione poetica di Barlow che rifiuta decisamente l'intervento del legislatore, ad una meno radicale in cui viene riconosciuto il ruolo del regolatore, pur mantenendo il codice come un punto di riferimento.

Manifesta attuazione di tale concetto è la nuova era sancita dalla tecnologia blockchain, un particolare tipo di *Decentralized Ledger Technology* ("DLT"), contraddistinto dalla presenza di un codice open-source neutrale, dalla decentralizzazione dell'autorità, dal consenso distribuito e dalla verificabilità delle transazioni che avvengono sul registro pubblico[4]. Tale tecnologia può essere adottata per innumerevoli scopi: oltre alle più conosciute finalità di diffusione di sistemi decentralizzati di pagamento, gestione di criptovalute e attuazione di *smart contracts*, non è da sottovalutare l'accesso a servizi governativi senza limiti territoriali.

La struttura intrinseca della blockchain elimina l'elemento di fiducia tradizionale tra le parti, necessario nelle tipiche e tradizionali interazioni nelle quali un'autorità terza garantisce non solo l'operato dei soggetti, ma la validità delle loro azioni e la sicurezza delle transazioni. La fiducia distribuita che risiede nei nodi si sostituisce alla fiducia derivata da un rapporto contrattuale, rendendo difficile l'individuazione di ruoli e responsabilità negli ecosistemi decentralizzati. A ben vedere, tuttavia, questa componente non è stata eliminata, ma ha permesso la nascita di nuovi intermediari: fornitori di "Blockchain as a service", consulenze su quale Blockchain sia meglio utilizzare, assicurazioni dedicate, etc. Per questo motivo i mercati maggiormente regolamentati stanno utilizzando soluzioni di DLT *permissioned*, in cui – cioè – i verificatori sono noti e l'informazione certificata.

Sebbene il codice sia legge nel ciberspazio, De Filippi e Hassan ci conducono al livello successivo nel quale il diritto si trasforma progressivamente in codice, ossia "Law is Code". L'incorporazione di regole, decisioni e prescrizioni nel codice, quali *smart contracts* o altre disposizioni contrattuali, conferiscono alla blockchain, per la sua natura decentralizzata, il potere di far osservare i vincoli registrati, anche in assenza di una norma legale a supporto. Questo concetto, seppur vero, deve tuttavia tenere in considerazione i limiti tra ciberspazio e mondo reale, nel quale la presenza di un intermediario di fiducia garantisce la possibilità e la funzione di convalidare all'esterno del codice una decisione e di garantirne l'attuazione. Non è inoltre da trascurare la componente interpretativa nell'applicazione di una norma giuridica, resa possibile da prescrizioni generiche che possono adattarsi ad una moltitudine di casi differenti; tale aspetto discorda con la necessità di un codice preciso, specifico, non ambiguo e di immediata attuazione[5].

In definitiva, l'approccio proposto da Lessig e abbracciato – consapevolmente o meno – dai legislatori di tutto il mondo è stato reso necessario per garantire una corretta adozione del Web e delle sue applicazioni: nel paragrafo successivo si cercherà di riportare brevemente gli interventi normativi più rilevanti tesi a proteggere gli utenti e garantire la fiducia nell'ecosistema di Internet. Senza una componente di trust, il mondo digitale sarebbe rimasto il ciberspazio di Barlow: affascinante ma privo delle tutele che oggi permettono ai cittadini di tutto il mondo di utilizzare piattaforme e altre forme di condivisione per scambiarsi valore.

2. Il ruolo della regolamentazione

La regolamentazione assume, nello scenario sopra descritto, un ruolo fondamentale nel delimitare quali siano – *de jure* – gli strumenti con cui il legislatore può garantire che il mercato digitale sia sicuro e, quindi, di facile adozione da parte di tutti i cittadini. Questo paragrafo vuole dare atto della complessa

rete di norme primarie che garantiscono un giusto – e delicato – equilibrio tra usabilità, sicurezza informatica e certezza giuridica.

Tralasciando gli aspetti normativi legati alla sicurezza informatica, e quindi quella branca regolamentare che viene ricondotta sotto la Direttiva NIS (Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione, NISUE 2016/1148)[6], sembra utile concentrarsi sulle Direttive e sui Regolamenti che, negli anni, hanno cercato di costruire fiducia nel mercato digitale. Questo percorso è iniziato nel 1999 con i primi progetti di regolamentazione delle firme elettroniche, e proseguito in modo più formale nel 2015 con il concetto di *Digital Single Market*: il tentativo di creare uno spazio digitale europeo all'interno del quale ciascun cittadino – o più in generale ciascun utente – potesse sfruttare, in un ecosistema tecnicamente sicuro e giuridicamente rilevante, le potenzialità del commercio elettronico. Questa espressione va qui intesa in senso lato: a partire dalle necessità prettamente commerciali di scambio di beni e servizi, a raggiera l'esigenza dell'utente si estende a tutti quegli aspetti della vita quotidiana che abilitano la presenza della singola persona online. Concetti fondamentali di questa "trasformazione digitale" sono l'identità digitale, i documenti e le firme elettroniche, gli strumenti di e-delivery sicuri e con un valore legale certo. L'approccio regolamentare ha tenuto conto non solo degli aspetti squisitamente normativi ma anche di quelli tecnici: tutti i provvedimenti di primo livello sono accompagnati da una normativa di secondo livello che determina un dettaglio tecnologico o – spesso – richiama standard internazionali, come quelli ETSI o ISO.

Già con la Direttiva 1999/93/CE[7], il legislatore europeo aveva fatto un timido tentativo di regolare le transazioni elettroniche e i servizi fiduciari: solo nel 2014, tuttavia, con il Regolamento UE n. 910/2014 (c.d. "eIDAS")[8] – proprio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno – si è venuta a creare una solida base giuridica che ha permesso lo sviluppo di un ecosistema digitale basato su concetti tradizionali di sicurezza e fiducia. In particolare, il Regolamento eIDAS, è diviso in due parti principali: la prima – artt. 6-12 – regola l'identità digitale, la seconda – artt. 13-46 – descrive il funzionamento dei servizi fiduciari. Per quanto riguarda l'identità (o anche "eID"), il legislatore europeo ha creato un ecosistema centralizzato in cui ciascuno Stato membro è tenuto a valutare e verificare la bontà del proprio strumento di identità digitale: attraverso una procedura di notifica ciascuno Stato è in grado di presentare la propria soluzione alla Commissione che – grazie ai propri organi di valutazione e ad un momento di peer-review – decide se lo strumento è sufficientemente sicuro per essere riconosciuto in tutti e 27 gli Stati membri. Questo aspetto è particolarmente importante: il completamento della notifica, infatti, rende lo strumento utilizzabile in ciascuno Stato membro, attraverso un sistema di nodi di intermediazione (proxy) che risolvono le criticità di interoperabilità tecnica. Un'accortezza interessante risiede nel fatto che il legislatore ha previsto tre diversi livelli di sicurezza – "fiducia" – per ciascuna eID: *basso*, *significativo* e *elevato*. Questo approccio, dettato dalle esigenze del mercato, permette di utilizzare una eID a seconda del caso d'uso: non tutti i casi d'uso hanno, infatti, bisogno degli stessi elevati livelli di sicurezza, che spesso hanno come contraltare il sacrificare l'usabilità lato utente. Si immagini, ad esempio, l'uso di una eID nel contesto bancario, dove gli standard di sicurezza sono sicuramente molto alti: sarà richiesto un livello *elevato* o per lo meno *significativo*. Al contrario, per l'accesso alla biblioteca di quartiere potrebbe essere sufficiente un livello *basso*, con una considerevole abbassamento dei costi e migliore utilizzabilità. Come descritto in premessa, esistono dettagli tecnici e funzionali sulle modalità con cui ciascun livello di fiducia può essere raggiunto: la Commissione – con l'Atto di implementazione n. 2015/1502[9] – ha definito tutti i parametri che il medesimo strumento deve rispettare per essere riconosciuto nel corretto *Level of Assurance* ("LoA").

La seconda parte del Regolamento è dedicata ai servizi fiduciari: questa descrive tutti quegli strumenti elettronici che permettono un corretto scambio di informazioni e valore online. Il legislatore si è concentrato sulle firme elettroniche, i sigilli elettronici, la conservazione dei certificati elettronici, le validazioni temporali e gli strumenti di recapito elettronici. Per ciascuna di queste categorie sono previsti due livelli di sicurezza: uno semplice e uno qualificato, fanno eccezione le firme e i sigilli, per cui è previsto un livello intermedio definito come "avanzato". Anche in questo caso, il legislatore ha previsto diversi livelli di "trust" per le singole soluzioni: sono definiti i requisiti dei servizi fiduciari *tout court* e quelli dei servizi fiduciari qualificati. In alcuni casi, come per la firma elettronica, viene anche prevista una classe residuale, o "semplice", che permette di dare consistenza al dettato dell'art. 25 co. 1, per cui «A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate».

Seppur sia rimesso a ciascuno Stato membro di individuare il valore giuridico e la forza probatoria di ciascuno strumento, l'art. 25 riconosce alla sola fir-

ma elettronica qualificata un valore equipollente alla firma autografa: questo permette di mantenere un altissimo grado di interoperabilità per questo strumento in ciascuno dei 27 Stati membri. Come per la notifica – e quindi il riconoscimento – dell'eID, anche per i servizi fiduciari esiste un complesso ecosistema di validazione: ciascuno Stato membro individua una autorità di vigilanza – in Italia AgID – che gestisce le *trust list*, un elenco di soggetti abilitati all'erogazione dei servizi fiduciari. Il livello "qualificato" si raggiunge solo a seguito di un esito positivo di una procedura di valutazione di specifici soggetti, i *conformity assessment body*, che attraverso audit e verifiche accertano che il prestatore di servizi in questione abbia tutte le caratteristiche per erogare un servizio di livello "qualificato". Questo aspetto non è da sottovalutare: è esattamente grazie a questa rete di accreditamento e controllo che il legislatore è in grado di garantire un alto grado di governance nel framework digitale europeo.

Il Regolamento eIDAS è poi integrato in ciascuno Stato membro da normative di settore che normano tutti gli aspetti non direttamente trattati dalla legge europea: in Italia, questo ruolo è ricoperto dal Codice dell'amministrazione digitale (anche conosciuto come "CAD"[10]) e dalle regole tecniche (o linee guida) che lo completano. Nel nostro caso, vengono regolati sia aspetti che sfuggono al Regolamento europeo – come la PEC o la conservazione a norma – sia aspetti di dettaglio come appunto il valore giuridico e probatorio di ciascuno strumento. Questo aspetto tende a indebolire la portata di governance generale del Regolamento, ma è un approccio necessario per evitare che l'armonizzazione tecnologica europea porti eccessivo squilibrio negli ordinamenti di ciascuno Stato membro: il bilanciamento trovato dal legislatore ha permesso negli anni di aumentare la fiducia nei servizi digitali.

Il Regolamento eIDAS risale al 2014, è in corso un'operazione di aggiornamento che comprende non solo la rimodulazione di strumenti già presenti, ma anche l'inserimento di nuovi servizi fiduciari: seppur si tratti di una prima proposta, soggetta probabilmente a future modifiche, possono già essere individuati alcuni punti di interesse.

Tra questi emergono nuovi servizi fiduciari, quali servizi di conservazione elettronica qualificata, registri elettronici, l'*European digital identity wallet* e gli attestati di attributi elettronici. Questi ultimi due sono particolarmente rilevanti per il percorso che stiamo cercando di fare con il presente articolo: si tratta di strumenti tecnologici già utilizzati da diversi anni, ma privi di un vero e proprio trust framework. A questo si aggiungono i registri elettronici: la gestione di database o ledger è destinata a diventare un servizio fiduciario. La somma di tutte queste variabili è un chiaro segnale che il legislatore sta cercando di addentrarsi nel nuovo Internet, quello delle DLT cui si faceva riferimento poco sopra, caratterizzato dalla decentralizzazione e da nuovi protagonisti che non sempre sono facilmente individuabili.

Regolare gli strumenti utilizzati, tuttavia, non è attività sufficiente per garantire una governance solida e creare un ecosistema di fiducia tale da permettere l'adozione estesa delle nuove tecnologie: il legislatore, infatti, ha previsto un'articolata disciplina degli acquisti online, improntata per lo più alla protezione del consumatore. Nel 2000 con la Direttiva sul commercio elettronico (Direttiva 2000/31/CE)[11], insieme al suo recepimento in Italia con il D.lgs. 70/2003[12], vengono regolati tutti quegli aspetti che attengono ai "servizi della società dell'informazione". In particolare, vengono descritte le modalità di conclusione dei contratti online (o telematici), compreso il dettaglio delle clausole vessatorie, gli obblighi informativi verso gli utenti, nonché le sanzioni previste per i prestatori di servizi. Questo punto è particolarmente importante, perché riflette la serietà del legislatore nel creare una cornice chiara e sicura all'interno della quale gli utenti possano acquistare e scambiare valore. Il concetto di acquisto da remoto può sembrare scontato a 20 anni di distanza, ma in quella sede il legislatore ha dovuto bilanciare gli interessi imprenditoriali con i diritti di soggetti in qualche modo "fragili": l'asimmetria informativa è stata la ragione principale dell'incapacità dell'utente di muovere passi sicuri nella contrattazione telematica, che il regolatore ha cercato di compensare imponendo ai prestatori di servizi oneri informativi e sanzioni di diverso grado, nonché ampi diritti a favore dei consumatori (si pensi al recesso *ad nutum* entro i 14 giorni dall'acquisto).

Anche la regolamentazione del contesto finanziario ha fortemente contribuito alla governance della rete, diventando nel tempo uno standard *de facto* e un *driver* per l'evoluzione tecnologica: le varie Direttive *Anti Money Laundering* ("AML") – e i rispettivi provvedimenti di ricezione, che si trovano all'interno del d.lgs. n. 231/2007[13] – hanno permesso la nascita e lo sviluppo di piattaforme bancarie online. In particolare, gli articoli dedicati al riconoscimento della clientela da remoto, hanno abilitato processi di *onboarding* digitali, altrimenti non praticabili. Inoltre, la Direttiva (EU) 2015/2366 sui *payment services* ("PSD2")[14] ha rafforzato la fiducia nelle transazioni, imponendo l'utilizzo di strumenti di digital trust, quali l'autenticazione a due fattori e l'autenticazione sicura tra server (QWAC), oltre a importanti

aspetti legati all'open banking: questo ha indubbiamente portato gli utenti ad approcciare con più serenità processi remoti e innovativi, in un contesto così delicato come quello dei pagamenti elettronici.

Un importante strumento di interconnessione tra le numerose normative sopra citate è il Regolamento Generale sulla Protezione dei Dati Personali ("GDPR")[15]: con questo intervento, come noto, il legislatore europeo ha rafforzato la tutela dei dati personali, sostituendo la precedente Direttiva 95/46/CE. Questo strumento è stato previsto sia per tutelare i dati dei cittadini – e quindi degli utenti – sia per garantire ai prestatori di servizi e agli Stati sovrani uno strumento in grado di assicurare un trattamento legittimo dei dati. Questo è un aspetto assolutamente rilevante per la governance del Web: il regolatore non si è limitato a creare uno strumento protettivo per gli interessati, ma si è spinto sino a cercare forme per cui i dati potessero essere utilizzati da quei titolari che – per motivi di opportunità o business – ne traessero utilità per i diversi scopi di business. Al netto dei recenti tentativi – si veda ad esempio la Direttiva 770/2019[16], relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali – di monetizzazione dei dati, che non sempre incontrano il favore del Garante per la protezione dei dati personali, è prevista una complessa architettura di consensi ed eccezioni per permettere un uso trasparente e legittimo dei dati. Questo aspetto si inserisce in maniera trasversale rispetto a tutte le normative sopra citate, in quanto da una parte la protezione dei dati è sempre richiamata formalmente, dall'altra un corretto trattamento dei dati è essenziale proprio per poter offrire servizi digitali, che – fondamentalmente – vengono alimentati proprio dai dati personali.

A sottolineare l'importanza dei dati nell'epoca dell'informazione, c'è anche il Regolamento (UE) 2018/1807[17], in materia di protezione dei dati non personali: la cura anche di questi aspetti permette di garantire al mercato unico digitale un trasferimento, trattamento e scambio di dati sicuro, alimentando così la transizione digitale.

Il legislatore si sta impegnando, inoltre, ad aggiornare l'intero impianto normativo: con due importanti proposte, il *Digital Services Act*[18] e il *Digital Markets Act*[19], intende definire un quadro giuridico idoneo alle tecnologie moderne che garantisca la sicurezza degli utenti online, stabilendo una governance con la protezione dei diritti, mantenendo allo stesso tempo appetibile la "Platform economy" per tutti gli attori nazionali e internazionali.

3. Identità digitale e presenza degli utenti in rete

L'evoluzione di Internet, l'incremento degli strumenti che la rete mette a disposizione e lo sviluppo di innumerevoli applicazioni Web hanno inevitabilmente influito, e continuano a incidere, sulla presenza degli utenti in rete. In un primo momento si assiste alla creazione di pagine Web statiche rivolte ai consumatori come strumento di sola lettura, adatte per fornire informazioni e strumenti con un approccio *top-down*, in particolar modo a livello istituzionale e ad opera di fornitori di servizi. Si è in seguito verificato il passaggio a quello che viene definito "Web 2.0", con una partecipazione attiva degli utenti e con possibilità di accesso e creazione di contenuti. La scoperta dei molteplici livelli di Internet, e la conseguente presenza interattiva degli utenti online, hanno inoltre introdotto per molti web-users il cambiamento della condizione di anonimato in volontà di coltivare un'identità online. La corsa alla creazione di spazi personali sul Web, come blog o profili su diversi social network, la propensione a geolocalizzarsi rendendo noti i luoghi frequentati, la partecipazione a discussioni in rete e l'integrazione di profili professionali hanno assecondato lo spirito di condivisione di molti internauti. Con l'aumentare delle informazioni diffuse sul Web, tuttavia, è cresciuta anche la consapevolezza degli utenti rispetto a ciò che stavano condividendo, le azioni che stavano compiendo, la loro effettiva presenza in rete e le implicazioni che queste attività hanno nel mondo offline. Questa cognizione, unita alla crescente attenzione del legislatore a disciplinare la materia come illustrato nel precedente paragrafo, ha portato molti utenti a vagliare il proprio comportamento online. L'iniziale frenesia di condivisione ha lasciato il passo alla moderata valutazione e, per alcuni, anche alla ricerca dell'anonimato. Conservare o raggiungere questa condizione, tuttavia, non è un fine che tutti gli utilizzatori desiderano perseguire, soprattutto se all'utente stesso sono forniti gli strumenti previsti dalla normativa atti a tutelare e gestire l'identità digitale e i propri dati personali. Emerge quindi il vero obiettivo: esercitare un controllo progressivo sulla propria individualità e sulle informazioni condivise nel corso del tempo su Internet[20].

Le prime forme di riconoscimento degli utenti in rete sono state scandite dalla scelta di username, in seguito arricchito da una password, abitualmente collegate ad un indirizzo e-mail, atte a creare profili digitali che permettessero all'utente di interagire con il servizio o la pagina Web di riferimento. Il proliferare di molteplici utenze diverse ha permesso al modello così detto "federato" di farsi strada. In rela-

zione a questo modello, l'identità è gestita da un solo service provider che mette a disposizione dell'utente il sistema di autenticazione centralizzato, userID e password, il quale permette di autenticarsi presso fornitori ulteriori rispetto al provider che ha creato l'identità, secondo un framework di fiducia tra i provider (*federation*). L'utente pertanto non deve ottenere dati di autenticazione per ogni servizio o creare un account per ogni prestazione online, ma con una sola autenticazione può identificarsi e accedere a servizi di diversi fornitori. La *user experience* di questo modello è certamente molto positiva; tuttavia, alcune criticità rispetto alla delegazione dell'identificazione in capo ad un unico soggetto possono essere individuate. Ad esempio, la gestione delle informazioni condivise dall'utente nel tempo, l'esercizio dei diritti dell'interessato in un'ottica di protezione dei dati personali ed eventuali rischi di sicurezza delle informazioni.

L'incremento della partecipazione online, la digitalizzazione di numerosi servizi – essenziali e non – e le nuove opportunità nate dall'economia digitale, hanno portato alla necessità di identificare gli utenti in rete in modo univoco, e in molti casi, all'esigenza di associare l'identità digitale ad un'identità fisica offline. Per garantire non solo questo collegamento, ma anche la sicurezza informatica dei dati e delle informazioni trattate e per evitare il delinearsi di diverse soluzioni frammentate, si è prospettato un modello basato sul concetto di identità decentralizzata. Questo framework si serve della crittografia e di una struttura decentralizzata, quale quella abilitata dalle *Decentralized Ledger Technologies* (DLT), di cui la Blockchain fa parte, per consentire all'utente di creare identità digitali decentralizzate sicure, che rimangano sotto la sua amministrazione e il suo costante controllo. Soluzioni crittografiche fornite da prestatori di servizi fiduciari qualificati quali la firma elettronica qualificata per la persona fisica, e i sigilli elettronici per le persone giuridiche, possono permettere agli utenti di attuare il collegamento con la propria identità offline e di ottenere credenziali verificabili (*verifiable credentials* VCs) a supporto di tale connessione.

Un approccio all'identità digitale decentralizzata, noto come *Self-Sovereign Identity* (SSI), permette al titolare di gestire, oltre alla propria identità digitale, ulteriori dati ad essa collegati; l'utente può infatti selezionare in modo attivo, ogni volta che un'identificazione si renderà necessaria, quali dati nello specifico condividere con il destinatario e mantenere la sua regolare supervisione su di essi[21]. Tale metodo permette di gestire il consenso, o la revoca dello stesso ai fini di trattamenti di dati personali, di assicurare il rispetto dei principi di minimizzazione e trasparenza e di garantire l'esercizio dei diritti dell'interessato in termini di accesso e portabilità.

La mancanza di fiducia, spesso effettiva nel mondo digitale, dovuta alla presenza di connessioni e scambi con soggetti dei quali non si ha modo di conoscere la vera identità, alla necessità di dover rivelare senza controllo informazioni, nonché alla difficoltà di dimostrare la provenienza di dati ricevuti, ha portato alla creazione di un progetto noto come "Trust Over IP" (TOIP) che nel 2020 ha assunto lo status di fondazione[22]. L'obiettivo di quest'ultima è ripristinare l'elemento fiduciario colmando il "trust gap" tra i diversi attori online con i seguenti strumenti, e non solo: l'accertamento di identità e attributi verificati, l'uso di *wallet* digitali interoperabili e l'adozione di standard globali per connessioni private. Tali concetti sono da tempo sostenuti da Drummond Reed, co-fondatore di TOIP Foundation e grande teorico dei temi di identità distribuita. Egli infatti già nel 2017 aveva dichiarato che le SSI fossero «il culmine naturale dell'evoluzione dell'identità in Internet, allora consegnarla richiede fiducia diffusa, portabilità, sicurezza e nessun singolo punto di fallimento o controllo» e la DLT risulta l'unico meccanismo sicuro per raggiungere tale obiettivo[23].

Dal punto di vista della normativa, come già indicato, il Regolamento eIDAS prescrive il riconoscimento reciproco all'interno dell'Unione europea tra regimi di identificazione elettronica, sia per le persone fisiche che per le persone giuridiche, e detta le modalità di notifica dei regimi stessi. L'evoluzione con il testo proposto per eIDAS 2.0[24] è nella presentazione di una soluzione di identità digitale sicura e affidabile riconosciuta tra gli Stati membri che amplifichi le funzioni dei documenti nazionali elettronici e che conduca all'affermazione di un'identità nel pieno controllo del suo titolare[25].

Sicurezza delle persone, sicurezza dei dati, facilità d'uso, accessibilità a servizi pubblici e privati, affidabilità, inclusività e interoperabilità sono solo alcuni dei punti cardine alla base dell'introduzione dell'identità digitale europea. Ogni Stato membro dovrà dotarsi di infrastrutture per emettere Portafogli europei di identità digitale (*European digital identity wallets*, nel prosieguo "wallet") con conseguenti costi amministrativi e finanziari che saranno tuttavia ripagati dai benefici che un'armonizzazione giuridica porterà a tutti gli utenti. Ogni prestatore di servizi, pubblico e privato, per la cui prestazione è richiesta un'autenticazione forte potrà garantire l'accesso e l'identificazione tramite soluzioni che siano in grado di dialogare con lo standard su cui i *wallet* sono costruiti. In particolare, in un contesto rispettoso

del paradigma SSI, ciascun utente potrà spendere le proprie VC attraverso il *wallet* al fine di dimostrare la propria identità o un attributo relativo alla propria sfera personale. Interessante notare come le azioni di autenticazione e identificazione garantite da questi oggetti possano essere effettuate anche offline, per rispondere ad esigenze di alcuni settori basati principalmente sull'interazione fisica, quale il settore sanitario. Per ottenere questa interoperabilità è ancora una volta fondamentale l'intervento del legislatore: ci si aspetta che con eIDAS 2.0 – come sopra descritto – si possa ottenere una soluzione unica per tutta l'Europa.

Numerosi aspetti dell'approccio SSI saranno implementati nel *wallet*, in modo da garantire che il titolare dell'identità digitale abbia a disposizione gli strumenti adatti per selezionare quali informazioni, attributi, qualifiche o credenziali condividere digitalmente in sicurezza. Questo approccio permette di rispettare i principi sanciti dal GDPR, quali il controllo del dato e la minimizzazione del trattamento, e rende particolarmente fluidi processi di raccolta e spendita del consenso al trattamento.

Da una gestione totalmente centralizzata dell'identità, tipica del Web 2.0, si è quindi transitati verso modelli frammentati, creati dall'utente ma la cui gestione rimaneva strutturalmente associata al proprietario della piattaforma di riferimento, per arrivare, con il Web 3.0, a modelli di identità digitale decentralizzata. Grazie al paradigma SSI, tali modelli garantiscono non solo la lettura e la scrittura, ma permettono di esercitare concretamente il controllo della e sulla propria identità. Venendo meno la centralizzazione, tutte le informazioni sono in capo e a disposizione del titolare, il quale tramite un *wallet* installato sul proprio cellulare potrà anche gestire certificati di proprietà e oggetti digitali quali NFT[26]. L'identità dell'utente in rete si apre, si confronta con l'identità reale del soggetto e non ne è distinta.

Uno strumento strettamente collegato all'identità digitale è il domicilio digitale, previsto dall'art. 3-*bis* del CAD per ricevere comunicazioni elettroniche aventi valore legale. Per eleggere il domicilio digitale è necessario essere in possesso di un recapito elettronico certificato o certificato qualificato. Ad oggi in Italia la designazione è possibile tramite il servizio di posta elettronica certificata e un'apposita procedura formale di elezione, che tuttavia non garantisce di per sé l'identità certa del titolare della casella. Tramite la creazione e consultazione di elenchi di corrispondenza tra domicili digitali e imprese, professionisti e cittadini è possibile avere a disposizione l'indirizzo PEC fornito dall'impresa, professionista o cittadino corrispondente. Dal 2013 con l'istituzione da parte del Ministero dello Sviluppo Economico di INI-PEC si è reso obbligatorio per imprese e professionisti iscritti in albi o registri eleggere un domicilio digitale. Si tratta di un elenco regolarmente aggiornato e consultabile da parte di tutti gli utenti senza necessità di autenticazione. Con la Determinazione n. 529/2021 AGID ha inoltre dato l'avvio a INAD, l'Indice dei domicili digitali che raccoglierà i domicili digitali volontariamente eletti da parte di persone fisiche, professionisti e altri soggetti non sottoposti all'obbligo di cui sopra. Prima di eleggere il domicilio digitale sarà necessaria una fase di identificazione univoca, tramite SPID, CIE o CNS. I domicili digitali eletti dalle persone fisiche saranno inoltre trasmessi quotidianamente all'ANPR (Anagrafe Nazionale Popolazione Residente) che raccoglie i dati anagrafici dei cittadini in modo da assicurare la consistenza delle informazioni alla base dei procedimenti di tutti gli enti della pubblica amministrazione. Questo percorso è strategico per la digitalizzazione della PA tanto auspicata in questi anni, ma comporta una serie di criticità stante la varietà di situazioni da regolare. Ad esempio, il Garante per la protezione dei dati personali ha sottolineato alcune problematiche in merito alla possibilità di utilizzare gli indirizzi PEC presenti in INI-PEC per l'invio di comunicazioni aventi valore legale[27]. Accade, infatti, che numerosi indirizzi PEC professionali di ordini o collegi siano gestiti non soltanto dal diretto titolare, ma anche da parte di collaboratori e colleghi, venendo quindi a mancare la riservatezza delle comunicazioni stesse. Tale è il caso della ricezione di verbali di accertamento per infrazioni del codice della strada, tema sul quale il Garante ha recentemente ribadito la sua posizione[28] escludendo la possibilità di inviare questo tipo di comunicazioni al domicilio digitale professionale. Per ovviare al problema il professionista iscritto nell'INI-PEC potrà registrarsi all'INAD in qualità di persona fisica, in modo da poter separare le comunicazioni di competenza lavorativa da quelle appartenenti alla sfera privata. Allo stesso modo, per garantire la divisione di questi due ambiti, all'interno dell'INAD sarà prevista la possibilità per i professionisti non presenti in INI-PEC di eleggere un domicilio digitale professionale, e uno personale, entrambi riferiti al medesimo soggetto. Sia a livello nazionale[29], che europeo[30], l'obiettivo è implementare le piattaforme per proporre recapiti elettronici certificati qualificati, in modo da garantire *ex ante* l'identità certa del titolare del recapito elettronico, e dipanare ogni dubbio in merito al tema della gestione del conseguente domicilio digitale eletto.

Per l'utente della rete si evince quindi sempre più la necessità di disporre di strumenti adeguati atti

a garantire il controllo sulle proprie informazioni, a permettere la gestione efficiente delle comunicazioni digitali, e a consentire l'esercizio dei diritti previsti dalle normative vigenti. Tali strumenti devono poter tenere in considerazione la dinamicità e la complessità del contesto digitale in cui sono declinati, e allo stesso modo saper sfruttare le opportunità che il framework di riferimento offre. Questo concerne tutti i diritti che concorrono alla macrocategoria di "diritto alla privacy" che annovera al suo interno distinti diritti quali il diritto alla protezione dei dati personali, alla reputazione, all'auto-determinazione e, non da ultimo, all'identità[31].

Il diritto all'identità, e il diritto all'identità digitale, sono parti della sfera personale dell'individuo, concorrono alla sua autodeterminazione e alla sua autonomia verso un modello di cittadinanza digitale consapevole, responsabile e affidabile. Sullivan ritiene fondamentale il riconoscimento e la protezione del diritto all'identità digitale, tema che frequentemente, ed erroneamente, viene messo in secondo piano rispetto alla protezione dei dati personali. In egual modo infatti questi diritti, ognuno secondo le proprie peculiarità, contribuiscono all'affermazione dell'individuo e si differenziano nella relazione con l'interesse pubblico[32]. Come difatti confermato dal GDPR[33], l'interesse pubblico in molteplici contesti sovrasta il diritto alla protezione dei dati personali, al contrario rispetto al diritto all'identità che non è subordinato a, o condizionato da, motivi di interesse pubblico.

Tale concetto è inoltre esposto ed affermato nell'art. 8 della Convenzione europea dei diritti dell'uomo[34]: ogni individuo ha diritto al rispetto della propria vita privata e familiare, e ogni forma di ingerenza pubblica deve essere giustificata dalla legge o da un interesse di grado superiore e collettivo.

Si potrebbe raffigurare l'identità digitale come composta da due set di informazioni: una prima parte riguarda dati statici, che indicativamente non si modificano con il passare del tempo, quali i dati anagrafici, e una seconda categoria di informazioni che si aggiornano periodicamente. Interessante notare come la prima tipologia consti di dati ampiamente reperibili in registri pubblici e quindi ipoteticamente meno tutelati giuridicamente sotto il profilo di protezione dei dati personali. Tali dati devono tuttavia essere protetti in quanto sono il punto di accesso per il secondo insieme di informazioni[35] che riguardano l'individuo, quali dati medico-sanitari, diplomi di istruzione o informazioni finanziarie.

Gli strumenti che abilitano l'identità digitale hanno quindi una duplice valenza, da un lato garantire e portare all'autodeterminazione dell'utente, come strumento di affermazione di individualità e controllo sui propri dati, dall'altro sono mezzi di cui avvalersi in relazione ai rapporti con lo Stato, che richiede informazioni certe per esercitare la propria governance.

4. Conclusioni

Siamo in un momento storico e sociale in cui Internet ha raggiunto una relazione molto intima con gli utenti: da una prima diffusione, che possiamo temporalmente collocare nell'ultimo decennio del Novecento, si è passati velocemente negli ultimi vent'anni a una fase in cui la rete e i servizi online sono progressivamente diventati via via più pervasivi nella vita degli utenti. Oggi ci troviamo in una situazione di quasi dipendenza di Internet: non solo i servizi critici, come quelli governativi o di difesa, non possono fare a meno della rete, ma anche i servizi essenziali, come quelli legati alla salute o all'istruzione, risultano di difficile utilizzo in assenza di una connessione. In questo contesto sembra ancora più necessaria una presa di posizione ferma da parte del regolatore, un sistema di governance che sia attuale e possa essere efficacemente utilizzato per gestire le nuove tecnologie del web: intelligenza artificiale, Internet of Things e DLT.

Il *Digital Market Act* ("DMA") è un ottimo esempio di questa tendenza: la qualificazione delle grandi piattaforme online quali "gatekeepers" (controllori dell'accesso) testimonia l'attenzione del legislatore alla creazione di un ecosistema controllato in cui l'utente possa autodeterminarsi senza temere la lesione dei propri diritti e senza delegare eccessivamente ai privati queste importanti attività. Il DMA, infatti, sancisce per i gatekeepers una nuova serie di obblighi che precludono l'attuazione di pratiche sleali avvalendosi della loro posizione predominante e consolidata nel mercato. Ai sensi del proposto art. 2, come "servizio di piattaforma di base" si individuano ad esempio: motori di ricerca online (come Google), servizi di social network online (Facebook), servizi di piattaforme per la condivisione di video (ad esempio YouTube), servizi di comunicazione elettronica interpersonale indipendente dal numero (ad esempio WhatsApp). L'obiettivo è garantire una concorrenza equa per tutti i fornitori di servizi digitali, accompagnata dall'incremento dell'innovazione, con una forte attenzione verso la protezione dei consumatori e, conseguentemente, dei loro dati personali.

eIDAS è stata la prima normativa che ha cercato di portare uniformità tecnologica all'interno del mercato europeo: la descrizione di diverse soluzioni, dall'identità digitale alla firma, per garantire uno scambio sicuro di informazioni e l'interazione tra cittadini e piattaforme, ha favorito la nascita di un trust *de facto* nei rapporti digitali. Gli utenti, le istituzioni e

le imprese sono confidenti nell'utilizzare le nuove tecnologie anche in rapporti complessi o che coinvolgono patrimoni ingenti. Per raggiungere questo obiettivo, il legislatore europeo non si è limitato a far un riferimento univoco a soluzioni tecnologiche ma ha creato un concetto di governance complesso, composto da una parte dai prestatori di servizi specifici – i prestatori di servizi fiduciari, anche qualificati – e dall'altra da enti di sorveglianza e accreditamento: in questo modo si è creato un ecosistema di fiducia digitale data dai costanti controlli e verifiche effettuati dai secondi nei confronti dei primi.

Tuttavia, la normativa che per quasi dieci anni ha guidato utenti e aziende verso la fiducia nel mondo digitale, ha inevitabilmente perso efficacia verso le più nuove tecnologie e le ultime logiche di interazione tra utenti, istituzioni e attori commerciali. È auspicabile che il nuovo Regolamento eIDAS, e l'evoluzione delle normative sopra richiamate (par. 2), prenda in considerazione da una parte il mutato scenario tecnologico e sociale – come, ad esempio, l'inclinazione del consumatore per il digitale oppure l'avvento di Intelligenza Artificiale, IoT e DLT – dall'altra non vengano dimenticati i limiti che l'attuale regolamentazione possiede, in modo da sfruttare il momento di aggiornamento per superarli. Su questo secondo punto si pensi ad esempio ad un approccio eccessivamente centralizzato, alla mancanza di uniformità giuridica delle soluzioni tecnologiche oppure ancora alla rigidità di determinati processi.

Come Internet e il Web sono nati da strumenti squisitamente tecnologici per poi essere regolamentati in modo da creare fiducia nel digitale e quindi adozione di massa, così le nuove tecnologie richiedono la presenza di ecosistemi di trust ben definiti, che possano garantire una continuità di utilizzo da parte degli utenti: trust framework dedicati che definiscano attori, ruoli e responsabilità. Questo approccio non solo garantisce il rispetto dei diritti ma abilita un mercato digitale cui il nostro Paese non può sottrarsi.

Note

[1] C. Costa, R. Torres, *To be or not to be, the importance of Digital Identity in the networked society*, in "Educação, Formação & Tecnologias", April 2011, p. 51.

[2] Una premessa semantica: seppur Internet e Web siano due concetti ben diversi, il primo un'infrastruttura e il secondo un software, in questo articolo saranno usati con il medesimo significato. Internet e Web come ecosistema, come luogo digitale in cui diversi attori interagiscono tra loro.

[3] P. De Filippi, S. Hassan, *Blockchain technology as a regulatory technology: From code is law to law is code*, in "First Monday", vol. 21, 2016, n. 12.

[4] M. Atzori, *Tecnologia blockchain e governance decentralizzata: lo Stato è ancora necessario?*, disponibile in SSRN, 1° dicembre 2015, p. 7.

[5] P. De Filippi, S. Hassan, *op. cit.*, pp. 15, 17.

[6] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[7] Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

[8] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

[9] Regolamento di esecuzione (UE) 2015/1502 della Commissione, dell'8 settembre 2015, relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

[10] Decreto legislativo 7 marzo 2005, n. 82 *Codice dell'amministrazione digitale* c.d. CAD.

[11] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[12] Decreto legislativo 9 aprile 2003, n. 70, *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.*

[13] Decreto legislativo 21 novembre 2007, n. 231, *Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.*

[14] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

[15] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[16] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

[17] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[18] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, 2020/0361 (COD).

[19] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) 2020/0374 (COD).

[20] *Ivi*, pp. 47-49.

[21] T. Lyons, L. Courcelas, K. Timsit, *Blockchain and Digital Identity. A thematic report prepared by the European Union Blockchain Observatory & Forum*, Blockchain for Government and Public Services, 2 May 2019.

[22] *Introducing the Trust over IP Foundation*, 5 May 2020.

[23] A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity. A white paper from the Sovrin Foundation*, 28 March 2017, p. 12, «if self-sovereign identity is the natural culmination of the evolution of Internet identity, then delivering it requires diffuse trust, portability, security and no single point of failure or control. Cryptographically secure distributed ledger technology provides the mechanism to make that happen».

[24] Proposta di Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea, COM/2021/281.

[25] European Commission – eIDAS Observatory, *eIDAS supported Self-Sovereign Identities*, May 2019.

[26] *Non Fungibile Token*, asset digitale intangibile e non fungibile realizzato con tecnologia crittografica che permette di certificare la proprietà di un ulteriore oggetto digitale, come ad esempio un'opera d'arte o un avatar in un ecosistema virtuale.

[27] Garante per la Protezione dei Dati Personali, *Parere all'AgID sullo schema di Linee guida dell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese*, 22 luglio 2021.

[28] Circolare Ministero dell'Interno n. 300-STRAD-1-10060. U-2021 del 17 novembre 2021, nota n. DRP/PS/147434 del 27 ottobre 2021.

[29] AgID, *Servizi di recapito certificato qualificato eIDAS*, 14 giugno 2021 e Id., *PEC: verso i servizi di recapito certificato qualificato*, 16 luglio 2021.

[30] Art. 44 eIDAS.

[31] S. Wachter, B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in "Columbia Business Law Review", 2019, n. 2, p. 125.

[32] C. Sullivan, *Digital Citizenship and the Right to Digital Identity Under International Law*, in S. Kierkegaard (ed.), "Information Ethics and Security", 2014, p. 72-84, disponibile in SSRN.

[33] A fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici (50), nel settore del diritto del lavoro e della protezione sociale e per finalità di sicurezza sanitaria (52), per finalità connesse alla salute (53), nel settore della sanità pubblica (54), fini di associazioni religiose ufficialmente riconosciute (55), nel corso di attività elettorali (56), per imporre limitazioni a specifici principi e diritti ove ciò sia necessario e proporzionato per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, per la tenuta di registri pubblici per ragioni di interesse pubblico generale (73), per trasferire dati se sussistono motivi di rilevante interesse pubblico (111), l'accesso del pubblico ai documenti ufficiali (154 e art. 86), l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6 lett. e), il trattamento di categorie particolari di dati personali (art. 9 lett. g e i), opposizione al diritto alla cancellazione (art. 17 co. 3 lett. c), deroga alla limitazione del trattamento (art. 18 co. 2), deroga al diritto di opposizione (art. 21 co. 6), limitare la portata di obblighi e diritti (art. 23 co. 1 lett. e), deroghe in specifiche situazioni (art. 49 co. 1 lett. d e co. 5).

[34] *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Roma, 4 novembre 1950.

[35] C. Sullivan, *op. cit.*

* * *

Internet governance: a digital trust matter

Abstract: There are two fundamental pillars that today grant a strong Internet with a reliable and globally usable governance: regulation and digital identity. The evolution of the Internet will be described starting from these two enablers of digital trust. Under the first aspect, initially the meaning and impact that Internet Governance has had at a theoretical-philosophical level will be analysed, investigating the relationship between law and code, and subsequently it will be examined in concrete terms what has been carried out by Italian and European legislators, who have long been looking for the best regulatory formula to guarantee an ecosystem capable of balancing the interests of citizens and the market. The second aspect of governance in an ecosystem as complex as the Internet is user identity. Attempts to approach the issue of online identity will be retraced: initial centralised solutions have given way to federated proposals, and trends towards democratisation and digital sovereignty have subsequently allowed a new approach, the one of Self Sovereign Identity, to flourish. Starting from an examination of the legislation in force in Europe, with some references to the regulatory interventions envisaged at EU level, it will be sought to explain which tools - technical and organisational - are most suitable for achieving a secure and reliable digital market.

Keywords: Digital trust – Digital identity – eIDAS

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0060
Articolo sottoposto a peer review

La Governance di Internet oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale

Angelo Alù

Il saggio identifica le principali questioni che il futuro ecosistema digitale pone, descrivendo il fenomeno della frammentazione di Internet come uno degli aspetti più complessi e problematici che emergono nell'attuale scenario geopolitico, ove si manifesta la tendenza degli Stati all'elaborazione di politiche "tecnonazionalistiche" volte alla costruzione di una Rete autonoma e indipendente, tecnologicamente difforme dall'originaria architettura distribuita e interoperabile su cui si basa il tradizionale modello operativo dell'Internet globale. Proliferano, infatti, nel panorama globale svariati interventi regolatori che impongono l'uso massivo di strumenti di sorveglianza generale per assicurare il controllo centralizzato della Rete, come obiettivo strategico prioritario di supremazia tecnologica stabilito a presidio delle infrastrutture critiche degli Stati, per evitare il rischio di possibili attacchi esterni in grado di destabilizzarne l'ordinamento interno. Rispetto alla progressiva balcanizzazione della Rete, si sta al contempo rafforzando, come imprevista variabile del mutato ecosistema di Internet, il potere – economico e politico – delle "Big Tech" nella veste di nuovi "players" dominanti che potrebbero dare vita ad un'inedita governance digitale oltre gli Stati.

Internet Governance – Frammentazione di Internet – Big-Tech – Splinternet – Sovranità digitale

Sommario: *1. Introduzione: verso nuovi modelli di governance digitale – 2. L'impatto delle politiche statali sulla frammentazione della Rete – 3. La sovranità digitale come nuova prospettiva europea del governo di Internet – 4. Scenari inediti e aspetti critici: una governance digitale oltre gli Stati?*

1. Introduzione: verso nuovi modelli di governance digitale

L'attuale ecosistema di Internet sembra manifestare una significativa metamorfosi dell'originario modello di governance digitale risalente alla sua iniziale configurazione delineata dalla cd. "Agenda di Tunisi"[1], che edifica un modello partecipativo funzionale a salvaguardare, nella definizione delle politiche dedicate alla gestione di Internet, il primato del settore pubblico, sul presupposto che debbano essere gli organi democraticamente legittimati nel circuito politico-istituzionale ad assumere le scelte finali sia pure all'esito di un costante dialogo di cooperazione multilaterale ispirato al criterio "multistakeholder"[2].

Rispetto alla prima fase di sviluppo embrionale della Rete[3], nell'ambito del percorso evolutivo dell'ecosistema digitale, si è progressivamente determinato, in un clima di crescenti tensioni tra le superpotenze a livello globale[4], uno speculare processo di "balcanizzazione" di Internet[5] che ha accentuato l'interesse degli Stati a intensificare le politiche di controllo per la gestione della Rete[6] anche nel tentativo di ridefinire i tratti della sua tradizionale architettura tecnica[7] al fine di raggiungere la supremazia tecnologica, economica ed industriale[8] e, al contempo, giustificare

A. Alù è dottore di ricerca in Giurisprudenza e consigliere della Internet Society Italia.
Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

l'estensione di pervasivi poteri di sorveglianza[9] che realizzano forme di "autoritarismo digitale"[10], senza spesso fornire adeguate protezioni contro gli abusi[11].

Alla luce di un contesto regolatorio sempre più divisivo e differenziato, emergono epocali cambiamenti tecnologici dalle rilevanti implicazioni non solo economiche ma anche politiche destinate a trasformare la società nel suo complesso[12].

In tale mutato scenario si manifestano i tratti peculiari di un'inedita governance digitale, in grado di formalizzare, mediante una ridefinizione dei rapporti di forza nei tradizionali assetti di equilibrio dei poteri, il primato – anche politico – delle imprese "high-tech" nella veste di nuovi "players" dominanti che, a fronte della progressiva frammentazione delle regolamentazioni nazionali su Internet, potrebbero infatti generare un nuovo – e attualmente indecifrabile – ecosistema tecnologico al di fuori degli ordinari circuiti decisionali di legittimazione democratica politico-istituzionale[13].

2. L'impatto delle politiche statali sulla frammentazione della Rete

Dalla sua originaria genesi risalente al primordiale progetto Arpanet, Internet si è rapidamente diffusa su scala globale – anche grazie alla creazione del cd. Web ("World Wide Web")[14] – determinando un incremento esponenziale degli utenti della Rete[15] che costituisce il "network of networks"[16] cui tutti possono accedere per reperire informazioni e diffondere informazioni fruibili in tutto il mondo.

L'espansione planetaria di Internet rende particolarmente controversa la regolamentazione della sua gestione tecnico-operativa, consentendo di comprendere il crescente interesse dei governi nazionali nei confronti di un'infrastruttura strategica, la cui concreta implementazione incide non solo sull'architettura logica della Rete, ma altresì sulle visioni politiche di controllo delle risorse digitali per assicurare l'erogazione dei servizi di telecomunicazione, l'esercizio dei diritti fondamentali degli individui e la tenuta degli standard democratici degli ordinamenti nazionali[17].

In tale prospettiva, si è intensificato il dibattito internazionale in ordine alla necessaria ridefinizione della governance digitale[18], per assicurare l'effettiva compartecipazione decisionale di tutti gli attori interessati al processo gestionale della Rete[19].

Già in occasione della rinegoziazione delle ITRs[20], è emerso un ostile contrasto, che sembra evocare l'inizio di un'inedita "digital cold war"[21], tra la visione decentralizzata di Internet (contraria a qualsivoglia regolamentazione frammentata della Rete in grado di limitarne la libertà) e la visione "statalista" (favorevole al riconoscimento di un maggiore potere degli Stati per assicurare, in nome di preminenti esigenze di sicurezza nazionale, una paritaria gestione nella funzione di controllo dell'infrastruttura tecnica di Internet)[22].

Alla luce delle divergenze esistenti sulla governance digitale nelle relazioni geopolitiche globali[23], si sta edificando, nell'ambito di una cornice regolatoria diversificata a livello nazionale, la costruzione di un'Internet alternativa (cd. "Splinternet"[24]) tecnologicamente difforme dall'originaria architettura distribuita e interoperabile della Rete.

In contrapposizione al tradizionale modello "aperto" di Internet, fondato sul primato tecnologico degli Stati Uniti d'America – che hanno (indirettamente) assunto a lungo, come unica superpotenza mondiale, il ruolo chiave di gestore principale della Rete attraverso l'attività dell'ICANN (*Internet Corporation for Assigned Names and Numbers*)[25] –, alcuni Stati stanno frammentando Internet, creando reti nazionali indipendenti dall'egemonia americana per evitare il rischio di ingerenze in grado di compromettere la sicurezza interna[26].

L'esigenza di proteggere lo spazio virtuale della Rete entro i propri confini nazionali viene invocata per rafforzare il ruolo degli Stati nazionali nell'ecosistema della Rete[27], anche mediante l'emanazione di leggi *ad hoc* volte alla creazione di un'Internet autonoma e sovrana[28] che consente di attuare forme pervasive di controllo sul flusso di informazioni veicolate online a presidio della cybersicurezza domestica[29].

La frammentazione di Internet, giustificata dalla necessità di ridurre la dipendenza esterna da organizzazioni straniere per rendere meno vulnerabili, mediante l'adozione di efficaci misure difensive, le infrastrutture nazionali critiche a fronte di possibili attacchi informatici in grado di pregiudicare gli interessi vitali di un Paese, realizza quindi un ingente controllo dei dati, anche intercettando le comunicazioni online – spesso con il supporto degli operatori telematici – per perseguire, sul versante interno, finalità di sorveglianza massiva con l'intento di contrastare e censurare gli avversari oppositori dei regimi politici in carica[30].

In tale scenario, la Russia, ad esempio, ha testato (nell'ambito di un ambizioso programma di implementazione dell'economia digitale[31]), la propria rete nazionale cd. "Runet"[32], come sistema alternativo di connessione Internet scollegato dal resto del mondo, che rappresenta il punto di inizio di una strategia di indipendenza tecnologica[33] in grado di bloccare l'accesso a servizi digitali stranieri, con indirette potenziali e insidiose ripercussioni per la libertà degli

utenti a causa di generalizzati effetti repressivi che potrebbero prodursi nell'ambiente virtuale mediante strumenti di "filtro" utilizzati per la selezione del flusso informativo veicolato online[34].

Internet risulta, pertanto, sottoposta a strategie massive di sorveglianza generale motivate dall'esigenza di assicurare la tutela della sicurezza nazionale, anche a costo di limitare le voci di dissenso esistenti, ove non allineate alla "narrazione" ufficiale della comunicazione istituzionale, consentendo il rafforzamento di regimi autocratici in grado di utilizzare massive tecnologie di manipolazione virtuale che trovano terreno fertile nel cyberspazio[35].

Anche le politiche tecnologiche del governo cinese alimentano ulteriormente la frammentazione della Rete[36] mediante il controllo centralizzato di Internet[37] che, pur sfruttando i vantaggi offerti dall'innovazione[38], richiede l'implementazione di specifici standard operativi funzionali a salvaguardare la sovranità digitale di Pechino[39], senza rendere le tecnologie volano di cambiamenti politici suscettibili di destabilizzare il sistema di potere vigente[40].

In particolare, l'infrastruttura cinese si basa su un'architettura digitale "separata e ideologicamente distinta"[41] dall'Internet globale che, in applicazione di un vasto e articolato insieme di leggi e regolamenti dettagliati[42], prevede svariati strumenti di censura[43] con funzioni di supervisione, blocco e monitoraggio del flusso comunicativo veicolato nell'ambiente digitale, grazie al sempre più sofisticato perfezionamento tecnico del cd. "Great Firewall"[44].

3. La sovranità digitale come nuova prospettiva europea del governo di Internet

Mentre ancora il dibattito internazionale si trova in una fase embrionale di ridefinizione teorica del governo digitale alla ricerca di soluzioni efficaci in grado di assicurare l'adeguamento dell'attuale ecosistema di Internet rispetto alle complesse sfide regolatorie[45] che l'innovazione pone, nel frattempo si assiste alla rapida implementazione di svariati progetti tecnologici, la cui configurazione applicativa espone al rischio di pervasivi strumenti di controllo automatizzato in grado di realizzare sofisticate forme di sorveglianza massiva per finalità generali di sicurezza[46], mediante inedite strategie di intelligence da "cyberwar"[47] legate all'utilizzo di tecnologie emergenti che consentono anche l'identificazione biometrica degli individui e il tracciamento computerizzato delle identità personali[48].

Nell'ambito dell'ecosistema digitale dell'Unione europea si registra un progressivo potenziamento delle azioni di cibersicurezza per combattere il crimine informatico, rafforzando le misure difensive a presidio delle infrastrutture critiche in presenza di uno scenario evolutivo sempre più insidioso, caratterizzato da un incremento esponenziale di inediti pericoli configurabili nell'ambiente virtuale, ove circola un flusso quotidiano di decine di quintilioni di byte di dati processati da miliardi di dispositivi IoT (che potrebbero raggiungere la quota di 125 miliardi entro il 2030[49]). Risulta, pertanto, necessario, in via prioritaria, predisporre una governance digitale autonoma e sovrana, stimolando le capacità strategiche e di cooperazione[50] dell'UE[51], per realizzare un cyberspazio aperto e sicuro, «come quinto dominio della guerra[52], fondamentale per le operazioni militari»[53].

Alla stato attuale sussiste un generale quadro di vulnerabilità riscontrabile negli Stati europei che impedisce il raggiungimento di adeguati standard di sicurezza[54], pur in presenza di un'economia digitalizzata sempre più interconnessa, sebbene esposta a possibili attacchi esterni ostili a causa di un diffuso deficit infrastrutturale aggravato da condizioni radicate di ritardo tecnologico[55] in stato di (cyber)"dipendenza neocoloniale"[56].

In tale prospettiva, l'Europa aspira a conquistare la cd. sovranità digitale[57], come obiettivo strategico di integrazione sovranazionale volto a realizzare un indispensabile riposizionamento geopolitico della propria centralità nella ridefinizione dei rapporti di forza esistenti su scala globale[58] rispetto alle dinamiche conflittuali della predominante competizione tecnologica dualistica USA-Cina, non solo per farsi trovare proficuamente pronta a cogliere le opportunità offerte dal progresso tecnologico (nell'ottica di favorire la crescita del mercato digitale e stimolare la competitività produttiva sulla spinta di ingenti investimenti e generali riforme dei settori maggiormente trainati dall'innovazione[59]), ma altresì, in chiave preventiva, per evitare di subire cd. "minacce ibride"[60] a causa di attacchi informatici, interventi di cyberspionaggio[61], campagne massive di disinformazione, azioni di disturbo e strategie di manipolazione sistemica dell'opinione pubblica in grado di destabilizzare la società nel suo complesso[62], mettendo a rischio la tenuta degli ordinamenti democratici[63].

Pur essendo ancora significativo il "gap" tecnologico rispetto alle superpotenze globali, l'Unione europea, grazie ad un recente incisivo approccio regolatorio[64] interventista e proattivo, sta consolidando un quadro giuridico sempre più vigoroso e sviluppato in grado di modellare la governance di Internet, la cui configurazione potrebbe imporsi nella concreta prassi in ragione del rilevante valore economico del mercato digitale europeo, con l'effetto catalizza-

tore di indurre il tessuto imprenditoriale "high-tech" su scala planetaria ad adeguarsi spontaneamente alle relative prescrizioni per poter instaurare vantaggiosi rapporti commerciali forieri di un ingente introito di profitti generati dal settore ICT[65].

4. Scenari inediti e aspetti critici: una governance digitale oltre gli Stati?

La governance di Internet[66] è stata formalizzata in sede internazionale con l'istituzione dell'Internet Governance Forum (IGF)[67] che opera, con un mandato quinquennale soggetto a revisione periodica[68], come *forum* multilaterale, aperto, inclusivo e collaborativo chiamato ad esprimersi sui temi legati all'ecosistema della Rete mediante la semplice formulazione di mere raccomandazioni senza però adottare decisioni vincolanti, pur garantendo la formale paritaria rappresentatività di tutte le parti interessate (Stati, istituzioni accademiche, settore privato e società civile) coinvolte nell'ambito dei lavori realizzati da gruppi consultivi che si riuniscono durante ogni consueto *meeting* annuale[69].

Sebbene siano stati promossi anche forum nazionali per stimolare ulteriormente la cooperazione su vasta scala secondo un maggiore diffuso livello di interazione e integrazione tra gli attori interessati al processo di definizione delle politiche sulla Rete[70], nella concreta prassi la partecipazione dei governi è progressivamente diminuita poiché l'IGF rappresenta in ogni caso un organismo informale privo di poteri cogenti, rendendo quindi l'incidenza dei relativi lavori conclusivi generalmente tenue e marginale in termini di azioni concrete tangibili sull'ecosistema digitale[71].

In tale prospettiva, l'attuale (ancora per poco?) modello di governance risulta progressivamente eroso dall'avvento di un inedito ecosistema digitale fondato sulla concentrazione di potere in capo alle autorità nazionali per isolare Internet, in reti sempre più disconnesse, entro i propri confini territoriali, unitamente al crescente dominio – economico e politico – delle imprese "high-tech"[72].

In un mutato scenario di contesa geopolitica, sembra pertanto delinearsi una progressiva perdita di centralità dell'IGF[73], al pari di qualsivoglia ulteriore iniziativa internazionale di cooperazione multilaterale[74].

Anche sulla spinta di esigenze di regolamentazione a "geometria variabile" volte al rafforzamento della "sovranità digitale"[75], in un crescente clima di tensioni tra le superpotenze globali (destinate verosimilmente a culminare in una possibile "alleanza tecnologica anti-cinese"[76]), emerge, infatti, la configurazione "tripolare"[77] di Internet che, lungi dal privilegiare forme di multilateralismo partecipativo, risulta scomponibile in distinti poli di influenza nella definizione delle regole applicabili all'ambiente digitale, dando vita ad un processo di balcanizzazione destinato a sfociare nella frammentazione di un variegato quadro giuridico sull'ecosistema della Rete, in cui i singoli Stati cercano sempre più spesso di imporre i propri specifici orientamenti politici "particolari" per definire le caratteristiche di un nuovo cyberspazio dalle caratteristiche di funzionamento del tutto diverse rispetto alla sua originaria conformazione libertaria[78].

Invero, lo sforzo competitivo dei governi nazionali per affermare la propria autorità su Internet si sta intensificando in parallelo al crescente potere dei "Colossi del web" che potrebbero rappresentare un'ulteriore variabile – ancora non del tutto decifrabile – per la nascita di un nuovo ordine "tecno-politico" globale.

Le aziende tecnologiche stanno, infatti, assumendo le inedite sembianze di dominanti "digital decision makers" per la definizione delle nuove "regole del gioco" da imporre a livello planetario – in una logica presumibilmente non neutrale e discriminatoria[79] – nell'ambito della progressiva frammentazione di Internet alimentata dai recenti interventi settoriali adottati dai singoli Stati che, piuttosto che rafforzare le garanzie di tutela dei diritti configurabili in Rete, approfittano dei pericoli di propaganda estremista, odio, disinformazione, attacchi informatici e illeciti di varia natura sempre più diffusi online[80] per rivendicare, spesso anche con la complicità degli stessi intermediari telematici fornitori dei servizi digitali[81], l'acquisizione di pervasivi poteri di controllo e repressione come decisa inversione di rotta rispetto all'originaria configurazione del governo della Rete esistente su scala globale[82].

In altri termini, si potrebbe progressivamente affermare un'inedita governance digitale[83] declinabile anche oltre gli Stati, cedendo quindi il passo al definitivo primato dei cd. "Colossi del web"[84], fondato sull'uso pervasivo di sofisticati e invisibili sistemi algoritmici di tracciamento, profilazione[85] e manipolazione[86] dalle implicazioni ancora non del tutto note[87].

Note

[1] Cfr. *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6, 18 November 2005.

[2] Al riguardo, l'Agenda di Tunisi sottolinea che: «a) l'autorità politica per le questioni di politica pubblica relative a Internet è il diritto sovrano degli Stati [...]; b) il settore privato ha avuto e dovrebbe continuare ad avere un ruolo importante nello sviluppo di Internet, sia in campo tecnico che economi-

co; c) anche la società civile ha svolto un ruolo importante in materia di Internet, in particolare a livello di comunità, e dovrebbe continuare a svolgere tale ruolo; d) le organizzazioni intergovernative hanno avuto e dovrebbero continuare a svolgere un ruolo di facilitazione nel coordinamento delle questioni di politica pubblica legate a Internet; e) anche le organizzazioni internazionali hanno avuto e dovrebbero continuare a svolgere un ruolo importante nello sviluppo di standard tecnici relativi a Internet e politiche pertinenti»: cfr. *Tunis Agenda for the Information Society*, cit., p. 35.

[3]Lo sviluppo tecnologico di Internet risale alla creazione della rete Arpanet, come sistema affidabile di comunicazione distribuita, progettato per garantire la trasmissione di informazioni tra le unità periferiche in condizioni di stabilità e sicurezza grazie al perfezionamento di una struttura aperta e decentralizzata, basata sulla tecnologia "packet switching", implementata per evitare rischi di paralisi e blocchi causati da vulnerabilità e criticità in grado di determinare possibili danneggiamenti con la conseguente perdita dei dati memorizzati. Sul tema: A. Di Corinto, *Internet non è nata come progetto militare, mettetevelo in testa*, in L. Abba, A. Di Corinto (a cura di), "Il futuro trent'anni fa. Quando Internet è arrivata in Italia", Manni, 2017.

[4]Cfr. C. Hobbs (ed.), *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*, European Council on foreign relations, 30 July 2020; M. Leonard, J. Shapiro, *Strategic sovereignty: How Europe can regain the capacity to act*, European Council on foreign relations, 25 June 2019.

[5]Per un approfondimento sul tema si rinvia a M. Bey, *The Age of Splinternet: The Inevitable Fracturing of the Internet*, in "Worldview", 25 April 2019.

[6]Al riguardo, si rinvia alle osservazioni di L. Zorloni, *La Cina non ha rinunciato al suo progetto per cambiare i connotati di internet*, in "Wired.it", 11 dicembre 2021. In particolare, l'autore descrive la strategia della Cina volta a sostituire, con il nuovo protocollo "New IP", l'attuale standard di Internet, per superare il modello TCP/IP, al fine di risolvere i problemi della Rete globale e garantire l'efficiente sviluppo dei servizi digitali, senza al contempo frenare il processo evolutivo dell'innovazione. Si veda anche L. Zorloni, *La silenziosa battaglia della Cina per cambiare le regole di internet*, in "Wired.it", 9 dicembre 2020.

[7]L'architettura tecnica di Internet si basa sul funzionamento del cd. "Internet Protocol Suite" (regolato dalla RFC 791/1981), e consta di due protocolli primari di trasmissione: il TCP (*Transmission Control Protocol*), e l'IP (*Internet Protocol*), che assicurano l'intercomunicabilità univoca dei dati trasmessi da reti diverse.

[8]Si veda N. Attrill, A. Fritz, *China's cyber vision: How the Cyberspace Administration of China is building a new consensus on global internet governance*, Policy Brief Report No. 52/2021, International Cyber Police Centre, November 2021.

[9]Secondo le rilevazioni empiriche contenute nel Report *Freedom House 2021*. Sul tema si segnala L. Zorloni, *La Cina può disconnettersi dall'internet globale quando vuole*, in "Wired.it", 20 agosto 2019.

[10]Cfr. R. Kemeny, *Brazil is sliding into techno-authoritarianism*, in "MIT Technology Review", 19 August 2020.

[11]Prolifera la frammentazione sempre più conflittuale e illiberale della Rete in sistemi autoreferenziali localizzati entro i confini statali, regolati da legge nazionali e separati dall'ecosistema globale di Internet, con il rischio di generare l'utilizzazione massiva di svariati sistemi di "filtri" dei contenuti controllati online per finalità politiche di censura e sorveglianza su vasta scala. Si vedano: J.C. Wong, *Revealed: the Facebook loophole that lets world leaders deceive and harass their citizens*, in "The Guardian", 12 April 2021; G. Porro, *Putin incassa il primo sì per isolare internet in Russia*, in "Wired.it", 12 aprile 2019.

[12]Sul versante imprenditoriale si assiste alla promozione, in via sperimentale, di numerose iniziative formative per sviluppare le competenze digitali richieste dal mercato del lavoro e incrementare le opportunità professionali legate al settore ICT, con l'intento di fornire soluzioni di alta specializzazione nei settori più altamente remunerativi (come, ad esempio, i cd. "Google Career Certificates"), unitamente all'inedita definizione di politiche di "cyber-welfare state" redistributive della ricchezza, mediante l'erogazione di un reddito universale di base come sussidio pagato agli individui, indipendentemente dal fatto che lavorino o meno, nell'ottica di compensare gli svantaggi derivanti da una possibile contrazione della forza lavoro provocata dalla cd. "automazione dei processi robotici". Sul tema: J. Sadowski, *Why Silicon Valley is embracing universal basic income*, in "The Guardian", 22 June 2016.

[13]Alla crescita continua di ricavi generati dall'utilizzo massivo di un'elevata varietà di applicazioni, piattaforme di e-commerce, servizi di messaggistica e social network offerti in regime di strapotere tecnologico a istituzioni pubbliche, imprese, operatori privati e utenti cittadini, si aggiunge l'ulteriore massiva acquisizione, da parte dei "Colossi del web", di un consistente patrimonio di dati personali, da cui discende un enorme potere gestito da imprese private che sono in grado di influenzare, anche indirettamente, le scelte dell'opinione pubblica sul dibattito politico e la libertà di autodeterminazione individuale. Sia consentito rinviare ad A. Alù, *Stati contro le big tech: siamo allo scontro finale? La linea dura di Ue, Usa e Cina*, in "Agendadigitale.eu", 13 maggio 2021.

[14]Il Web è stato sviluppato da Tim Berners-Lee, insieme a Robert Calliau, nel 1991 presso il CERN di Ginevra, come innovativo servizio di organizzazione dei contenuti disponibili online, basato sul linguaggio "html" (*Hypertext markup language*) che consente agli utenti di reperire facilmente le informazioni ricercate mediante collegamenti ipertestuali (cd. "link"), con l'intento di promuovere, come "mission" valoriale sottesa alla realizzazione del progetto, la diffusione di una Rete universale, libera e accessibile. Per un approfondimento, T. Berners-Lee, *L'architettura del nuovo web*, Feltrinelli, 2001.

[15]Secondo il Report "Global Digital 2020", a fronte di poco meno di 8 miliardi di persone, sono 4,66 miliardi gli utenti che accedono ad Internet, come quota che rappresenta il 59,5% di penetrazione globale (con un incremento del 7,3% rispetto al precedente anno), mentre risultano attivi 4,20 miliardi di utenti delle piattaforme sociali, registrando una penetrazione dei social pari al 53% della popolazione mondiale (con un incremento del 13% rispetto al 2020). Circa 5,22 miliardi di persone utilizzano telefoni cellulari, pari al 66,6% della popolazione globale. L'utente medio di Internet trascorre online 6 ore e 43 minuti ogni giorno (corrispondenti a più di 100 giorni di connessione l'anno), di cui circa 2 ore e 30 minuti nei social network (cfr. Report *Digital 2021 – Global Overview Report*, in "We are Social", in collaborazione con Hootsuite).

[16]Cfr. Corte Federale degli Stati Uniti – Distretto Orientale della Pennsylvania, sentenza 11 giugno 1996, caso *American Civil Liberties Union e American Library Association v. Stati Uniti d'America*.

[17]Su tali aspetti si rinvia a L. Abba, A. Alù, *Internet Governance Forum: l'evoluzione del modello multi-stakeholder tra criticità e prospettive future*, in questa Rivista, 2020, n. 1.

[18]In tal senso, Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni *Governance e politica di Internet, il ruolo dell'Europa nel forgiare il futuro della governance di Internet*, doc. COM(2014) 72 del 12 febbraio 2014.

[19]*Principles for the Governance and Use of the Internet*, elaborati nell'ambito del Council Working Group on

International Internet-Related Public Policy Issue, Brasile, 2012.

[20]Le *International Telecommunication Regulations* (ITRs), adottate dall'ITU nel 1998 a Melbourne a conclusione della *World administrative telegraph and telephone conference*, costituiscono la fonte di regolamentazione internazionale delle telecomunicazioni. Poiché le ITRs erano inizialmente applicabili alle sole comunicazioni radiotelegrafiche e telefoniche con esclusione della Rete Internet, si è svolta, a Dubai nel dicembre 2012, la *World Conference on International Telecommunication* (WCIT-2012), su impulso dell'International Telecommunication Union (ITU) per assicurare il necessario adeguamento di tali norme al progresso tecnologico del sistema delle comunicazioni, in attuazione della Resolution 146 (Antalya, 2006), *Rewiew of the International Telecommunication Regulations*.

[21]L.S., *A digital cold war?*, in "The Economist", 14 December 2012.

[22]Sul tema, si rinvia alle osservazioni di T. Natoli, *Il ruolo delle organizzazioni internazionali nella gestione delle reti digitali globali*, in F. Marcelli, P. Marsocci, M. Pietrangelo (a cura di), "La Rete Internet come spazio di partecipazione politica. Una prospettiva giuridica", Editoriale Scientifica, 2015, p. 116 ss.

[23]Nel corso dei lavori dell'*Internet Governance Forum* di Rio de Janiero del 2007, ad esempio, è stato approfondito l'attuale meccanismo di gestione della radice di Internet indirettamente affidata agli USA per il tramite dell'ICANN.

[24]A. Di Corinto, *Splinternet, la frammentazione della Rete è servita, e dobbiamo preoccuparci*, in "Italian.Tech", 11 giugno 2021.

[25]L'ICANN, costituita il 18 settembre 1998, su impulso del Dipartimento del Commercio degli Stati Uniti d'America, nella forma di un organismo privato, malgrado il riconoscimento di una sfera di autonomia ed indipendenza (avvenuto ad opera dell'*Affirmation of Commitments* del 2009), resta comunque in qualche modo legata al governo americano (anche attraverso un contratto di consulenza rinnovato ogni tre anni). L'ICANN rappresenta l'organismo di vertice della governance di Internet, che esercita la funzione primaria di gestione della radice logica di Internet, mediante la configurazione delle risorse di identificazione (indirizzi IP e nomi di dominio), l'assegnazione e la gestione dei nomi di dominio, degli indirizzi IP e la supervisione dei tredici *root server*, di cui la cd. *root authority* (o *root administration*), contenente il database ufficiale di tutti i Tld registrati, e regola la struttura gerarchica dei nomi di dominio. L'ICANN esercita, pertanto, un rilevante potere di regolamentazione della Rete che manifesta implicazioni formalmente tecniche, ma dal sostanziale contenuto politico. Per un approfondimento: D. De Grazia, *L'Internet Governance tra tecnica, politica e diritto*, in "Informatica e Diritto", 2009, n. 1, pp. 29-45.

[26]Emblematico il caso della Cina, cha ha implementato il cd. "Great Firewall" in grado di controllare l'accesso al cyberspazio nazionale, limitando la fruizione di determinati contenuti veicolati online. P. Banerjee, *How nationalism gave birth to the splinternet*, in "Mint", 18 February 2021.

[27]Cfr. E. Claessen, *Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU*, in "Journal of Cyber Policy", vol. 5, 14 February 2020, n. 1, p. 140-157.

[28]Sulla falsariga del modello cibernetico predisposto dalla Corea del Nord: cfr. J. McCurry, *North Korea only has 28 websites, according to leak of official data*, in "The Guardian", 21 September 2016.

[29]Come prevede, ad esempio, il progetto di riforma predisposto in Russia, recante modifiche alle leggi federali in materia di comunicazioni, tecnologie informatiche e protezione dei dati. In particolare, la *ratio* dell'intervento legislativo mira ad assicurare l'introduzione di misure di protezione finalizzate a garantire il funzionamento stabile di Internet nel rispetto di stringenti regole di instradamento del traffico, mediante una gestione centralizzata dei contenuti per fronteggiare possibili disconnessioni dalla Rete globale in caso di minacce esterne suscettibili di pregiudicare la sicurezza e la stabilità dei servizi essenziali del Paese. Per un approfondimento A. Shcherbovich, *The Russian Bill On Internet Sovereignty Adopted By The State Duma In First Reading*, in "CyberBRICS", 27 February 2019.

[30]Cfr. *Russia Plants Its Flag in the Digital Realm*, in "Worldview", 19 March 2019.

[31]Cfr. *Digital Economy National Program*.

[32]J. Wakefield, *Russia 'successfully tests' its unplugged internet*, in "BBC", 24 December 2019. Si veda anche G. Porro, *La Russia sta facendo passi avanti nella costruzione della sua internet indipendente*, in "Wired.it", 12 aprile 2021.

[33]In attuazione della Strategia per la sicurezza nazionale, che ha recepito la cd. "Information Security Doctrine", la Russia mira a neutralizzare i fattori esterni di destabilizzazione derivanti dalla superiorità tecnologica di alcuni Paesi (come, ad esempio, gli USA), in grado di dominare il cyberspazio, per evitare il rischio di subire un controllo, da parte di forze straniere, sul flusso di informazioni veicolate nello spazio virtuale della Rete. A tal fine, nell'ottica di proteggere l'infrastruttura critica del paese, la Russia ha implementato il funzionamento affidabile di una rete nazionale sovrana completamente isolata per garantire, in caso di minacce esterne, un controllo centralizzato delle risorse digitali attraverso nodi di accesso autorizzati ed elencati in un apposito registro governativo, nel rispetto delle prescrizioni indicate dalla legge "Sovereign internet" n. 608767-7.

[34]Per un approfondimento si veda M. Smeltzer, I. Linzer, *Russian Elections Will Put the Kremlin's Internet Controls to the Test*, in "Freedom House", 14 September 2021.

[35]Si veda lo studio *Splintered Speech - Digital Sovereignty and the Future of the Internet*, in "PEN America".

[36]Cfr. K. O'Hara, W. Hall, *The dream of a global internet is edging towards destruction*, in "Wired.co.uk", 24 December 2019.

[37]S. Hoffman, D. Lazansky, E. Taylor, *Standardising the splinternet: how China's technical standards could fragment the internet*, in "Journal of Cyber Policy", vol. 5, 29 August 2020, n. 2, p. 239-264.

[38]Particolarmente rilevante è l'iniziativa "Internet Plus" con cui la Cina mira a stimolare l'innovazione tecnologica incentivando lo sviluppo di un florido ecosistema nazionale per sostenere la crescita economica del Paese (cfr. Z. Wang, C. Chen, B. Guo, Z. Yu, X. Zhou, *Internet Plus in China*, in "IT Professional", vol. 18, 2016, n. 3, p. 5-8). Pechino ha, inoltre, realizzato il vasto programma internazionale di sviluppo infrastrutturale cd. "Belt and Road Initiative" (anche noto come cd. "via della seta digitale"), che prevede una strategia di esportazione tecnologica del modello di governance digitale cinese mediante il consolidamento di relazioni bilaterali con circa 40 altri Paesi (cfr. A. Chatzky, J. McBride, *China's Massive Belt and Road Initiative*, in "Council on Foreign Relations", 28 January 2020).

[39]Sul tema J.Min, *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, in "SAIS Review of International Affairs", Project MUSE, vol. 30, 2010, n. 2, p. 71-89.

[40]Si riscontra la tendenza a frammentare Internet soprattutto nei regimi autoritari, ove reti nazionalizzate prevedono barriere tecnologiche di blocco anche per reprimere proteste pacifiche di mobilitazione pubblica (cfr. *Report #KeelptOn 2019*, AccessNow, 22 June 2019). Peraltro, la pandemia "Covid-19" ha ulteriormente accentuato il ricorso a svariate forme di li-

mitazione generale della libertà di informazione, giustificando a tal fine la legittimità del controllo statale per la salvaguardia della salute e dell'ordine pubblico (cfr. *COVID-19 Civic Freedom Tracker*, International Center for Not-for-Profit Law, European Center for Not-for-Profit Law).

[41] F. Kenyon, *China's 'splinternet' will create a state-controlled alternative cyberspace*, in "The Guardian", 3 June 2021.

[42] A tal fine, il governo cinese configura la cd. "sovranità informatica" come peculiare paradigma del dominio nazionale fondante l'infrastruttura normativa e tecnologica dello Stato, da cui discendono stringenti poteri di controllo sulle informazioni pubblicate in Rete. Cfr. State Council Information Office of People's Republic of China (SCIO), *Full Text: White paper on the Internet in China*, in "China Daily", 6 August 2010.

[43] Secondo il report *Freedom on the Net 2019*, in Cina, per il quarto anno consecutivo, si registrano le peggiori violazioni della libertà di Internet a causa di livelli di censura "senza precedenti", unitamente alla circolazione di contenuti a "senso unico" di sostegno al regime politico in grado di plasmare il conformismo ideologico di massa orientato a supportare la visione governativa, con il risultato di ridurre sensibilmente il pluralismo informativo soprattutto in relazione alla discussione su argomenti politici, economici e militari ritenuti "sensibili" dal regime.

[44] Il cd. "Great Firewall", noto anche come *Golden Shield Project*, è il progetto di censura e sorveglianza di Internet del governo cinese che, nel perseguire l'obiettivo di incrementare la competitività della Cina secondo standard di sviluppo occidentale, promuove l'uso e la diffusione delle tecnologie come strumenti in grado di stimolare la crescita economica del Paese, evitando però il rischio che l'accesso generalizzato ad Internet possa minare la stabilità politica interna mediante un sistema di filtraggio dei contenuti, reso ancor più efficace – in contrapposizione all'ideologia occidentale – dalla dominante cultura cinese dell'autocensura, alimentata da un pervasivo controllo delle informazioni realizzato con il supporto di volontari reclutati per segnalare contenuti offensivi, oggetto di denunce indirizzate alle forze di polizia. Nel rispetto di quanto previsto da una recente legge in materia di sicurezza informatica che impone la raccolta e la conservazione di tutti i dati personali nel territorio cinese, allo scopo di proteggere i cittadini cinesi da interferenze esterne di governi stranieri, anche le aziende tecnologiche straniere sono tenute ad adeguarsi, per evitare l'interruzione dei propri servizi, alle disposizioni normative vigenti, localizzando obbligatoriamente i prescritti dati su server gestiti da società statali cinesi. Per un approfondimento generale sul tema si rinvia a G.R. Barme, S. Ye, *The Great Firewall of China*, in "Wired.com", 1 June 1997.

[45] Prendendo atto del rilevante impatto delle tecnologie emergenti grazie al progressivo incremento della potenza di calcolo dei sistemi automatizzati, il 12 febbraio 2019, il Parlamento europeo ha approvato la Risoluzione "su una politica industriale europea globale in materia di robotica e intelligenza artificiale", ove si sottolinea la necessità di promuovere una «società supportata dall'intelligenza artificiale e dalla robotica», come fattore indispensabile per migliorare la produttività delle imprese, la crescita economica e il benessere sociale delle persone. Si tratta pertanto di una prioritaria azione di intervento, che richiede la necessaria predisposizione di regole chiare e omogenee, evitando la frammentazione del quadro normativo, per gestire le opportunità e le minacce dell'IA, alla luce degli attacchi informatici che possono mettere in pericolo la sicurezza pubblica e privata, con conseguenti rischi per la democrazia e per la tutela dei diritti fondamentali degli utenti, anche a causa della possibile manipolazione di contenuti personalizzati in grado di provocare distorsioni della percezione della realtà, da cui discendono effetti negativi sulla formazione delle opinioni pubbliche e sulla libertà di scelta delle persone. A tal fine, il 20 ottobre 2020, il Parlamento ha adottato un documento che illustra le coordinate di regolamentazione dell'Unione europea in materia di IA, con l'intento di promuovere l'innovazione, garantire il rispetto degli standard etici ed assicurare la fiducia nell'uso consapevole della tecnologia, mediante l'elaborazione di raccomandazioni volte a sollecitare il potere di iniziativa della Commissione europea, che, il 21 aprile 2021, ha ufficialmente formulato la Proposta di Regolamento del Parlamento europeo e del Consiglio recante regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale).

[46] Al riguardo, l'ultima edizione del report *Automating Society 2020* descrive le prospettive future caratterizzanti lo sviluppo evolutivo dei sistemi decisionali automatizzati, evidenziando rilevanti criticità e aspetti problematici derivanti dalla crescente diffusione di dispositivi e sensori in grado di raccogliere un'enorme quantità di dati processati da algoritmi sempre più sofisticati: cfr. F. Chiusi, S. Fisher, N. Kayser-Bril, M. Spielkamp (eds.), *Automating Society Report 2020*, AlgorithmWatch, October 2020.

[47] Cfr. L. Damiano, L. Franchina, *Cyberwar sulle infrastrutture critiche: i nuovi scenari*, in "Agendadigitale.eu", 29 marzo 2021.

[48] Diventa prioritaria la pianificazione operativa di strategie militari in grado di realizzare il cd. "dominio dell'identità" per finalità antiterroristiche e contro-insurrezionali, mediante la raccolta di un'ingente quantità di dati biometrici per tracciare le persone sospettate di essere una potenziale minaccia per la sicurezza: cfr. M. Hu, *Cautionary tale: The Taliban could get access to Afghans' biometric data collected by the US*, in "Scroll.in", 1 September 2021.

[49] Cfr. *Number of connected IoT devices will surge to 125 billion by 2030*, in "Semiconductor Digest", 2017.

[50] In particolare, l'Unione europea, al fine di proteggersi dalle minacce informatiche provenienti dall'esterno dei suoi confini, collabora con il Servizio europeo per l'azione esterna e gli Stati membri per l'attuazione coordinata di una risposta diplomatica congiunta in caso di attività informatiche dannose, nell'ambito di concrete forme di cooperazione e di dialogo in grado di predisporre misure preventive contro gli attacchi informatici. Parimenti rilevanti risultano, altresì, in materia di difesa nel ciberspazio le attività dell'Agenzia europea per la difesa, nonché dell'ENISA, dell'Europol e della direzione generale della Commissione responsabile dell'industria della difesa: cfr. European Commission, *Cybersecurity Policies*.

[51] Per costruire un'Europa resiliente, verde e digitale, è stata adottata nel 2020 la Strategia UE per la cibersicurezza che (come pilastro chiave del documento *Shaping Europe's Digital Future*, in attuazione del *Recovery Plan for Europe* e della *Strategia per l'Unione della sicurezza 2020-2025*), prevede una serie di interventi legislativi finalizzati a tutelare gli utenti contro il rischio di minacce informatiche. Prendendo atto del crescente aumento del numero di attacchi informatici, l'Unione europea si impegna a realizzare un ecosistema digitale sicuro e tecnologicamente sovrano, mediante l'elaborazione di standard tecnici affidabili definiti nell'ambito di un quadro omogeneo di certificazione unico a presidio delle infrastrutture critiche. A tal fine, la Commissione europea ha anche proposta nel 2020 una revisione della direttiva NIS 2016/1148 sulla sicurezza delle reti e dei sistemi informativi per intensificare la lotta contro la criminalità informatica. Inoltre, nell'ottica di migliorare le capacità esistenti in materia di cibersicurezza, la Commissione europea ha sviluppato la piattaforma *Atlante*, unitamente all'istituzione del *Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza*, con il compito di costruire un'agenda comune per gli investimenti nella sicurezza informatica e decidere le priorità di finanziamento per la ricerca, lo sviluppo e l'implementazione di

soluzioni di sicurezza informatica. In attuazione della strategia dell'UE per la cibersicurezza e della strategia dell'UE per l'Unione della sicurezza, è stata inoltre prevista la costituzione del *Joint Cyber Unit* per garantire una risposta coordinata dell'UE a crisi e incidenti informatici verificabili su larga scala.

[52]Oltre a terra, mare, aria e spazio.

[53]Cfr. Consiglio dell'Unione europea, *Cybersecurity: how the EU tackles cyber threats*.

[54]*Ibidem*.

[55]Più del 90% dei dati provenienti dall'Occidente risulta, infatti, ospitato e custodito negli Stati Uniti d'America, a causa della mancanza di server di raccolta europei. Pertanto, nell'ottica di colmare tale ritardo e attenuare le condizioni di arretratezza tecnologica è stato sviluppato il progetto *Gaia-X*, come infrastruttura di dati fondante un ecosistema digitale aperto, trasparente e sicuro. Peraltro, rispetto al primato economico dei cd. "Colossi del web" (identificati dall'acronimo "GAFA" che comprende, tra le più importanti realtà tecnologiche del mondo, note aziende americane leader nel settore tecnologico), non risultano invece aziende europee classificate nella Top 20 delle migliori imprese "high-tech"; cfr. S. Fleming, *What is digital sovereignty and why is Europe so interested in it?*, in "The European Sting", 16 March 2021.

[56]Cfr. C. Hobbs, *op. cit.*

[57]K. Propp, *Waving the flag of digital sovereignty*, in "New Atlanticist", 11 December 2019.

[58]Per un'analisi esaustiva sul tema della sovranità europea si rinvia a M. Leonard, J. Shapiro, *op. cit.*

[59]Lo studio *PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution* afferma che entro il 2030 l'IA genererà ricavi stimati pari a 15,7 trilioni di dollari, con un aumento del 26% del PIL globale grazie al miglioramento della produttività globale di circa il 40%, mentre il 65% del PIL globale sarà digitalizzato entro il 2022 con una stima di oltre 6,8 trilioni di dollari nel prossimo triennio; cfr. *Idc FutureScape: Worldwide digital transformation 2021 predictions*.

[60]G. Gressel, *Protecting Europe against hybrid threats*, European Council on Foreign Relations, 25 June 2019. In particolare, l'autore ricostruisce la nozione di "minacce ibride" per indicare «l'uso di attori sponsorizzati dallo Stato, ma non ufficialmente affiliati (negabili), che non ricorrono alla violenza fisica [...] Lo scopo delle minacce ibride è costringere l'oggetto di una minaccia a conformarsi agli interessi strategici dell'aggressore», come insidioso pericolo configurabile nell'ambito di una "guerra non lineare", "conflitto asimmetrico" e "sovversione".

[61]L. Cerulus, *Europe raises flags on China's cyber espionage*, in "Politico.eu", 4 ottobre 2018.

[62]La disinformazione online è un fenomeno sempre più dilagante che, a causa della creazione di cd. "bolle di filtro", favorisce la circolazione di fake news con conseguente "polarizzazione ideologica" degli utenti attirati da informazioni (anche se false o distorte) corrispondenti alle proprie convinzioni personali e inconsapevolmente sottoposti a sofisticate tecniche di manipolazione predisposte, anche mediante l'uso di falsi account e bot automatizzati, per "inquinare" il dibattito pubblico. Al riguardo, lo studio *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation*, sottolinea che «rispetto a 48 paesi nel 2018 e 28 paesi nel 2017 [...] in ogni paese, c'è almeno un partito politico o un'agenzia governativa che utilizza i social media per plasmare gli atteggiamenti pubblici a livello nazionale [...] per sopprimere i diritti umani fondamentali, screditare gli oppositori politici e soffocare le opinioni dissenzienti». Il report *Misinformation Review* mette in evidenza gli effetti della cd. "infodemia" nella diffusione di informazioni false e fuorvianti pubblicate sui social network per manipolare l'opinione pubblica (A. Bridgman, E. Merkley, P.J. Loewen, T. Owen, D. Ruths, L. Teichmann, O. Zhilin, *The causes and consequences of COVID-19 misperceptions: Understanding the role of news and social media*, in "The Harvard Kennedy School Misinformation Review", vol. 1, 18 June 2020, n. 3, Special Issue on *COVID-19 and Misinformation*).

[63]La ricerca *Survey on the Future of Democracy in the Digital Age* prospetta un progressivo peggioramento del sistema politico democratico entro il 2030 a causa dell'uso strategico dei social media utilizzati per veicolare disinformazione in grado di minare la fiducia delle persone nei confronti delle istituzioni, esponendo inoltre gli utenti al rischio di violazioni della privacy, nonché a forme svariate di controllo realizzato da sistemi massivi di sorveglianza e censura per scopi politici.

[64]Si pensi alla regolamentazione vigente in materia di protezione dei dati, sicurezza informatica e antitrust, oltre al recente intervento normativo realizzato nel settore dell'Intelligenza Artificiale. Sul tema si rinvia a A. Grotto, M. Schallbruch, *The Great Anti-China Tech Alliance*, in "Foreign Policy", 16 September 2019.

[65]Secondo l'analisi di C. Hobbs, *op. cit.* Si veda anche F. Gueham, *Digital sovereignty - steps towards a new system of internet governance*, Fondation pour l'innovation politique, February 2017.

[66]Definita sulla base delle indicazioni formalizzate nel *Rapporto finale* del Working Group on Internet Governance, June 2005.

[67]L'IGF, convocato per la prima volta nel 2006 ad Atene, è giunto alla sua 16ma edizione che si è recentemente svolta a Katowice dal 6 al 10 dicembre 2021.

[68]Cfr. *Tunis Agenda for the Information Society*, cit., p. 73. Nel rispetto del mandato delineato dall'Agenda di Tunisi nel 2005, l'IGF è stato rinnovato per 5 anni nel 2010 (2011-2015) e nel 2015 per altri 10 anni (2016-2025): cfr. revisione WSIS + 10 attuata dalla Risoluzione ONU 68/198 del 20 dicembre 2013, tenuto conto delle modalità di attuazione dei risultati indicati in occasione del vertice mondiale sulla Società dell'Informazione di cui alla Risoluzione ONU 68/31 del 31 luglio 2014.

[69]Nel tentativo di realizzare un sistema più "statalista" di governance di Internet, è stata costituita nel 2001, da Cina, Kazakistan, Kirghizistan, Russia, Tagikistan e Uzbekistan, l'Organizzazione internazionale per la cooperazione di Shanghai, creata nel 2001 come modello alternativo di governo digitale, fondato sul diritto sovrano degli Stati nazionali, osteggiato dagli USA e dall'UE. Si veda S. McKune, *An Analysis of the International Code of Conduct for Information Security*, in "The Citizen Lab", 28 September 2015.

[70]Nel rispetto della metodologia applicativa indicata nel documento *A Toolkit to assist communities in establishing the IGF initiatives* che descrive i requisiti di base per realizzare un'iniziativa IGF in conformità ai principi fondamentali di inclusività, apertura, trasparenza e multi-partecipazione, al fine di facilitare lo scambio di idee e opinioni.

[71]Su tali problematiche L. Abba, *Carenze attuali e soluzioni future nei meccanismi per la cooperazione digitale*, in questa Rivista, 2021, n. 1, delinea le future prospettive dell'ecosistema digitale emerse in occasione della pubblicazione, da parte delle Nazioni Unite, della *Road map for digital cooperation* alla luce delle criticità riscontrate negli attuali meccanismi intergovernativi adottati a livello internazionale.

[72]I cd. "Colossi del Web" stanno dimostrando indiscutibili capacità imprenditoriali orientate alla massimizzazione del profitto in grado di realizzare un costante incremento del fatturato aziendale grazie all'implementazione di servizi e strumenti, in regime di strapotere tecnologico (resi ancor più indispensabili, nello svolgimento della maggior parte delle attività quotidiane, dalla situazione emergenziale della pandemia "Covid-19"). Al contempo, però, essi manifestano anche un'inclinazione "politica" che potrebbe entrare presto in rotta di

collisione con la visione "tecno-nazionalistica" – spesso conservativa e poco lungimirante – degli apparati statali nella ricerca di soluzioni regolatorie del cyberspazio. Non a caso, rispetto al tradizionale approccio *soft-law*, ricognitivo di un atteggiamento neutrale a lungo manifestato dai governi nei confronti delle grandi aziende digitali, cominciano ora ad intensificarsi le "tensioni" tra i contrapposti "players". Ad esempio, negli USA, contestualmente alle indagini antitrust avviate dalla Federal Trade Commission per limitare il potere monopolistico detenuto dalle "Big Tech" come necessaria misura correttiva proconcorrenziale in grado di stimolare l'innovazione nell'economia digitale, l'amministrazione Biden ha più volte annunciato l'avvio di un'organica riforma della Sezione 230 del "Communications Decency Act" del 1996 che, per favorire la libertà di innovazione a tutela dello spazio "autarchico" di Internet, garantisce agli intermediari telematici un esonero di responsabilità dalle conseguenze dannose, riconoscendo uno specifico "scudo legale" di immunità contro il rischio di pubblicazione di contenuti illeciti online immessi dagli utenti terzi. Nella stessa direzione si sta muovendo il governo in Cina, ove si registra un accentuato interventismo legislativo motivato dalla necessità di salvaguardare inderogabili esigenze di stabilità politica e di sicurezza nazionale nella gestione centralizzata dei dati e nel controllo del flusso comunicativo veicolato online. Pertanto, dopo un'iniziale fase di tendenziale libertà imprenditoriale generalmente riconosciuta in assenza di sostanziali restrizioni, come precisa scelta strategica di accelerazione espansionistica del proprio modello capitalistico, le autorità cinesi, in un mutato clima più ostile ai comportamenti anticoncorrenziali, hanno multato il gigante di Internet Alibaba per pratiche anticoncorrenziali in conseguenza della violazione della legge antimonopolio, contestualmente all'adozione di un provvedimento inibitorio volto alla revisione della governance delle controllate della holding societaria. Anche in Europa sono in corso riforme legislative dirette a contenere lo strapotere delle imprese "high-tech" in un'ottica di liberalizzazione dei mercati, come si evince dal "pacchetto" *Digital Services Act* e *Digital Markets Act*, al pari della Direttiva UE "Copyright" 2019/790, sino alla recente proposta di Regolamento europeo in materia di Intelligenza Artificiale, caratterizzata dalla medesima *ratio* applicativa. Sul tema, A. Alù, *Stati contro le big tech: siamo allo scontro finale? La linea dura di Ue, Usa e Cina*, cit.

[73]Pur nell'ottica di migliorare il processo decisionale dell'IGF, rendendolo più efficace e incidente nella formulazione delle proposte che emergono all'esito dei relativi lavori, l'istituzione di una sorta di "Leadership Panel", come organismo multistakeholder di "alto livello", è stata duramente contestata da alcune organizzazioni della società civile che, contrarie alla formazione di tale gruppo, hanno chiesto di boicottarne la relativa procedura di nomina, per evitare di alterare le originarie caratteristiche fondanti il *forum*, mediante la creazione di speciali categorie di attori differenziati per "status", al punto da compromettere la partecipazione "bottom-up" del *meeting*; cfr. M. Mueller, *Civil Society Groups Resist IGF "Leadership Panel"*, Internet Governance Project, 26 November 2021.

[74]Prendendo atto del declino degli attuali processi internazionali esistenti, di fronte alle sfide che la cooperazione geopolitica della Rete pone, il rapporto *The Open Internet on the Brink: Recommendations for a Future Model*, prospetta una possibile riforma della governance di Internet. A tal fine, si prevede la creazione di una sorta di "Nato per Internet", come vera e propria "Alleanza per le infrastrutture e la difesa digitale", con il compito di valutare e orientare lo stato di salute dell'ecosistema digitale, delineando un nuovo modello di "internazionalismo" su Internet, caratterizzato da un maggiore e più accentuato coinvolgimento politico dei governi nazionali in grado di contrapporsi alla visione "nazionalistica" della Rete frammentata sostenuta da alcuni Stati.

[75]Sul tema, J. Pohle, T. Thiel, *Digital sovereignty*, in "Internet Policy Review", vol. 9, 17 December 2020, n. 4.

[76]A. Grotto, M. Schallbruch, *op. cit.*

[77]Secondo l'autorevole analisi di C. Hobbs, *op. cit.* L'autore, in particolare, individua l'esistenza di una rete "Internet statunitense" di matrice imprenditoriale costituita dal complesso di regole stabilite dalle principali società che forniscono i servizi digitali utilizzati in tutto il mondo; una "Internet cinese", come rete di riferimento per i governi autoritari, controllata a livello nazionale da Pechino, funzionale al perseguimento degli interessi generali dello Stato mediante un sistema integrale di sorveglianza massiva; e una "Internet europea" dalla configurazione più spiccatamente democratica, orientata alla promozione proattiva della concorrenza nella regolamentazione dei mercati digitali e alla protezione dei diritti dei consumatori/utenti/fruitori dei servizi telematici.

[78]Cfr. J.P. Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, 8 February 1996.

[79]Cfr. A. Chander, *The Racist Algorithm?*, in "Michigan Law Review", vol. 115, 2017, n. 6; I. Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, in "Cardozo Law Review", vol. 41, 10 March 2016, n. 5.

[80]Sul tema sia consentito rinviare ad A. Alù, *Algoritmi che incitano all'odio? Così i video alterano le opinioni e amplificano la violenza*, in "Agendadigitale.eu", 6 maggio 2021.

[81]Si veda A. Alù, *Disinformazione social, Facebook distratta e i regimi se ne approfittano*, in "Agendadigitale.eu", 19 aprile 2021.

[82]Si rinvia all'analisi del rapporto *Splintered Speech - Digital Sovereignty and the Future of the Internet*, cit.

[83]H. Farrell, M. Levi, T. O'Reilly, *Mark Zuckerberg runs a nation-state, and he's the king*, in "Vox.com", 10 April 2018.

[84]Sul tema, E. Guo, *Facebook is now officially too powerful, says the US government*, in "MIT Technology Review", 9 December 2020.

[85]Si veda V.M. Schönberger, K. Cukier, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere. E già minaccia la nostra libertà*, Garzanti, 2013.

[86]Per un approfondimento R. Berman, Z. Katona, *Curation Algorithms and Filter Bubbles in Social Networks*, NET Institute Working Paper No. 16-08, 21 September 2019; E. Pariser, *Il Filtro. Quello che Internet ci nasconde*, Il Saggiatore, 2012.

[87]Emblematica, in tal senso, come peculiare manifestazione del nuovo prospettato sistema di governance, è la creazione, promossa da Facebook, di un'inedita struttura, denominata *Oversight Board*, presentata come una sorta di "Corte Suprema" (composta da 20 "giudici" - tra cui un ex Primo Ministro danese e un vincitore del Premio Nobel per la Pace – dotati di un *mix* diversificato di competenze specialistiche, con maggiore preminenza di cultura giuridica e istituzionale), molto simile al tradizionale modello dei tribunali. L'*Oversight Board* opera, infatti, come un organo giudicante indipendente, al quale gli utenti possono appellarsi in casi di controversie che riguardano la cancellazione di profili e post ritenuti ingiusti, per ottenere decisioni "definitive" e "vincolanti" sui contenuti consentiti e/o rimossi. Si tratta, pertanto, di un'iniziativa senza precedenti realizzata da un'impresa privata che sembra dotarsi di organi "para-giurisdizionali" sulla falsariga della tipica tripartizione dei poteri che caratterizza un ordinamento statale (cfr. A. Alù, *Oversight board di Facebook alla prima prova: così si disvela il suo ruolo*, in "Agendadigitale.eu", 1 febbraio 2021). Parimenti singolare risulta il progetto *Metaverso*, presentato in occasione dell'annuncio di Zuckerberg sulla ridenominazione della holding societaria, con l'obiettivo di realizzare una nuova versione di Internet, fondata sull'integrazione tra mondo fisico e digitale, come ambiente ibrido di interazioni reali

tra persone che – nella veste di "avatar" – lavorano, giocano, sviluppano relazioni interpersonali, incontrandosi secondo le dinamiche "normali" della vita quotidiana. Il sistema *Metaverso* sembra, invero, delimitare i confini virtuali di uno nuovo spazio "cyber-sovrano" popolato da quasi 3 miliardi di utenti sottoposti al rispetto delle regole prescritte dalla piattaforma che tende ad assumere le caratteristiche tipiche di uno "Stato digitale" (cfr. A. Alù, *Perché il Metaverso potrebbe (davvero) essere la nuova "internet revolution"*, in "Agendadigitale.eu", 2 novembre 2021).

* * *

Internet Governance beyond the States? The unprecedented traits of the future digital ecosystem

Abstract: The essay identifies the main questions that the future digital ecosystem poses, describing the phenomenon of Internet fragmentation as one of the most complex and problematic aspects that emerges in the current geopolitical scenery, where the tendency of States to elaborate "techno-nationalistic" aimed at the construction of an autonomous and independent network, technologically different from the original distributed and interoperable architecture on which the traditional operating model of the global Internet is based. In fact, various regulatory interventions proliferate in the global panorama that require the massive use of general surveillance tools to ensure centralized control of the Internet, as a strategic priority objective of technological supremacy established to protect the critical infrastructures of the States, to avoid the risk of possible external attacks capable of destabilizing the internal order. With respect to the progressive balkanization of the Internet, the economic and political power of the "Big Tech" in the guise of new dominant "players" is strengthening as an unexpected variable of the changed Internet ecosystem.

Keywords: Internet Governance – Internet fragmentation – Big-Tech – Splinternet – Digital sovereignty

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0076
Articolo sottoposto a peer review

Lo sviluppo sostenibile del patrimonio culturale tra emergenze e tecnologie digitali

Gloria Mancini Palamoni

Il saggio analizza come le nuove tecnologie e il governo di Internet impattano sul patrimonio culturale fortemente provato dagli eventi emergenziali. Il nostro Paese si è trovato ad affrontare crisi che hanno prodotto effetti negativi anche nella prospettiva delle funzioni di tutela, valorizzazione e gestione dei beni culturali e del paesaggio. La chiave di lettura ipotizzata come faro per l'equilibrio tra i molteplici interessi coinvolti potrebbe essere l'applicazione dello sviluppo sostenibile come principio-obiettivo trasversale anche nell'ottica delle misure da adottare in esecuzione del PNRR.

Patrimonio culturale – Sviluppo sostenibile – Governance di Internet – Nuove tecnologie

Sommario: *1. Lo sviluppo sostenibile come principio-obiettivo trasversale – 2. Tecnologie digitali e sostenibilità per i beni culturali e il paesaggio – 3. Il problema: il patrimonio culturale durante le emergenze – 4. Il patrimonio culturale nel PNRR tra sviluppo sostenibile e tecnologie digitali – 5. La valorizzazione delle tecnologie digitali per lo sviluppo sostenibile dei beni culturali e del paesaggio. Luci e ombre – 6. L'influenza del governo di Internet sugli aspetti sociali, giuridici ed economici dello sviluppo sostenibile del patrimonio culturale – 7. Una prospettiva: il principio dello sviluppo sostenibile alla guida della valorizzazione delle tecnologie digitali per il patrimonio culturale*

1. Lo sviluppo sostenibile come principio-obiettivo trasversale

Da tempo lo sviluppo sostenibile è presente in numerosi documenti, accordi internazionali e iniziative[1]. È codificato come principio all'art. 3, par. 3, TUE[2], all'art. 3-*quater* del d.lgs. 3 aprile 2006, n. 152[3] (che lo colloca tra i principi generali delle norme in materia ambientale facendogli ricoprire un ruolo di egemonia nell'ambito del governo dell'ambiente[4]) ed è ora esplicitamente menzionato nella Carta costituzionale[5]. Nel contempo, è un obiettivo al quale ogni Paese dovrebbe tendere[6].

Nato dal presupposto per cui, non essendo le risorse inesauribili, occorre far sì che esse soddisfino i bisogni dell'attuale generazione senza pregiudicare la capacità di quelle future di rispondere ai propri, tende, oggi, anche alla non compromissione della qualità della vita. In quest'ottica il concetto[7] mira a guidare un processo di cambiamento tale per cui lo sfruttamento delle risorse, la direzione degli investimenti, l'orientamento dello sviluppo tecnologico e i mutamenti istituzionali siano resi coerenti anche con i bisogni futuri[8], potendo essere ritenuto un principio-obiettivo trasversale a contenuto solidaristico.

Dal punto di vista ambientale in senso ampio, si caratterizza per il legame intergenerazionale che collega i popoli del passato a quelli presenti e futuri; nell'ottica economica e giuridica, guida (o almeno aspira a guidare) le scelte dei cittadini e dell'amministrazione. È in quest'ultima prospettiva che la sua natura

G. Mancini Palamoni è assegnista di ricerca in Diritto amministrativo presso l'Università di Camerino.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

di obiettivo emerge con maggiore vigore proiettandosi verso una dimensione amplissima di attuazione dell'interesse generale.

Nella veste di principio, con particolare riferimento al diritto interno, rappresenta uno dei paradigmi di legittimità degli atti amministrativi: in generale, di quelli intrisi di discrezionalità tale per cui nella scelta comparativa degli interessi quelli alla tutela dell'ambiente e del patrimonio culturale devono essere prioritariamente considerati; in particolare, di quanti vertono sulle risorse collettive, non illimitate, e sui beni comuni, diventando indicatore dell'azione amministrativa. Si pensi, ad es., agli strumenti della VIA[9], della VAS[10], dell'AIA[11] e della IPPC[12], alle norme in materia di governo del territorio[13] e di tutela, valorizzazione e gestione del patrimonio culturale[14] e di contratti pubblici[15], che rappresentano le massime espressioni concrete dello sviluppo sostenibile quale parametro dell'agire amministrativo e confermano la natura di principio orientatore universale oltre che di obiettivo da perseguire. Ogni attività amministrativa dovrebbe farsi carico della questione ambientale[16] come problema di interesse generale, posto che qualunque azione o omissione può costituire per esso una minaccia, un pericolo, un danno[17].

In rapporto ai beni culturali, la trasversalità del principio emerge nella connessione tra questi ed i beni paesaggistici. La l. 29 giugno 1939, n. 1497 (art. 1 nn. 3 e 4) comprende nelle "bellezze d'insieme" le cose immobili e le bellezze panoramiche; la l. 8 agosto 1985, n. 431 rende autonoma la disciplina del paesaggio da quella dei beni culturali[18]. Oggi, con l'ampliamento dell'oggetto della tutela, alla dimensione estetica si aggiunge quella geografica satura di elementi storici ed ambientali[19] e si discute dell'esistenza di un "diritto alla bellezza" che si caratterizza per la sua universalità e per la pretesa di diventare strumento per perseguire il benessere collettivo, migliorando la qualità della vita di tutti anche attraverso l'adeguamento ai mutamenti del contesto sociale[20].

Nel quadro appena delineato le tecnologie digitali e la loro valorizzazione rivestono un ruolo di primo piano e rendono opportuno interrogarsi sui limiti e le potenzialità offerte dall'ordinamento per la realizzazione di un patrimonio culturale 4.0[21] nel quale la sostenibilità rappresenta presupposto, strumento e fine dell'applicazione degli strumenti digitali. È proprio il carattere trasversale e interdisciplinare del principio a presentarlo come il più adeguato mezzo di raccordo del rapporto tra tutela e valorizzazione dei beni culturali e del paesaggio attraverso le tecnologie digitali anche – e forse soprattutto – durante le emergenze.

2. Tecnologie digitali e sostenibilità per i beni culturali e il paesaggio

Sebbene il principio dello sviluppo sostenibile nasca e si rafforzi, almeno fino ad un certo momento, identificandosi con l'ambiente, gli ecosistemi, la biosfera e il paesaggio, il binomio natura-beni culturali è indissolubile; permea l'intero Codice dei beni culturali e del paesaggio [d'ora in avanti anche "Codice"], è evidenziato nel Codice dell'ambiente e rappresenta il criterio di scelta dell'Unesco per l'individuazione dei siti da proteggere[22]. Basti pensare alle disposizioni aventi ad oggetto le misure di conservazione, inclusive della prevenzione intesa come limitazione delle «situazioni di rischio connesse al bene culturale nel suo contesto»[23]; a quelle di tutela che prescrivono determinate distanze o misure, oppure, ancora, alle norme dirette ad evitare che sia messa in pericolo l'integrità dei beni culturali immobili, che ne sia danneggiata la prospettiva o la luce o ne siano alterate le condizioni di ambiente e di decoro[24]. L'art. 112 del d.lgs. n. 42/2004, nell'ambito degli accordi di valorizzazione tra Stato, regioni ed enti pubblici, non tralascia il contesto territoriale e comprende tra gli obiettivi della funzione anche la cura di tutto quanto circonda il bene culturale[25]. Nell'ambito della cooperazione tra pubbliche amministrazioni per la conservazione e la valorizzazione del paesaggio le attività devono tenere conto delle esigenze della tutela, dovendo essere considerate anche le finalità di sviluppo (questa volta specificamente) territoriale sostenibile[26]; l'attività di pianificazione paesaggistica, per perseguire lo sviluppo sostenibile, deve orientare gli interventi di trasformazione del territorio[27].

Dal punto di vista dell'organizzazione, il rapporto è confermato anche dalla previsione della Direzione generale e della Soprintendenza Archeologia, belle arti e paesaggio[28], dalla quale «si evince un approccio al patrimonio storico, artistico, architettonico, etnoantropologico, paesaggistico e archeologico italiano, globale, integrato sul piano disciplinare, "territorialista" (nel senso di teso a cogliere nello studio come nella tutela la complessità del territorio)»[29].

Nel secondo caso (come criterio di scelta per l'inserimento nella lista dei siti da proteggere), l'integrazione tra beni culturali e paesaggio/natura è ben evidenziata nella Convenzione Unesco del 1972, mentre l'interdipendenza tra beni culturali e sviluppo sostenibile nella *Hangzhou Declaration* del 2013 (che sottolinea il valore strategico del recupero del patrimonio culturale e della ripresa delle attività culturali nelle aree colpite da violenti conflitti o da catastrofi naturali per consentire alle popolazioni di rinnovare la propria identità e di ritrovare una normalità)[30] e

nelle Conclusioni del Consiglio d'Europa del 21 maggio 2014. Il rapporto tra patrimonio culturale e paesaggio e ambiente si delinea come una relazione di reciprocità tale per cui la tutela dell'uno è funzionale a quella dell'altro[31], sebbene l'approccio integrato al patrimonio, nonostante in parte previsto[32], resti, di fatto, ancora limitato[33]. In questo complesso legame si aggiunge un terzo elemento, l'innovazione digitale, che sempre più profondamente investe il patrimonio culturale, influenzandolo, ad es., attraverso la fruizione virtuale dei beni culturali[34] ed il supporto nella ricostruzione dei beni distrutti[35].

L'Assemblea Generale dell'ONU, nel 2015, ha adottato sul tema la Risoluzione *Trasformare il nostro mondo: l'Agenda 2030 per lo Sviluppo Sostenibile*, definita programma di azione per le persone, il pianeta e la prosperità. Il documento, riprendendo parzialmente quanto già dichiarato nel *Rapporto Brundtland*, individua nella lotta alla povertà attraverso la sostenibilità e la resilienza lo scopo del viaggio collettivo in esso descritto. Gli obiettivi per lo sviluppo sostenibile sono diciassette, centosessantanove i traguardi annunciati.

Il paragrafo che inquadra il principio dello sviluppo sostenibile è intitolato *Pianeta*. Questo deve essere protetto dalla degradazione, attraverso un consumo ed una produzione consapevoli delle risorse naturali ed una loro gestione sostenibile, mediante l'adozione di misure urgenti riguardo il cambiamento climatico, così che possa soddisfare i bisogni delle generazioni presenti senza compromettere quelli delle generazioni future.

La Risoluzione è di assoluto interesse poiché dà contezza di come il principio-obiettivo calzi alla perfezione anche ai beni culturali, materiali e immateriali, al paesaggio e alla cultura in senso più ampio. Il paragrafo successivo, intitolato *Prosperità*, completa il quadro riferendosi al raggiungimento del godimento di vite prosperose e soddisfacenti per tutti gli esseri umani e ad un progresso economico, sociale e tecnologico in armonia con la natura.

Le finalità principali (settori strategici) sono quattro: educazione, economia, insediamenti umani e turismo. Il punto 4.7 tende a garantire entro il 2030 la conoscenza per la promozione dello sviluppo sostenibile (in senso ampio inteso) da parte di tutti i discenti, anche attraverso l'educazione ad uno stile di vita sostenibile, ai diritti umani, alla parità di genere, alla promozione di una cultura pacifica e non violenta, alla cittadinanza globale e alla valorizzazione delle diversità culturali. L'obiettivo 8.9 è particolarmente attuale in questo momento storico poiché rivolto ad implementare e favorire le politiche per il turismo sostenibile produttivo di lavoro e promotore della cultura e dei prodotti locali; l'11.4 tende, invece, a rendere le città e gli insediamenti umani inclusivi, sicuri, duraturi e sostenibili, attraverso il potenziamento degli sforzi per la salvaguardia del patrimonio culturale e naturale del mondo. L'obiettivo 12.b, infine, è diretto a garantire modelli sostenibili per quanto riguarda i consumi e si preoccupa di implementare gli strumenti per il monitoraggio degli impatti dello sviluppo per il turismo sostenibile. Tutte finalità per la cui realizzazione ricoprono un ruolo di assoluto rilievo le nuove tecnologie[36].

Il 23 settembre 2020 è stata approvata la ratifica della Convenzione di Faro, la città portoghese dove il 27 ottobre 2005 è stata stipulata, sul valore del patrimonio culturale per la società. La Convenzione definisce il patrimonio culturale «l'insieme di risorse ereditate dal passato che le popolazioni identificano, indipendentemente da chi ne detenga la proprietà, come riflesso ed espressione dei loro valori, credenze, conoscenze e tradizioni, in continua evoluzione», comprensivo di «tutti gli aspetti dell'ambiente che sono il risultato dell'interazione nel corso del tempo fra le popolazioni e i luoghi»; definisce, altresì, la "comunità di patrimonio" come «un insieme di persone che attribuisce valore ad aspetti specifici dell'eredità culturale, e che desidera, nel quadro di un'azione pubblica, sostenerli e trasmetterli alle generazioni future», attribuendole una responsabilità comune circa l'uso sostenibile.

In riferimento al paesaggio, la Convenzione chiede, all'art. 8, l'adozione di strategie di mitigazione dei danni e la promozione di un approccio integrato alle politiche per garantire un equilibrio tra le diversità culturale, biologica, geologica e paesaggistica.

Come per altri diritti la tutela del patrimonio culturale non può dirsi effettiva senza strumenti, risorse e misure, cioè senza l'agire dei pubblici poteri; perciò l'art. 10 chiede un aumento di consapevolezza e un maggiore utilizzo del potenziale economico del patrimonio culturale nell'elaborazione delle politiche.

La valorizzazione delle nuove tecnologie e di Internet per lo sviluppo sostenibile e la tutela dei beni culturali e del paesaggio diventa allora la chiave di lettura di questi obiettivi e trova stimolo negli intenti del PNRR.

3. Il problema: il patrimonio culturale durante le emergenze

Gli elementi appena descritti, oggi, non possono non fare i conti con le emergenze che hanno colpito il Paese. L'interdipendenza tra beni culturali, ambiente, paesaggio e tecnologie e l'interdisciplinarietà del-

lo sviluppo sostenibile spiccano durante i disastri: da un lato, la visione culturale è rafforzata e assume una vitalità unificatrice[37], dall'altro, si relativizza la loro permanenza[38] e diventa essenziale preservarne la memoria[39].

Osservando gli effetti prodotti da due recenti emergenze di diversa natura, la calamità naturale[40] e la pandemia[41], emerge come i differenti caratteri provochino conseguenze altrettanto diverse sul patrimonio culturale.

Da un lato, le calamità naturali (così come guerre[42] e attacchi terroristici) producono danni immediatamente tangibili e visibili: un terremoto distrugge chiese, palazzi e interi centri storici; il fango di un'alluvione travolge opere d'arte, danneggia edifici, altera il paesaggio, compromettendo prima la tutela (la "fisicità") e dopo la valorizzazione e la fruizione; diversi effetti, sebbene dannosissimi e apparentemente meno "fisici", produce l'emergenza sanitaria: le nefaste conseguenze sono meno visibili all'istante e incidono, all'inverso, prima sulla fruizione e la valorizzazione e dopo sulla tutela.

Il patrimonio culturale distrutto dall'emergenza sismica che nel 2016 ha colpito il centro Italia[43] non è ancora ripristinato e molte persone non possono fruirne[44]: dopo le ordinanze di protezione civile per la messa in sicurezza, le misure per la ricostruzione tardano[45] rendendo la risposta dell'amministrazione insoddisfacente. Diventa fondamentale una ricostruzione consapevole, affinché l'area del cratere divenga laboratorio di rinascita sostenibile ed esempio di buone pratiche, e indispensabile l'utilizzo delle nuove tecnologie. Il patrimonio compromesso non può perdersi: raffigura un insieme di tradizioni, costumi, abitudini, rapporti sociali, tutti testimonianze avente valore di civiltà. La ricostruzione culturale assume valenza sociale, dovendosi ricucire una rete di comunità. Lo sviluppo sostenibile è preponderante: il sisma distruggendo interi centri storici comporta per le generazioni future una perdita gravissima, ancor più dannosa qualora la ricostruzione non rispetti la culturalità dei luoghi.

In questo contesto l'obiettivo 11 dell'Agenda 2030 è essenziale. Il titolo *Rendere le città e gli insediamenti umani inclusivi, sicuri, resilienti e sostenibili* è l'efficace dimostrazione dell'importanza di una ricostruzione non solo rapida, ma sicura e sostenibile, a protezione del patrimonio culturale e naturale del mondo, che dia un senso, oltre che un'utilità. La ricostruzione post-sisma nell'ottica dello sviluppo sostenibile è fondamentale apparendo perfetta occasione di rispetto di detto principio sia dal lato dei beni culturali, come testimonianze aventi valore di civiltà, sia da quello del paesaggio, anche in riferimento al consumo di suolo[46] relativamente alla ricostruzione degli edifici di civile abitazione.

A livello organizzativo, segue questa direzione l'istituzione della Direzione generale per la Sicurezza del patrimonio culturale, articolata nel servizio emergenze e nel servizio ricostruzione. Offre una risposta organizzativa alle situazioni di rischio antropico e derivante da calamità naturali e incendi da attuare in collaborazione con il Comando dei carabinieri per la tutela del patrimonio culturale, con la Direzione generale Archeologia, Belle Arti e Paesaggio e con il Dipartimento per la protezione civile[47].

Anche la pandemia compromette il settore culturale: alla prima fase di chiusura totale di teatri, cinema e musei[48] (questi ultimi riaperti, nelle zone "gialle", solo dal gennaio 2021) ne è seguita un'altra[49], con la conseguenza che all'utenza è stata preclusa o limitata la fruizione e i gestori si sono visti diminuire l'indotto economico che tali attività, anche accessorie al bene culturale stesso, generano.

La normativa emergenziale restituisce la fotografia di un settore trascurato e ritenuto meno strategico di altri[50]; al controllo si è preferito un blocco generalizzato[51], un «lockdown della bellezza»[52], insomma. Tra l'altro indiscriminato, essendo posti sullo stesso piano (quindi, di pari potenziale rischio di contagio) un luogo chiuso e circoscritto come un cinema o un piccolo museo e un parco archeologico all'aperto; tutto questo nonostante la tutela, la fruizione e la valorizzazione del patrimonio culturale siano espressamente riconosciute attività rientranti tra i livelli essenziali delle prestazioni *ex* art. 117, co. 2, lett. m), Cost.[53] e l'apertura al pubblico regolamentata di musei e altri istituti e luoghi della cultura di cui all'art. 101, co. 3, del Codice dei beni culturali e del paesaggio, siano compresi tra i servizi pubblici essenziali[54].

Ripensare al patrimonio culturale mettendo al centro delle funzioni il principio dello sviluppo sostenibile aiuta ad orientare le scelte e ad adottare azioni consapevoli in un'ottica progettuale di lungo periodo. Le emergenze illuminano anche le criticità dell'ordinario aiutando a far sì che certi errori non si ripetano; ciò può accadere attualizzando un principio che vuole garantire a chi verrà dopo di noi le nostre stesse possibilità e i medesimi diritti, anche culturali.

Alla luce delle descritte considerazioni, è innegabile il ruolo di assoluto rilievo delle pubbliche amministrazioni in relazione alle misure da attuarsi nella prospettiva della sostenibilità e in ottemperanza ai contenuti dei programmi adottati proprio a ridosso dell'emergenza pandemica.

4. Il patrimonio culturale nel PNRR tra sviluppo sostenibile e tecnologie digitali

La valorizzazione del principio dello sviluppo sostenibile attraverso le tecnologie digitali diventa cruciale nel *Next Generation EU* (NGEU) e nel *Piano nazionale di ripresa e resilienza* (PNRR)[55] redatti all'indomani della crisi pandemica.

Il primo programma (NGEU) prevede investimenti e riforme tesi ad accelerare la transizione ecologica e digitale, migliorare la formazione delle lavoratrici e dei lavoratori e conseguire una maggiore equità di genere, territoriale e generazionale, anche modernizzando la pubblica amministrazione e rafforzando il sistema produttivo per intensificare il contrasto alla povertà, all'esclusione sociale e alle diseguaglianze[56]. Il secondo (PNRR), parte di un disegno più ampio, prevede una vasta ed ambiziosa strategia per l'ammodernamento dell'Italia che pone al centro proprio sviluppo e mobilità sostenibili, ambiente e clima, idrogeno, automotive e filiera della salute[57].

Entrambi i piani si inseriscono perfettamente nella cornice più estesa dell'Agenda 2030 poc'anzi richiamata e dei nuovi obiettivi europei, mirando ad un rinnovato modello di sviluppo italiano ed eurounitario[58] in cui l'innovazione tecnologica è chiave essenziale.

Il nesso tra patrimonio culturale, digitalizzazione e sviluppo sostenibile in contesti emergenziali è qui ben evidenziato. Si rappresenta l'Italia come un Paese fortemente vulnerabile agli eventi idrogeologici[59] e sismici e, nello stesso tempo, come territorio avente un patrimonio unico da proteggere composto da un «ecosistema naturale e culturale di valore inestimabile, che rappresenta un elemento distintivo dello sviluppo economico presente e futuro»[60] ove è fondamentale l'incremento di una cultura dell'ambiente che permei tutti i comportamenti della popolazione[61]. Sono previsti investimenti che coinvolgono l'ambito territoriale su più fronti: i siti culturali delle grandi aree metropolitane (mediante lo sfruttamento della partecipazione culturale come leva di inclusione e "rigenerazione" sociale); i piccoli centri e le aree rurali (al fine di favorire la nascita di nuove esperienze turistico-culturali, bilanciare i flussi turistici in modo sostenibile e sostenere la ripresa dello sviluppo e delle attività turistico-culturali nelle isole minori). Tutte azioni caratterizzate da una filosofia di sostenibilità ambientale e da interventi tesi a garantire una forte accelerazione alla digitalizzazione di questi settori: «le misure di ripristino e rinnovamento del patrimonio fisico culturale saranno accompagnate da un programma di digitalizzazione volto a virtualizzare, con approccio standard e ispirato alle migliori pratiche internazionali, il patrimonio culturale e turistico italiano»[62]. In questo modo, si garantirà un accesso universale alle opere d'arte anche abilitando iniziative di approfondimento e divulgazione innovative[63].

Gli interventi, in particolare, si dirigono verso quattro aree di azione determinate da un forte connubio tra sostenibilità, cultura in senso ampio, comprensiva del turismo come leva per la valorizzazione[64], e nuove tecnologie[65].

Sul tema, sempre nel PNRR, è emblematico il paragrafo intitolato *Patrimonio culturale per la prossima generazione*[66]. Ai fini della più ampia partecipazione, anche delle fasce giovani della popolazione, si prevedono sia interventi sul patrimonio "fisico", sia uno sforzo teso alla digitalizzazione di quanto custodito in musei, archivi, biblioteche e altri luoghi della cultura, così da consentire a cittadini e operatori del settore l'esplorazione di nuove forme di godimento del patrimonio culturale, oltre ad un più semplice ed efficace rapporto con la pubblica amministrazione. Ciò attraverso una infrastruttura digitale nazionale che raccolga, integri e conservi le risorse digitali aumentando la fruizione pubblica mediante piattaforme dedicate. Altri obiettivi riguardano la creazione di contenuti culturali nuovi e lo sviluppo di servizi digitali ad alto valore aggiunto da parte di imprese culturali e creative e di start-up innovative, tesi a stimolare un'economia basata sulla circolazione della conoscenza[67].

In questa prospettiva, si inseriscono anche gli investimenti diretti alla rimozione delle barriere architettoniche per l'incremento dell'accessibilità, quelli finalizzati a migliorare l'efficienza energetica nei cinema, nei teatri e nei musei, alla rigenerazione di piccoli siti culturali ricchi di patrimoni anche religiosi e rurali. Quest'ultimo obiettivo è diretta espressione del principio dello sviluppo sostenibile poiché mira ad evitare la polarizzazione di luoghi la cui fruizione sempre più intensa rischia di usurarli e impoverirli a scapito di percorsi e mete culturali meno battuti perché posti al di fuori dei flussi turistici ma di altrettanto valore artistico, culturale e naturalistico (borghi, architettura e paesaggio rurale, parchi e giardini storici).

Stesse finalità perseguono le misure di prevenzione sismica dedicate al ripristino del patrimonio culturale dopo un evento calamitoso, aventi, altresì, l'obiettivo di ridurre lo spreco di risorse economiche necessarie alla ricostruzione post-sisma e onde evitare che gli interventi effettuati in fase emergenziale producano un aggravamento dei danni ai beni stessi. L'investimento contempla la «realizzazione del Centro Funzionale Nazionale per la salvaguardia dei beni

culturali dal rischio di natura antropica e naturale (CEFURISC) consentendo un utilizzo più sinergico delle tecnologie esistenti e dei sistemi ambientali per il monitoraggio, la sorveglianza e la gestione dei luoghi culturali»[68].

5. La valorizzazione delle tecnologie digitali per lo sviluppo sostenibile dei beni culturali e del paesaggio. Luci e ombre

Nell'era della realtà aumentata, della *blockchain*, dell'intelligenza artificiale[69] e della digitalizzazione, le funzioni di tutela, valorizzazione e gestione del patrimonio culturale non possono sottrarsi alle influenze delle nuove tecnologie, piuttosto da qualche tempo ne supportano la gestione potenziandone la pubblicità[70].

Di messa in rete di contenuti culturali di elevata qualità per le diverse generazioni parla, nel 2011, Neelie Kroes, allora membro della Commissione europea e responsabile dell'Agenda digitale. Pochi anni dopo, il Mibact istituisce il TDLab, un laboratorio per il turismo digitale finalizzato a definire e favorire una strategia digitale per il turismo e, nel 2016, insieme al Mise e all'Agid, sottoscrive un protocollo di intesa per la creazione di nuovi servizi digitali per il turismo capaci di agevolare a cittadini e visitatori l'accesso al patrimonio artistico, culturale e naturale. Il *Piano strategico per la digitalizzazione del turismo italiano* prodotto dal TDLab, sebbene ancora attuale, non ha portato i risultati sperati, nonostante abbia evidenziato come «l'innovazione tecnologica [debba, n.d.r.] permeare anche settori fondamentali per il turismo italiano come quello dei beni culturali che purtroppo sconta un forte ritardo sui modelli di offerta e che si trova alle prese con diffusi ed urgenti problemi di conservazione e tutela del patrimonio» e sottolineato l'importanza di uno sviluppo che ponga al centro il paesaggio come elemento fondamentale e di un contenimento di fenomeni distorcenti quali il «consumo di suolo e l'abbandono progressivo dei territori rurali e montani che minano la sostenibilità futura del turismo»[71].

Nuove tecniche digitali (come la ricostruzione tridimensionale e il restauro virtuale bidimensionale, l'utilizzo di droni marini per la ricomposizione del paesaggio archeologico sommerso o le applicazioni per esperienze di realtà aumentata) sono utilizzate per la gestione, la conservazione, il recupero e la fruizione dei beni culturali[72] e la validazione temporale tramite *blockchain* applicata al mercato dell'arte è un meccanismo adoperato in alcune iniziative italiane e straniere[73].

Musei e aree archeologiche pubblicizzano sui propri siti Internet o attraverso le applicazioni per dispositivi mobili le collezioni permanenti offrendo una riproduzione della classica esposizione oppure descrivono mostre ed eventi temporanei a scopo promozionale; il tutto è reso accessibile (virtualmente) ad un pubblico sempre più vasto e situato anche a chilometri di distanza. Altri, sempre più numerosi, consentono di approfondire le informazioni su un luogo di interesse prima della visita oppure la supportano sostituendosi alle classiche audio-guide.

Dall'altro versante, la diagnostica per immagini permette l'esplorazione non invasiva di opere d'arte e il recepimento di informazioni fondamentali altrimenti non visibili (ad es. datazione dell'opera, stato di conservazione, eventuali interventi di restauro). I droni consentono di individuare le opere da recuperare nelle aree colpite da calamità naturali, gli archivi digitali di conservare e far consultare nel tempo opere pregiatissime, le immagini satellitari di analizzare i siti danneggiati o in pericolo. Nel complesso, l'IA soprattutto può dare un contributo concreto allo sviluppo sostenibile fornendo un supporto per analizzare gli impatti delle possibili strategie e suggerire soluzioni innovative[74].

Le luci appena messe in risalto si amplificano durante le emergenze: sebbene non si possa essere travolti dal contagio artistico[75] né posti nella situazione emotiva data dalla presenza fisica dell'opera d'arte o del monumento, in tempi di chiusure, i luoghi e le cose della cultura possono essere ammirati grazie alle numerose iniziative attuate da musei, gallerie e siti archeologici. Del tutto gratuitamente possono vedersi mostre ed esposizioni, conoscere le raccolte dei siti culturali situati dall'altra parte d'Italia o del mondo, osservare paesaggi e assistere a rappresentazioni teatrali. Anche pellicole inedite sono trasmesse sulle piattaforme digitali.

Recente è l'istituzione dell'Istituto centrale per la digitalizzazione del patrimonio culturale-*Digital library* ad opera del d.P.C.M. 2 dicembre 2019, n. 169 (art. 35) con lo scopo di curare il coordinamento e promuovere i programmi di digitalizzazione del patrimonio culturale di competenza ministeriale, valorizzando le potenzialità della trasformazione digitale anche per la tutela e la valorizzazione del patrimonio culturale e della sua memoria.

Come spesso accade, tuttavia, l'impianto normativo attuale sconta ancora il divario dovuto alla velocità delle nuove tecnologie e alle lentezze del diritto (ad es., i ritardi nel recepimento dei decreti previsti nel d.lgs. 18 maggio 2015, n. 102 e della direttiva UE in materia di diritto d'autore)[76].

Il secondo profilo da indagare concerne il paesaggio, la cui disciplina, sebbene contenuta nel d.lgs. 22 gennaio 2004, n. 42, è fortemente influenzata dalle fonti (specialmente pattizie) dell'UE[77].

Oltre alle azioni e agli investimenti messi a punto nel PNRR per la valorizzazione delle tecnologie digitali per lo sviluppo sostenibile, occorre riflettere sul paesaggio in un'ottica culturale[78] e di visione di insieme, mediante un approccio integrato al patrimonio. I valori identitari che in esso risiedono come dimensione di testimonianza avente valore di civiltà rappresentano un ponte intergenerazionale da tutelare e valorizzare a più livelli. Come evidenziato nel Codice, entrambe le funzioni concorrono a preservare la memoria della comunità nazionale e del suo territorio e a promuovere lo sviluppo della cultura (art. 1, co. 2) attraverso criteri direttivi di azione tesi al rispetto dei principi di «uso consapevole del territorio e di salvaguardia delle caratteristiche paesaggistiche e di realizzazione di nuovi valori paesaggistici integrati e coerenti, rispondenti a criteri di qualità e sostenibilità»[79] assicurando «la conservazione dei suoi aspetti e caratteri peculiari»[80].

Ciò accade attraverso una serie di strumenti messi a disposizione dal legislatore ai fini della salvaguardia e della conservazione ulteriori all'individuazione, quali la dichiarazione di pubblico interesse, l'autorizzazione paesaggistica, le attività di pianificazione e i provvedimenti di vincolo. Minore è (o almeno è stata fino ad un certo momento) l'attenzione nei confronti delle misure per la valorizzazione del paesaggio soprattutto da parte del legislatore statale[81] che le individua nell'aumento di pregio del bene e in quell'insieme di azioni strumentali alla migliore conoscenza e fruizione dello stesso.

Ai fini di queste riflessioni, assume assoluto interesse la Direttiva del Mibact del 16 dicembre 2015 tesa alla programmazione ed alla realizzazione di interventi per la valorizzazione di itinerari storico-culturali e paesaggistici pedonali (i c.d. cammini) percorribili a piedi o con forme di mobilità sostenibile caratterizzata dalla forte commistione di elementi ambientali, paesaggistici, agricoli, artigianali e, naturalmente, turistico-culturali.

Tra le luci, non mancano le ombre: se da un lato le tecnologie digitali consentono di migliorare le funzioni di tutela, valorizzazione e gestione, dall'altra, resta ferma l'esigenza di gestire i rischi collegati al loro utilizzo come quelli in materia di impatto ambientale (poiché per addestrare le reti neurali e gli algoritmi di *machine learning*, dal cui utilizzo dipendono molti dei successi attuali dell'IA, è necessaria una quantità rilevante di energia, spesso generata da combustibili fossili[82]) o la compromissione di alcuni diritti[83].

La tecnologia investe la disciplina del patrimonio culturale[84] in maniera così preponderante che diventa tanto complesso distinguere il bene immateriale dalla materialità[85] e porta a chiedersi se la stessa dematerializzazione potrebbe diventare oggetto di specifica tutela.

Quando si discute di aspetti tecnologici, infine, non si può prescindere dal collegamento con l'industria culturale e creativa, comprensiva della produzione di contenuti per la comunicazione e per l'informazione anche digitali, e alla sempre maggiore necessità di un diritto del patrimonio culturale digitale. Il PNRR diventa occasione ideale per la sua attuazione.

Sia le azioni di tutela sia quelle di valorizzazione abbracciano tecnologie digitali e sviluppo sostenibile sotto diversi profili. Anzi, le tecnologie digitali e la loro valorizzazione diventano efficace strumento di protezione. Da una parte, potenziano lo scambio interculturale e favoriscono la diffusione di conoscenze anche attraverso la rapidità di divulgazione di informazioni e notizie utili alla sensibilizzazione di politiche di tutela e all'educazione alla cultura, al paesaggio e alla sostenibilità e ne accrescono l'accessibilità; dall'altra, consentono di moltiplicare le occasioni di partecipazione alle attività di pianificazione ai sensi dell'art. 135 Codice. Attraverso la valorizzazione delle tecnologie digitali possono maggiormente attuarsi i principi di pubblicità e partecipazione di cui all'art. 144 Codice in un'ottica di facilitazione e di attuazione dello sviluppo sostenibile.

6. L'influenza del governo di Internet sugli aspetti sociali, giuridici ed economici dello sviluppo sostenibile del patrimonio culturale

Queste riflessioni si inseriscono nel più recente dibattito sul governo di Internet, che negli ultimi decenni fortemente influenza diritti e libertà giuridiche investendo ogni settore della vita di ciascuno[86], divenendo centrale anche nella prospettiva della capacità di gestione degli aspetti sociali, giuridici ed economici dello sviluppo sostenibile del patrimonio culturale. Le due questioni, innovazione tecnologica e sviluppo sostenibile della cultura, sono ormai intimamente connesse acquisendo un rilievo ulteriore alla luce delle recenti vicende emergenziali che puntano un faro sulle sfide della trasformazione digitale[87].

Le potenzialità dell'innovazione tecnologica sono molteplici (dall'accesso alle informazioni alla velocità di comunicazione, dall'Internet delle cose al lavoro da remoto, dalla possibilità di aggregazione di gruppi di persone che si trovano ai lati opposti del globo al

confronto tra scienziati), ma non ne scongiurano possibili usi scorretti ed effetti distopici nel caso di attuazioni improprie dei modelli applicativi. Tale contesto induce interventi di regolazione da parte dei governi attraverso l'introduzione di misure tese a preservare l'efficienza del sistema e, nel contempo, garantire la sicurezza dei cittadini[88], rendendo la realizzazione della governance di Internet, necessariamente multilivello e collaborativa, nello Stato democratico uno dei nodi da sciogliere[89].

Le tecnologie dell'informazione e della comunicazione producono effetti sociali, giuridici ed economici rilevanti. Abbattono le distanze geografiche grazie all'interazione sociale in spazi virtuali, influenzano i comportamenti, la formazione dell'opinione pubblica e la manifestazione del pensiero[90], ma anche le modalità di esercizio della sovranità degli Stati (specialmente nel caso di utilizzo di algoritmi predittivi[91], giungendo a mettere, talvolta, in crisi anche il concetto di Stato democratico[92]) e le decisioni amministrative[93]. Dal punto di vista economico, ricadono sui processi di globalizzazione[94] dando vita ad un mercato interdipendente incidente sulla riduzione dei costi degli scambi e sulla massimizzazione di domanda e offerta autonome. Dall'altra parte, il patrimonio culturale e le ambivalenze che da tempo si sono fatte strada nel rapporto tra uomo e tecnologia fanno emergere l'esigenza di individuare un punto di equilibrio capace di incidere e orientare l'organizzazione dei pubblici poteri nella prospettiva della innovazione tecnologica che sempre di più condiziona la quotidianità.

Appare allora fondamentale individuare il punto di equilibrio tra i plurimi interessi in gioco posto che la tecnologia influenza lo sviluppo sostenibile del patrimonio culturale da una molteplicità di profili. Oltre alle implicazioni giuridiche, lo sviluppo sostenibile del patrimonio culturale per il tramite delle tecnologie digitali assume una valenza anche sociale ed economica: è strumento indispensabile alla ricostruzione del patrimonio culturale distrutto e assume un ruolo preponderante nella doppia prospettiva della fruizione virtuale dei beni culturali e della interpretazione dell'all'art. 9 Cost. quale diritto di ciascuno a liberamente fruire della cultura[95] anche durante le emergenze. Prospettive che, pur riguardando aspetti anche sociali, riportano la questione sul piano giuridico: il patrimonio culturale si caratterizza per il suo essere testimonianza avente valore di civiltà, accezione che rappresenta il paradigma cui devono fare riferimento i pubblici poteri nell'esercizio di funzioni di tutela, valorizzazione e gestione il cui fine ultimo è quello di preservare la memoria culturale insita nel patrimonio stesso. Nonostante questo sia fisicamente distrutto, il suo valore culturale immanente permane (nell'immaterialità) e può tramandarsi grazie a strumenti digitali. In questo senso, occorre fare in modo che le tecnologie per lo sviluppo sostenibile, da un lato, pongano al centro non soltanto l'uomo come persona (affinché da utente-spettatore diventi cittadino), ma l'intero ecosistema; dall'altro, che si rendano in grado di stimolare sia lo sviluppo economico, sia il benessere ambientale e sociale contribuendo al progresso anche culturale della società.

7. Una prospettiva: il principio dello sviluppo sostenibile alla guida della valorizzazione delle tecnologie digitali per il patrimonio culturale

Oltre trent'anni fa, Giovanni Urbani parlava di "ecologia culturale" come approccio al restauro inteso quale protezione attraverso la messa in sicurezza dei beni da eventi calamitosi, sostenendo che «in un'epoca in cui l'uomo comincia ad avvertire la terribile novità storica dell'esaurimento del proprio ambiente di vita, i valori dell'arte del passato cominciano ad assumere la nuova dimensione di componenti ambientali antropiche, altrettanto necessarie, per il benessere della specie, dell'equilibrio ecologico tra le componenti ambientali naturali»[96].

La riflessione, sempre attuale, è il sintomo di come sia ancora oggi indispensabile ripensare ad un approccio integrato del patrimonio culturale e di come lo sviluppo sostenibile diventi imprescindibile principio da seguire prima e dopo le emergenze e in tutti i settori, sempre più accentuato dal diffondersi delle tecnologie digitali.

È fondamentale che divenga il parametro di ogni funzione legata ai beni culturali affinché ciascuno riconosca ad essi un ruolo strategico ed una prospettiva rinnovata, tra tradizione culturale materiale e immateriale, adattamento delle comunità ai disastri e diffusione di nuove tecnologie. Una visione che consenta di rispondere alla crescente domanda[97] di bellezza come sintesi di identità e memoria e, insieme, di benessere, quale pieno dispiegamento della formazione della persona e segno di inclusione. Le emergenze recentemente vissute, la pandemia specialmente, hanno fatto rilevare un bisogno più forte di natura[98], di arte e di cultura al quale l'ordinamento può rispondere solo attraverso l'attuazione dello sviluppo sostenibile e la valorizzazione delle tecnologie per un'ampia e sicura digitalizzazione. Quest'ultima sarà fondamentale per regolamentare gli accessi in determinati siti di interesse, per la ricostruzione di mo-

numenti e centri storici distrutti, per contingentare gli ingressi nei cinema e nei teatri etc.; l'uso delle tecnologie dovrà integrarsi allo sviluppo sostenibile in sede di pianificazione paesaggistica e quando dovranno autorizzarsi attività commerciali vicino a siti archeologici o storici e, ancora, quando mostre ed esposizioni d'opere d'arte sono diffuse su Internet.

Il pregio di cui il patrimonio culturale è intriso è unico e appartiene a tutti, e tutti devono poterne godere nonostante l'impianto normativo non sia ancora completo. L'ora della regolazione dei meccanismi attraverso i quali la realtà digitale si pone al servizio di quella materiale per la piena attuazione della funzione culturale di cui al rinnovato art. 9 Cost. tra arte, diritto, scienza e sviluppo sostenibile è prossima.

Note

[1]Ad es., tra i più recenti: Agenda 2030, Accordo di Parigi sui cambiamenti climatici, Rapporto ILO 2018, Strategia Europa 2020, Piano d'azione per l'economia circolare (2015). Già la Convenzione de L'Aja (1954) utilizza l'espressione *cultural heritage* per indicare un interesse superiore e universale alla tutela della cultura globale nella sua dimensione intergenerazionale e, come tale, da tramandare alle generazioni future.

[2]È il mercato interno a doversi adoperare per lo sviluppo sostenibile dell'Europa, «basato su una crescita economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente».

[3]Secondo cui ogni attività umana giuridicamente rilevante ai sensi del Codice deve conformarsi ad esso al fine di garantire che il soddisfacimento dei bisogni delle generazioni attuali non comprometta la qualità della vita e le possibilità delle generazioni future.

[4]Il tema, da sempre approfondito, negli ultimi anni è diventato protagonista di numerosi studi. *Ex multis*: M. Antonioli, *Sviluppo Sostenibile e giudice amministrativo tra tutela ambientale e governo del territorio*, in "Rivista italiana di diritto pubblico comunitario", 2019, n. 2, pp. 201-225; B. Tonoletti, *I cambiamenti climatici come problema di diritto pubblico universale*, in "Rivista giuridica dell'ambiente", 2021, n. 1, pp. 37-51; R. Ferrara, *Etica, ambiente e diritto: il punto di vista del giurista*, in R. Ferrara, M.A. Sandulli (a cura di), "Trattato di diritto dell'ambiente", Giuffrè, 2014, p. 19 ss.; M. Renna, *I principi in materia di tutela dell'ambiente*, in "Rivista quadrimestrale di diritto dell'ambiente", 2012, n. 1-2, p. 73 ss.; F. Salvia, *Ambiente e sviluppo sostenibile*, in "Rivista giuridica dell'ambiente", 1998, n. 2, pp. 235-244; E. Tiezzi, N. Marchettini, *Che cos'è lo sviluppo sostenibile? Le basi scientifiche della sostenibilità e i guasti del pensiero unico*, Donzelli, 1999; G. Rossi (a cura di), *Diritto dell'ambiente*, Giappichelli, 2008, spec. p. 41; F. Fracchia, *Lo sviluppo sostenibile. La voce flebile dell'altro tra protezione dell'ambiente e tutela della specie umana*, Editoriale Scientifica, 2010; Id., *Principi di diritto ambientale e sviluppo sostenibile*, in P. Dell'Anno, E. Picozza (diretto da), "Trattato di diritto dell'ambiente", CEDAM, 2012, p. 592 ss.

[5]Art. 9, co. 3, primo periodo, Cost.

[6]Gli obiettivi di sviluppo sostenibile devono essere realizzati entro il 2030 a livello globale da tutti i Paesi membri dell'ONU secondo quanto disposto dall'Agenda 2030 per lo sviluppo sostenibile. Su questi temi M. Cocconi, *La traiettoria della Circular Economy nel quadro del Green New Deal europeo*, in "Orizzonti del diritto pubblico", 14 maggio 2021.

[7]L'utilizzo del termine "concetto" riferito allo sviluppo sostenibile ha lo scopo di liberarlo da orpelli che possano troppo imbrigliarlo in un'idea strettamente legata al mondo giuridico (proprio in ottica di interdisciplinarietà) e vuole tendere a renderlo quanto più "neutro".

[8]World Commission on Environment and Development, *Our Common Future. World Commission on Environment and development*, Oxford University Press, 1987 (trad. it. *Il Futuro di noi tutti: rapporto della Commissione mondiale per l'ambiente e lo sviluppo*), Bompiani, 1988 (c.d. *Rapporto Brundtland*) definisce lo sviluppo sostenibile come «lo sviluppo che soddisfi i bisogni del presente senza compromettere la capacità delle generazioni future di soddisfare i propri».

[9]Recentemente, sul tema, D. D'Alessandro, *La procedura di V.I.A.: alla ricerca della qualificazione delle prerogative partecipative*, in "Il diritto dell'economia", 2021, n. 2, pp. 149-201 alla cui bibliografia sia consentito il rinvio.

[10]Su VIA e VAS nell'ottica dello sviluppo sostenibile F. Fracchia, F. Mattassoglio, *Lo sviluppo sostenibile alla prova: la disciplina di Via e Vas alla luce del d.lgs. 152/2006*, in "Rivista trimestrale di diritto pubblico", 2008, n. 1, pp. 121-158.

[11]Recentemente V. Di Capua, *Ambiente, complessità sistemica e semplificazione*, in "Diritto amministrativo", 2020, n. 4, pp. 965-981.

[12]Artt. 4 ss. d.lgs. 3 aprile 2006, n. 152.

[13]TAR Toscana, I, n. 567/2015 e, sulla scia, TAR Emilia-Romagna, II, Bologna, n. 790/2017 e n. 233/2018. Direttiva 2001/42/CE del 27 giugno 2001; Consiglio d'Europa, *Council of Europe Framework Convention on the Value of Cultural Heritage for Society* (Convenzione di Faro), 27 ottobre 2005.

[14]Artt. 115 (gestione dei beni culturali) e 131, 133 e 143 (su tutela e valorizzazione del paesaggio) d.lgs. 22 gennaio 2004, n. 42.

[15]Artt. 3, 30, 34, 68, 95 e 96 del d.lgs. 18 aprile 2016, n. 50.

[16]Le operazioni definitorie sono sempre giuridicamente complesse. Definire i concetti di ambiente, paesaggio e territorio, in ragione dei molteplici punti di sovrapposizione tutti oggetto di regolamentazione giuridica, è ancor più difficoltoso, così come lo è differenziare gli interessi coinvolti in materie che da ben definite risultano oggi dai contorni sfumati e difficilmente delimitabili. Ecco perché in questo contesto, anche in ragione della interdisciplinarietà delle questioni sottese, si preferisce usare il termine più generale "ambiente" come contenitore vastissimo nel quale inserire l'attuazione del principio in esame.

[17]M. Renna, op. cit., p. 73.

[18]In argomento P. Chirulli, *Urbanistica e interessi differenziati: dalle tutele parallele alla pianificazione integrata*, in "Diritto amministrativo", 2015, n. 1, pp. 51-120.

[19]Sul punto, C. cost., 7 novembre 2007, n. 367; Cons. St., VI, 27 luglio 2015, n. 3669. Basta, tra l'altro, pensare ai siti Unesco che, da una parte, appaiono come porzioni di paesaggio da proteggere da azioni di modificazione territoriale, dall'altra, rappresentano beni culturali alla cui tutela e gestione occorre provvedere con strumenti specifici (cfr. l. 20 febbraio 2006, n. 77).

[20]M.A. Cabiddu, *Diritto dei beni culturali e del paesaggio*, Giappichelli, 2021, pp. 2-3. Id., *Bellezza. Per un sistema nazionale*, Doppiavoce, 2021.

[21]L'espressione richiama quella, forse più nota, di "Industria 4.0". Sul tema (anche per una ricostruzione del panorama legislativo) recentemente F. Costantino, *Impresa pubblica e amministrazione: da Industria 4.0 al decreto semplificazioni*,

in "Diritto amministrativo", 2020, n. 4, pp. 877-902; D.U. Galetta, J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in "Federalismi.it", 2019, n. 3.

[22]Si pensi a siti come Venezia o Matera, nei quali le interazioni tra beni culturali e ambiente è fortissimo. V. il d.l. 20 luglio 2021, n. 103 (che conferisce alle vie d'acqua dignità legislativa qualificandole beni culturali, in una strettissima connessione tra paesaggio e bene culturale), spec. artt. 1 e 2, che dà conto «della proposta del Comitato del patrimonio mondiale UNESCO di inserire "Venezia e la sua laguna" nella lista dei siti in pericolo». Su questo tema, recentemente L. Casini, *La salvaguardia di Venezia "città acquatica": dall'utopia alla realtà*, in "Aedon", 2021, n. 2.

[23]Art. 29, co. 2.

[24]Spec. artt. 45, co. 1, e 145.

[25]Sul tema S. Gardini, *La valorizzazione integrata dei beni culturali*, in "Rivista trimestrale di diritto pubblico", 2016, n. 2, pp. 403-425.

[26]Art. 133.

[27]Art. 143, co. 1, lett. h) e (riferito allo sviluppo economico) art. 145.

[28]La cui attuale struttura è disciplinata dal d.P.C.M. 2 dicembre 2019, n. 169.

[29]G. Sciullo, *Il completamento della riforma organizzativa del Mibact. Direzione generale "unica" e soprintendenze "uniche"*, in "Aedon", 2016, n. 1.

[30]Adottata in occasione del Congresso Internazionale su *La cultura: chiave dello sviluppo sostenibile*.

[31]P. Capriotti, *Per un approccio integrato al patrimonio culturale*, in "Aedon", 2017, n. 1.

[32]Seppure senza un diretto richiamo all'ambiente, è il d.lgs. n. 42/2004 a definire il patrimonio culturale come l'insieme dei valori culturali e paesaggistici anche se già la legge Galasso (1985) aveva anticipato un'integrazione tra i due.

[33]V. Azzarita, *Quanto conta il patrimonio culturale per l'Europa?*, in "Il Giornale delle Fondazioni", 14 dicembre 2016.

[34]V. Ministero per i beni e le attività culturali, *Piano triennale per la digitalizzazione e l'innovazione dei musei* 2019-2021.

[35]V. l'attività svolta da *Iconem*.

[36]Oltre a titolare un paragrafo dell'*Agenda 2030*, la parola, variamente declinata, è ripetuta almeno una cinquantina di volte.

[37]È quanto accaduto dopo il sisma de L'Aquila del 2009 che ha fatto registrare una ripresa del dialetto poiché in ragione della mancanza di beni oggettuali della comunità a seguito dei crolli ci si è «aggrappati al bene "inoggettuale" per eccellenza»: F. Avolio, *Osservazione sull'«Alfabeto Aquiliano»*, in L. Klautke, M. Föcking, S.A. Sanna et al. (eds.), "Italienisch. Zeitschrift für italienische Sprache und Literatur", vol. 37, 2015, n. 2, p. 50.

[38]Il riferimento alla permanenza si intende sotto due punti di vista, entrambi concreti: durante e dopo emergenze causate da calamità naturali si è impossibilitati ad accedere e godere di taluni beni culturali a causa di crolli o altre circostanze che rendono inagibile l'accesso ai luoghi; nel corso dell'emergenza pandemica, per limitare i contagi, gli ingressi ai luoghi della cultura sono stati interdetti o molto limitati.

[39]Recentemente M.F. Cataldo, *Preservare la memoria culturale: il ruolo della tecnologia*, in "Aedon", 2020, n. 2.

[40]La normazione emergenziale nel nostro Paese è tradizionalmente e principalmente rappresentata dalle leggi tese a regolamentare gli interventi e le misure da attuare per fronteggiare e superare le calamità naturali: da ultimo, il d.lgs. 2 gennaio 2018, n. 1.

[41]L'emergenza sanitaria è stata in più occasioni definita in parte inaspettata non solo nel "quando", come per ogni emergenza (si pensi alle calamità naturali che, in ragione delle caratteristiche territoriali del Paese, sono invece fenomeni piuttosto ricorrenti), ma anche nell'"an": L. Poma, *Governo Conte e Coronavirus. Analisi sulle frequenze della paura*, in "formiche.net", 25 marzo 2020. Ciò nonostante vi sia chi l'ha ritenuta un evento non imprevedibile: N.N. Taleb, *Dal coronavirus una scossa al sistema, ma questo non è il mio Cigno Nero*, in "la Repubblica", 4 marzo 2020.

[42]Con riferimento all'aggressione della Russia all'Ucraina si parla di "catastrofe culturale": R. Capozucca, *Guerra in Ucraina è catastrofe culturale*, in "il Sole 24 ore", 5 marzo 2022.

[43]Quella che la protezione civile ha definito la sequenza sismica di Amatrice, Norcia, Visso.

[44]Dopo il sisma, alla data del 5 novembre 2021, sono ventiduemila gli edifici censiti come inagibili e per i quali non è stata ancora presentata né la richiesta di contributo, né la prenotazione come comunicato dalla struttura del Commissario straordinario Giovanni Legnini e riportato da Ansa.it nella sezione *sisma&ricostruzione*.

[45]Dopo il d.l. 17 ottobre 2016, n. 189 e ss.mm.ii. (spec. art. 17), sono le ordinanze del Commissario straordinario per la ricostruzione n. 38 del 2017 ad approvare il piano di interventi sul patrimonio artistico e culturale anche tutelato dal Codice e la n. 84 del 2 agosto 2019.

[46]Sul tema, recentemente, W. Gasparri, *Consumo di suolo e sviluppo sostenibile nella destinazione agricola dei suoli*, in "Diritto pubblico", 2020, n. 2, pp. 421-466.

[47]Art. 17, d.P.C.M. n. 169/2019.

[48]d.P.C.M. 4 marzo 2020, d.P.C.M. 8 marzo 2020, d.P.C.M. 9 marzo 2020. In argomento: A. Ciervo, *La chiusura dei musei e degli altri istituti e luoghi di cultura pubblici durante l'emergenza sanitaria*, in "Aedon", 2020, n. 2; R. Capozucca, M. Pirrelli, *La cultura chiusa ai tempi del coronavirus*, in "il Sole 24 ore", 25 febbraio 2020.

[49]d.P.C.M. 24 ottobre 2020.

[50]In argomento TAR Lazio, ord., 14 gennaio 2021, n. 192, che peraltro ha respinto le doglianze del ricorrente ritenendo «non manifestamente irragionevole, nell'ambito e nei limiti del sindacato consentito al giudice amministrativo, la decisione dell'Autorità di comprimere per un periodo di tempo circoscritto ... la fruizione dei musei e degli altri luoghi di cultura, in ragione della particolare gravità della emergenza sanitaria in atto», ritenendo «prevalente l'esigenza sottostante all'adozione delle misure impugnate di tutelare il diritto alla salute, a seguito della recrudescenza del contagio epidemiologico, attraverso una significativa riduzione delle attività da svolgersi in presenza».

[51]V., ad es., il d.l. 23 febbraio 2020, n. 6, conv. dalla l. 5 marzo 2020, n. 13; d.l. 25 marzo 2020, n. 19, conv. dalla l. 22 maggio 2020, n. 35; d.l. n. 33 del 16 maggio 2020, conv. dalla l. 14 luglio 2020, n. 74; d.P.C.M. 3 novembre 2020.

[52]L'espressione è di P. Maci, *Il lockdown della bellezza il patrimonio culturale italiano e la pandemia. La chiusura dei musei e degli altri istituti e luoghi della cultura tra diritto alla fruizione e tutela della salute*, in "Ambientediritto.it", 2021, n. 4.

[53]Art. 1 d.l. 20 settembre 2015, n. 146.

[54]Art. 1, co. 2, lett. a), ult. periodo, l. 12 giugno 1990, n. 146 introdotto dall'art. 1 del d.l. n. 146/2015. Sul punto G. Piperata, *Sciopero e musei: una prima lettura del d.l. n. 146/2015*, in "Aedon", 2015, n. 3. Sul tema, anche: C. Zoli, *La fruizione dei beni culturali quale servizio pubblico essenziale: il decreto legge 20 settembre 2015, n. 146 in tema di sciopero*, *ivi*, e L. Casini, *L'essenziale è (in)visibile agli occhi: patrimonio culturale e riforme*, *ivi*; G. Biasutti, *Brevi note intorno alla nozione di servizio pubblico culturale. Nomina sunt consequentia rerum?*, in "Aedon", 2021, n. 3.

[55]Il PNRR è stato approvato dal Governo nell'aprile 2021 e il 30 aprile 2021 è stato inviato alla Commissione europea. Detti piani fanno parte di una procedura prevista dal Regolamento UE 2021/241 attraverso cui gli Stati membri ricevono i finanziamenti del *Next Generation EU* per l'attuazione di percorsi di riforma.

[56]Evidenziano il divario esistente anche dal punto di vista della distanza culturale M. Maltagliati, N. Bellanca, *I divari territoriali in Italia. Una misura becattiniana dello sviluppo locale*, in "Stato e mercato", 2020, n. 3, p. 461. Su questi temi A. Giusti, *La rigenerazione urbana tra consolidamento dei paradigmi e nuove contingenze*, in "Diritto amministrativo", 2021, n. 2, pp. 439-473.

[57]In argomento, Convegno *Le riforme orizzontali previste nel PNRR*, in "Orizzonti del diritto pubblico", 16 giugno 2021.

[58]Modello che «intende intervenire per ridurre le emissioni inquinanti, prevenire e contrastare il dissesto del territorio, minimizzare l'impatto delle attività produttive sull'ambiente» per il miglioramento della «qualità della vita e la sicurezza ambientale, oltre che per lasciare un Paese più verde e una economia più sostenibile alle generazioni future» (PNRR, cit., p. 14).

[59]Anche in relazione a questi eventi, la normazione si dimostra di carattere post-emergenziale: eccetto il r.d. 30 dicembre 1923, n. 3267, incentrato sul vincolo idrogeologico, la normazione in tema di gestione dei boschi e la sistemazione idraulico-forestale dei bacini montani, fino alla fine degli anni '80, si è trovata in forte ritardo nella promulgazione di norme che imponessero alle istituzioni di considerare i fenomeni di origine naturale (come frane e alluvioni) nella pianificazione territoriale e urbanistica e, in linea generale, si è trattato di una normativa post-emergenziale e tampone.

[60]PNRR, cit., p. 20.

[61]*Ivi*, p. 21.

[62]Il binomio cultura-turismo è da sempre fortissimo e, anzi, il patrimonio culturale dev'essere inteso come suo fulcro. Si segnala, sul punto, il cambio di denominazione dell'organo di vertice da MiBACT (Ministero dei beni culturali e del Turismo) a MiC (Ministero della Cultura). Sulla riorganizzazione ministeriale anche in rapporto all'attuazione del PNRR: L. Casini, *Il ministero della Cultura di fronte al PNRR*, in "Aedon", 2021, n. 2.

[63]PNRR, cit., p. 109: con le misure previste dal Piano si vuole infatti impostare una strategia di sostegno e rilancio dei settori della cultura e del turismo, focalizzata sulla rigenerazione del patrimonio culturale e turistico, sulla valorizzazione degli asset e delle competenze distintive nonché sulla digitalizzazione attraverso il miglioramento della capacità attrattiva, dell'accessibilità e della sicurezza.

[64]L'idea del turismo come leva alla valorizzazione del patrimonio culturale è un modello già ampiamente diffuso: A. Papa, *Il turismo culturale in Italia: multilevel governance e promozione dell'identità culturale locale*, in "Federalismi.it", 2007, n. 4; G. Bottino, *Turismo e beni culturali*, in A. Cicchetti, M. Gola, A. Zito, "Amministrazione pubblica e mercato del turismo", Maggioli, 2012, p. 200; A. Sau, *Turismo culturale: alcune considerazioni a margine delle nuove competenze del Mibact*, in "Federalismi.it", 2014, n. 21; Id., *Le frontiere del turismo culturale*, in "Aedon", 2020, n. 1; S. Sergio, *La valorizzazione dei beni culturali mediante il turismo*, in "Federalismi.it", 2018, n. 6. Il PNRR dedica ad esso ampio spazio, specialmente sotto il profilo del "turismo digitale" (p. 111 ss.).

[65]Le quattro aree di azione individuate sono: *Patrimonio culturale per la prossima generazione*, *Rigenerazione di piccoli siti culturali, patrimonio culturale religioso e rurale*, *Industria culturale e creativa 4.0* e *Turismo 4.0*.

[66]PNRR, M1C3.1, cit., p. 110.

[67]*Ivi*, Investimento 1.1, p. 110.

[68]*Ivi*, pp. 107-113, spec. p. 113.

[69]Di grande interesse sul tema S. Ferilli, E. Girardi, C. Musto et al., *L'intelligenza artificiale per lo sviluppo sostenibile*, marzo 2022, che basa la strategia italiana dell'IA per lo sviluppo sostenibile su «azioni relative alla protezione ambientale e alle infrastrutture sostenibili» (p. 156).

[70]M.S. Giannini, *I beni culturali*, in "Rivista trimestrale di diritto pubblico", 1976, n. 1, p. 5 ss., ove evidenzia come il bene culturale è pubblico non per appartenenza ma in quanto bene di fruizione. Su questi temi v. il dibattito di cui la Rivista *Aedon* dà contezza nella sezione "Sulla digitalizzazione del patrimonio culturale" contenuta nel fascicolo 1, 2021. Sul rapporto tra i fenomeni tecnologici e la materia culturale, con particolare riguardo alla circolazione, recentemente: E. Bufano, Blockchain *e mercato delle opere di interesse artistico: piattaforme, nuovi beni e vecchie regole*, in "Aedon", 2021, n. 2; M. Sterpi, *L'impatto delle nuove tecnologie sulla creazione, distribuzione e vendita delle opere d'arte*, in G. Liberati Buccianti (a cura di), "L'opera d'arte nel mercato. Principî e regole", Giappichelli, 2019, p. 214 ss.; A. Lazzaro, *Innovazione tecnologica e patrimonio culturale tra diffusione della cultura e regolamentazione*, in "Federalismi.it", 2017, n. 24.

[71]TDLab, *Piano strategico per la digitalizzazione del turismo italiano*, Roma, 16 ottobre 2014, pp. 6-7.

[72]Tra l'altro gli «esperti di diagnostica e di scienze e tecnologia applicate ai beni culturali» sono tra i professionisti competenti ad eseguire interventi sui beni culturali ai sensi dell'art. 9-bis del d.lgs. n. 42/2004.

[73]Ad es.: *Art.Certo*, *Artcollective*, *Verisart*, *Codex*, *Blockchain Art Collective* e altri strumenti di ausilio a garanzia dell'attribuzione dell'opera (autenticità).

[74]S. Ferilli, E. Girardi, C. Musto et al., *op. cit.*

[75]M. Ainis, M. Fiorillo, *L'ordinamento della cultura*, Giuffrè, 2015, p. 3 ss.

[76]C. Barbati, M. Cammelli, L. Casini et al., *Diritto del patrimonio culturale*, il Mulino, 2020, p. 221.

[77]Tra le molte, la *Convenzione europea del paesaggio* (Firenze, 2000) ratificata con la l. 9 gennaio 2006, n. 14 ed espressamente richiamata all'art. 132, co. 2, Codice e la *Convenzione di Parigi* del 1972.

[78]G. Volpe, *Un patrimonio italiano. Beni culturali, paesaggio e cittadini*, UTET, 2016.

[79]Art. 131, co. 6.

[80]Art. 131, co. 4.

[81]L. Casini, *Ereditare il futuro*, il Mulino, 2016, p. 141 ss.

[82] S. Ferilli, E. Girardi, C. Musto et al., *op. cit.*, p. 57.

[83]Si pensi all'universalità di Internet come diritto, oramai urgente. Già S. Rodotà, *Una Costituzione per Internet?*, in "Politica del diritto", 2010, n. 3, pp. 337-351; A. Simoncini, *Il diritto alla tecnologia e le nuove diseguaglianze*, in F.S. Marini, G. Scaccia (a cura di), "Emergenza Covid-19 e ordinamento costituzionale", Giappichelli, 2020, p. 191 ss.

[84]Non soltanto quella legata alla liberalizzazione delle riproduzioni fotografiche dei beni culturali pubblici *ex* art. 108, co. 3, Codice.

[85]G. Morbidelli, A. Bartolini, *L'immateriale economico nei beni culturali*, Giappichelli, 2016.

[86]La dottrina ha più volte affrontato il tema evidenziandone le molteplici criticità: su tutti S. Rodotà, *Il mondo nella rete: quali diritti, quali vincoli*, Bari, 2014; S. Rodotà, A. Masera, G. Scorza, *Internet, i nostri diritti*, Bari, 2016. Da ultimo, G. Scorza, *In principio era Internet e lo immaginavamo diverso*, in questa Rivista, 2022, n. 1.

[87]La pandemia ha evidenziato come per la maggior parte della popolazione mondiale che ha accesso alla rete essa abbia un ruolo essenziale e sia stata uno strumento benefico.

[88]Cfr. V.G. Cerf, *On Internet Governance*, in questa Rivista, 2022, n. 1.

[89]V. le proposte in materia di "Cooperazione digitale" del Segretario generale delle Nazioni Unite ed il capitolo quinto di S. Ferilli, E. Girardi, C. Musto et al., *op. cit.*.

[90]A. Nicita, *Libertà d'espressione e pluralismo 2.0: i nuovi dilemmi*, in "MediaLaws", 10 marzo 2019.

[91]A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal", 2019, n. 1.

[92]L. Casini, *Lo Stato nell'era di "Google"*, in "Rivista trimestrale di diritto pubblico", 2019, n. 4, pp. 1111-1148.

[93]G. Avanzini, *Decisioni amministrative e algoritmi informatici*, Editoriale Scientifica, 2019.

[94]R. Baldwin, *La grande convergenza. Tecnologia informatica, web e nuova globalizzazione*, il Mulino, 2018.

[95]R. Cavallo Perin, *Il diritto al bene culturale*, in "Diritto amministrativo", 2016, n. 4, pp. 495-510.

[96]G. Urbani, *La scienza e l'arte della conservazione dei beni culturali*, in B. Zanardi (a cura di), "Intorno al restauro", Milano, 2000, p. 46.

[97]La crescente domanda di cultura, contrapposta all'avanzare delle forze distruttive dell'ambiente, era stata già evidenziata da M.S. Giannini, *Uomini, leggi e beni culturali*, ora in Id., *Scritti*, VI, Giuffrè, 2005, p. 285. Id., *Difesa dell'ambiente e del patrimonio naturale e culturale*, *ivi*, p. 249: «l'uomo, in ogni momento, crea, modifica, distrugge il proprio ambiente, il proprio patrimonio culturale, il proprio patrimonio naturale: la sua opera è continua creazione così come è continua distruzione».

[98]Si pensi al progetto *Seeing Stars* a Franeker nato dalla collaborazione tra i residenti, il governo e le imprese, Unesco Olanda e Studio Roosegaarde.

* * *

Sustainable development of the cultural heritage between emergencies and digital technologies

Abstract: This paper evaluates the impact of the new technologies and Internet governance on the cultural heritage, which has been strongly stressed by disastrous events. Our country has faced emergency crisis which negatively affected the functions of protection, enhancement and management of cultural heritage and landscape. Sustainable development could represent the balancing element among the several involved interests. It could also act as a transversal principle-objective defining parameters to apply during the PNRR implementation.

Keywords: Cultural heritage – Sustainable development – Internet governance – New technologies – Disasters

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0073
Articolo sottoposto a peer review

Open data per l'*e-democracy*

Anna Federica Spagnuolo • Elisa Sorrentino

Le restrizioni imposte dall'emergenza da Sars-CoV-2 hanno aumentato il desiderio di essere cittadini attivi. In questo le tecnologie digitali hanno un ruolo fondamentale. Usando dati organizzati, aperti e liberamente accessibili è possibile attuare una governance trasparente, partecipata e collaborativa migliorando la qualità dei servizi pubblici, la conoscibilità dell'azione amministrativa e la sua semplificazione. In questo modo sarebbe possibile rafforzare il controllo dei cittadini e degli stakeholder, favorendo, il passaggio dall'e-government all' e-democracy. Affinché ciò si realizzi, è indispensabile, tuttavia, che gli open data siano tutelati come veri e propri beni comuni.

Cittadinanza digitale – *e-Democracy* – Open data – Trasformazione digitale – Open government

Sommario: *1. Introduzione – 2. Dall'e-government all'open-government – 3. Open data per l'e-government – 4. La governance dei diritti digitali – 5. Conclusioni*

1. Introduzione

Il distanziamento sociale e l'isolamento imposto dall'emergenza da Sars-CoV-2 si è tradotto in molti territori in un forte desiderio di convivenza e socialità cui hanno fatto seguito richieste di maggiore partecipazione da parte dei cittadini. In tal senso, riemerge in tutto il suo valore giuridico e sociale il concetto di cittadinanza attiva, per la cui realizzazione l'uso del digitale può avere un ruolo fondamentale, soprattutto nel favorire un'idea di governance trasparente, partecipata e collaborativa. Il processo di trasformazione digitale ancora in atto, unito alla possibilità di disporre di dati organizzati, aperti e liberamente accessibili può, difatti, contribuire al miglioramento della qualità dei servizi pubblici, alla conoscibilità e alla semplificazione dell'azione amministrativa ma, soprattutto, ad una ridefinizione della forza e del potere di controllo dei cittadini e degli stakeholders sull'azione pubblica e, di riflesso, all'esercizio dei diritti di cittadinanza digitale e al corretto svolgimento della vita democratica[1]. Le amministrazioni, dal canto loro, possono intercettare bisogni e desiderata della comunità di riferimento, spesso inespressi o sommersi, e garantire ai cittadini di vedere attuato pienamente il principio di sussidiarietà sancito dall'art. 118 della nostra Costituzione[2]. Parimenti, è necessario realizzare buone pratiche di e-government[3] valorizzando ogni attività e/o iniziativa in materia di *e-democracy* così come sancito dall'art. 9 del CAD[4] rispondendo contestualmente alle attese dell'Unione europea, agli obiettivi individuati dall'Agenzia per l'Italia Digitale (AgID) nel Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022[5], al Piano nazionale innovazione 2020-2025[6], al d.l. 16 luglio 2020, n. 76 (c.d. Decreto Semplificazioni)[7] e infine al Piano Nazionale di Ripresa e Resilienza (PNRR)[8].

Se è vero, dunque, che le tecnologie digitali rappresentano il luogo in cui oggi l'individuo crea, svi-

A.F. Spagnuolo ed E. Sorrentino afferiscono all'Istituto di Informatica e Telematica del CNR, Sede di Cosenza, dove ricoprono rispettivamente i ruoli di tecnologo e collaboratore tecnico.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

luppa e forgia la propria cittadinanza digitale[9] è altrettanto vero che una società inclusiva dovrebbe agire *in primis* sulle precondizioni della partecipazione[10] garantendo ai cittadini un accesso diretto e facilitato alle informazioni provenienti da fonte pubblica.

2. Dall'e-government all'open-government

Il termine e-government (amministrazione digitale), utilizzato per la prima volta nella Comunicazione del 26 settembre 2003 della Commissione europea, indica «l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche organizzative ed all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici ed i processi democratici e di rafforzare il sostegno alle politiche pubbliche»[11].

In altri termini, quando si parla di e-government, si fa «riferimento a tutti quei processi di riorganizzazione della Pubblica Amministrazione e della sua attività che mirino a sviluppare servizi amministrativi utilizzando una varietà di strumenti elettronici intesi ad aumentare l'efficienza del settore pubblico»[12]. L'idea è che attraverso le tecnologie dell'informazione e della comunicazione (ICT) si possano ridurre le distanze e velocizzare i processi di comunicazione tra cittadini e pubblica amministrazione (PA) con un ritorno evidente in termini di riduzione dei tempi burocratici della macchina amministrativa e di maggiore efficienza della stessa. Non si tratta, dunque, di una semplice automazione dei procedimenti, ma di un vero e proprio processo di riorganizzazione, razionalizzazione, reingegnerizzazione delle attività e dei servizi offerti dalle PA che, attraverso l'uso delle nuove tecnologie[13], possono rispondere con maggiore efficacia ai principi di trasparenza, partecipazione e collaborazione[14]. Da tutto ciò discende un rinnovato rapporto tra l'amministrazione pubblica, che, in ossequio anche al principio dell'accountability, garantisce pieno accesso al suo patrimonio informativo, e il cittadino che esercita il suo diritto/dovere di controllo democratico.

Questo perché la filosofia dell'*open government* è quella di operare per una «maggiore condivisione tra pubblico e privato, con l'idea che ciò conduca a una maggiore giustizia sociale»[15].

Nonostante le entusiasmanti premesse, ci siamo trovati in piena emergenza da Sars-CoV-2 quasi del tutto impreparati. In effetti, sebbene il concetto di e-government sia da tempo presente negli obiettivi programmatici derivanti non solo da vincoli europei ma anche da puntuali obblighi internazionali[16], l'Italia ha palesato la mancanza di una contestuale predisposizione e implementazione di piani strutturati *ad hoc*, finalizzati a rendere gli interventi efficaci ed efficienti. Del resto, per come si evince dal *Digital Economy and Society Index* (DESI) 2021[17], il nostro Paese continua ad essere agli ultimi posti nelle diverse graduatorie in termini di digitalizzazione. L'indice, in particolare, misura la "performance digitale" attraverso quattro dimensioni: connettività, capitale umano, uso di servizi digitali, integrazione della tecnologia digitale nelle imprese e servizi pubblici digitali. Se si guarda più nel dettaglio la performance dell'Italia nelle varie dimensioni, ci si rende conto che le maggiori criticità si riscontrano nel primo ambito strategico, ovvero "capitale umano", che ricomprende: competenze degli utenti di Internet e competenze digitali avanzate[18].

I più recenti provvedimenti legislativi nello specifico sono tesi a favorire un tangibile processo di semplificazione e accelerazione della trasformazione digitale quali misure urgenti e necessarie, finalizzate anche e soprattutto a contrastare gli effetti dell'emergenza epidemiologica da Sars-CoV-2[19].

Sul fronte europeo, a dicembre 2020, il Parlamento e il Consiglio raggiungono un accordo provvisorio sul dispositivo per la ripresa e la resilienza[20]; mentre ad aprile 2021 viene istituito, con Regolamento[21], il programma *Europa digitale* per il periodo 2021-2027[22] con una importante dotazione finanziaria che mira, tra l'altro, a potenziare le competenze digitali dei cittadini europei, così come pianificato anche dal nostro Paese attraverso il già citato Piano nazionale innovazione 2020-2025[23] la cui *ratio* è rintracciabile negli "Obiettivi di sviluppo sostenibile" (SDGs) dell'Agenda 2030 delle Nazioni Unite[24].

Infine, il *Next Generation EU* (NGEU)[25], documento programmatorio che integra il Quadro finanziario pluriennale 2021-2027, attraverso un piano di ripresa che mira a coadiuvare l'Unione europea nel fronteggiare i danni economici e sociali derivanti dall'emergenza sanitaria e a gettare le basi per rendere le economie e le società dei paesi aderenti più sostenibili, resilienti e preparate alle sfide e alle opportunità della transizione ecologica e digitale. La componente principale è rappresentata dal Dispositivo per la ripresa e la resilienza (*Recovery and Resilience Facility*, RRF), programma di investimenti e riforme ideato per ricostruire il futuro dell'Europa[26] in cui si inserisce il PNRR, approvato in Consiglio dei ministri il 12 gennaio 2021. Quelle citate rappresentano una serie articolata di misure nazionali e sovranazionali volte ad innescare un cambiamento strutturale e capillare anche nella prospettiva di una rinnovata organizzazione della PA[27]. Si rende, dunque, neces-

sario attivare un processo di automazione e digitalizzazione della PA, che sia supportato oltre che dall'implementazione di infrastrutture/piattaforme interoperabili anche da una significativa virata verso la semplificazione/sburocratizzazione delle procedure e verso una serie di azioni volte a contrastare gli effetti derivanti dalla carenza di personale qualificato. Si prospetta per il nostro Paese una grande sfida; difatti, se è vero che la transizione digitale[28] costituisce uno dei tre assi strategici del PNRR è altrettanto vero che i timori che il nostro Paese possa rischiare di restare indietro non sono del tutto infondati.

3. Open data per l'e-government

Nonostante in tema di amministrazione digitale vi sia un consolidato e stratificato costrutto normativo nazionale[29], sovranazionale ed internazionale[30], notevoli sono ancora i gap che impediscono di valorizzare e rendere l'ingente mole di dati pubblici fruibili in maniera organica e capillare da parte di tutti i cittadini. È chiaro che non è sufficiente pubblicare e rendere accessibili i dati ma è, altresì, indispensabile rimuovere le diverse limitazioni esistenti, di natura giuridica, finanziaria o tecnologica. Allo stesso modo, non basta il semplice accesso ai dati per promuovere la partecipazione e, soprattutto, la collaborazione fra cittadini e amministrazioni. Per raggiungere tali fini è, difatti, necessario promuovere anche la disciplina dell'apertura e del riuso delle informazioni[31].

È doveroso, quindi, aprire un varco in seno alle amministrazioni pubbliche affinché siano consapevoli dell'importanza assunta dal principio del libero accesso ai dati ed ai documenti (c.d. open data[32]). Partendo dalla definizione di open data fornita dalla Open Knowledge Foundation possiamo affermare che «un contenuto, una informazione o un dato si definisce aperto se chiunque è in grado di utilizzarlo, riutilizzarlo e ridistribuirlo per qualunque scopo senza alcuna restrizione legale, tecnologica o sociale o, al massimo, con l'obbligo di garantirne la provenienza e l'apertura»[33]. Ciò significa che l'enorme mole di dati pubblici disponibili può realmente esprimere il suo potenziale solo a condizione che la stessa sia offerta in formato aperto. Solo in tal senso, difatti, è possibile rielaborare preziose informazioni e riutilizzarle per sviluppare e fornire servizi innovativi e calibrati alle reali esigenze del cittadino affinché possa realizzarsi compiutamente anche il principio di trasparenza sull'operato della PA.

Il concetto è ben radicato nel CAD e meglio esplicitato con le successive modifiche e integrazioni[34]. Da una disamina del testo si evince, difatti, quanto la nostra normativa sia estremamente puntuale e ben articolata e quanto lo specifico tema sia più volte rimarcato sin dai primi articoli dello stesso Codice[35].

La linea tracciata dal nostro legislatore è chiaramente quella di valorizzare i dati pubblici raccolti ed elaborati dalle PA consentendone esplicitamente il riutilizzo[36]. Del resto, i dati da queste creati e prodotti mediante investimenti di risorse collettive non possono che essere soggetti ad un processo di totale apertura e condivisione con concrete e fattive possibilità di rielaborazione a vantaggio dell'azione amministrativa anche in termini di accountability[37]. È esattamente per questo che il Parlamento europeo, nella Direttiva n. 2019/1024 al paragrafo 5, identifica l'accesso all'informazione come diritto fondamentale[38] incoraggiando gli Stati membri a «promuovere la creazione di dati basati sul principio dell'apertura fin dalla progettazione e per impostazione predefinita». È, in altri termini, la natura pubblica dei dati che impone di renderli accessibili a terzi, portatori di un interesse e legittimati a richiederli[39]. L'accesso all'informazione pubblica rappresenta, dunque, presupposto imprescindibile in un modello di governance orientato a principi di trasparenza, partecipazione ed accountability ma è la condivisione di dati aperti ad enfatizzare il controllo della cittadinanza sull'operato pubblico e a consentire di realizzare una vera e propria forma di democrazia monitorante[40].

Dati aperti e disponibili per il riuso[41], dunque, da intendersi alla stregua di veri e propri beni comuni[42] e valorizzati come beni comuni digitali[43], giuridicamente riconosciuti e opportunamente tutelati, per la cui gestione giocano un ruolo fondamentale i principi FAIR (*Findable*, *Accessible*, *Interoperable*, *Reusable*)[44]. L'implementazione dei suddetti principi, sin dalla fase di progettazione del sistema di raccolta (FAIR *by design*) e la cui valutazione, in termini di quali dati riutilizzare sulla base di un'analisi dei metadati[45], garantirebbe una maggiore tutela anche ai fini privacy, qualora fossero trattati dati personali, scongiurando in tal senso eventuali pericoli derivanti dall'accentramento di dati e dall'eventuale incrocio di informazioni presenti in diversi database. L'analisi dei metadati, associati ad un set di dati personali e individuati attraverso identificatori univoci e persistenti, andrebbe, difatti, a scongiurare i predetti rischi oltre a favorire il principio di minimizzazione così per come richiamato dal Regolamento UE 679/2016 (GDPR)[46]. Inoltre, affinché i diversi interventi in tema di trasformazione digitale del Paese, possano realmente tendere verso un sistema di *e-democracy*, a parere di chi scrive, sarebbe necessario animare il dibattito sull'importanza del riconoscimento dei dati come veri e propri beni comuni giuridicamente riconosciuti. Una nuova cultura del dato[47] è, difatti, in-

dispensabile per un nuovo modello di governance[48] finalizzata a migliorare la vita della cittadinanza. In questo modo si andrebbe a delineare, altresì, il passaggio da un sistema orientato all'e-government ad un sistema di *e-democracy*. La differenza non è per nulla banale, difatti, mentre l'e-government, secondo una logica *top-down*, fornisce specifici input definiti dalle amministrazioni e funzionali all'ottimizzazione delle attività di cittadinanza, l'*e-democracy* presuppone un processo orizzontale che dovrebbe favorire l'adozione di politiche *bottom-up*[49] in attuazione del succitato art. 118 Cost.

4. La governance dei diritti digitali

Senza ombra di dubbio, la chiave di volta per una governance digitale più equa ruota intorno al riconoscimento di un diritto di accesso diffuso, da parte dei cittadini e degli stakeholder in generale, alle nuove tecnologie, alle informazioni attraverso l'accessibilità a dati aperti e disponibili, e ovviamente ad Internet[50]. Va da sé, infatti, che per un effettivo esercizio del diritto all'uso delle tecnologie digitali è indispensabile rafforzarne l'utilizzo attraverso una politica di accesso ampia e generalizzata ad Internet[51]. In tale ottica, l'art. 24 del citato d.l. n. 76/2020[52] ha disposto diverse modifiche agli artt. 3-*bis*, 6-*bis*, 6-*quater*, 64, 64-*bis*, 65 del CAD.

Il d.l. n. 76/2020 impone sostanzialmente l'uso di strumenti informatici e telematici nello svolgimento dell'azione amministrativa della PA con il precipuo scopo di semplificare e innovare la macchina burocratica e contestualmente di facilitare e sostenere il dialogo tra le PA e i cittadini.

Ciò detto, è necessario approntare una serie di misure che possano intercettare e colmare il persistente *digital divide*[53] con l'obiettivo di trarre maggiori benefici per l'empowerment personale e sociale[54] non limitando l'attenzione sui "connessi" ma anche sui "disconnessi", poiché «non disporre effettivamente del diritto di accedere a Internet, nell'era dell'accesso, significa, difatti, essere [...] eremiti analogici in un mondo digitale»[55]. In altri termini l'insieme dei servizi che sono offerti su Internet è, oramai tale da renderne imprescindibile l'accesso, in quanto «nello spazio digitale gli individui soddisfano un ampio spettro di bisogni fondamentali per lo sviluppo della persona[56]». Pertanto, se è vero che l'accesso alle ICT moltiplica le chance di cittadinanza per i soggetti connessi è pur vero che moltiplica le disuguaglianze dei soggetti non connessi[57].

Anche in questo caso il nostro impianto normativo è più che puntuale. Il CAD, difatti, non si limita a dettare una disciplina in supporto alla definizione di un'amministrazione digitale[58] ma delinea, così come è stato evidenziato nel paragrafo precedente, il percorso da attuare per un nuovo processo democratico fra cittadini ed amministrazioni, incentrato sui diritti digitali. Diritto all'uso delle tecnologie[59], all'identità digitale e al domicilio digitale[60], a servizi online semplici e integrati[61]. Di assoluto rilievo, il diritto all'alfabetizzazione informatica dei cittadini disposta dall'art. 8, secondo cui lo Stato e le amministrazioni pubbliche promuovono iniziative volte all'alfabetizzazione informatica dei cittadini con particolare riguardo ai minori ed alle categorie a rischio di esclusione in modo da consentire una riduzione del *digital divide*[62]. Infine, ma non per importanza, il diritto alla *partecipazione democratica elettronica* ai sensi dell'art. 9, che incentiva lo sviluppo degli strumenti di *e-democracy*. Nello specifico, il legislatore italiano dispone che i vari soggetti pubblici, obbligati all'applicazione del CAD, devono favorire l'utilizzo delle tecnologie oltre che per migliorare la qualità dei propri atti anche e soprattutto per promuovere la partecipazione[63] dei cittadini al processo democratico. Si facilita, in tal modo, l'esercizio dei diritti politici e civili, anche attraverso la realizzazione di forme di democrazia diretta[64]. Come già affermava l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) nel 2009[65], la partecipazione dei cittadini alle politiche pubbliche è la precondizione di una governance effettiva. In tal senso, se pianificare politiche in tema di sviluppo urbano e territoriale così come in altri domini si assume come un'operazione complessa e ad alto rischio di fallimento, va da sé che i processi decisionali inclusivi possono incidere strategicamente su questa problematica rendendola più facilmente governabile. La prospettiva che le organizzazioni della società civile lavorino con le amministrazioni pubbliche alla definizione, all'attuazione, al monitoraggio e alla valutazione delle diverse strategie consente, difatti, di migliorare la qualità degli interventi messi in atto, semplicemente perché condivisi con la comunità di riferimento. Alla base di tutto ciò, è necessario vi sia la condivisione di dati e informazioni aperti, liberi da qualsiasi limitazione che ne impedisca il riuso, la modifica, la combinazione con altri dati e l'interoperabilità[66], così che tutti possano accedervi in maniera diretta e trasparente, al fine di rendere i cittadini più consapevoli e dunque più liberi.

Tutto ciò premesso, se le nostre amministrazioni saranno in grado di recepire in tempi rapidi quanto indicato dal legislatore potremo riuscire a superare una grande prova in cui sono in gioco non solo la credibilità dell'operato delle istituzioni ma anche il fondamentale diritto ad una cittadinanza digitale e partecipativa.

5. Conclusioni

Se è vero che la pandemia ha acuito problemi più o meno latenti e che alla crisi economica si è aggiunta una diffusa sfiducia nei confronti delle istituzioni e delle decisioni da queste assunte, è altrettanto vero che il legislatore ci ha fornito tutti gli strumenti per poter sfruttare al meglio le potenzialità espresse dalle tecnologie digitali anche al fine di favorire un contatto più agevole con le amministrazioni e mantenere una maggiore coscienza sull'operato delle stesse. Restano indubbiamente una serie di criticità da risolvere che, da un lato sono, direttamente connesse al *digital divide* e, dall'altro, alla carenza di linee politiche e programmatiche in seno alle nostre amministrazioni volte ad implementare una riorganizzazione in ottica di digitalizzazione, atta a semplificare i procedimenti e i processi amministrativi e a facilitare e favorire la comunicazione con i cittadini. Per questi motivi è necessario attuare strategie che possano esaltare il valore sociale della trasformazione digitale tesa all'inclusione e alla condivisione garantendo a tutti le medesime possibilità di usufruire dei vantaggi della società digitale e di esserne parte attiva.

Appropriandosi della tecnologia, sfruttandone i vantaggi, mettendo a disposizione e condividendo le competenze digitali di alcuni per il bene della comunità, si potrà realizzare una vera e propria rivoluzione digitale *bottom-up*.

Per questi motivi è lecito che i cittadini rivendichino i propri diritti digitali, anche e soprattutto perché sono essi stessi la fonte primaria delle indagini e delle raccolte da cui viene generata l'enorme quantità d'informazioni detenute dalle PA[67].

Per di più, viviamo in un'epoca in cui è possibile comprendere le scelte politiche e amministrative alimentando la spinta partecipativa dei cittadini e ricostruendo, in tal senso, la fiducia all'interno del tessuto sociale, ma per far sì che ciò avvenga, bisogna, altresì, lavorare su una nuova politica del dato.

Accesso agli open data, dunque, da parte di tutti coloro che ne hanno interesse senza che ciò comporti una particolare qualificazione giuridica dell'interesse medesimo, giungendo così ad una totale trasparenza dell'operato della PA, sia sotto il profilo dell'attività procedimentale che della organizzazione amministrativa. Soltanto, dunque, attraverso la totale apertura verso le parti interessate potrà realizzarsi un effettivo coinvolgimento delle stesse nel processo decisionale responsabilizzando maggiormente le pubbliche amministrazioni in un'ottica non soltanto giuridica ma anche etica[68].

Note

[1]Si veda a tal proposito E. De Marco, *Democrazia in trasformazione: i nuovi orizzonti della democrazia diretta*, in "Federalismi.it", numero speciale 1/2017, p. 4.

[2]In forza dell'ultimo comma dell'art. 118 Cost., «Stato, Regioni, Città metropolitane, Province e Comuni favoriscono l'autonoma iniziativa dei cittadini, singoli e associati, per lo svolgimento di attività di interesse generale, sulla base del principio di sussidiarietà».

[3]Si veda OECD, *The OECD Digital Government Policy Framework: Six dimensions of a Digital Government*, OECD Public Governance Policy Papers No. 02, OECD Publishing, 2020. L. Torres, V. Pina, S. Royo, *E-government and the transformation of public administrations in EU countries: Beyond NPM or just a second wave of reforms?*, in "Online Information Review", vol. 29, 2005, n. 5, p. 531 ss.; C.B. Stahl, *The Ethical Problem of Framing e-Government in Terms of e-Commerce*, in "The Electronic Journal of E-Government", vol. 3, 2005, n. 2, p. 77-82; D.F. Norris, M.J. Moon, *Advancing E-Government at the Grassroots: Tortoise or Hare?*, in "Public Administration Review", vol. 65, 2005, n. 1, p. 64 ss.; S.S. Dawes, *The Evolution and Continuing Challenges of E-Governance*, *ivi*, vol. 68, 2008, n. s1, p. 86 ss.; D.F. Norris, *E-Government 2020: Plus ça change, plus c'est la meme chose*, *ivi*, vol. 70, 2010, n. s1, p. 180 ss.; C.A. Hardy, S.P. Williams, *Assembling E-Government Research Designs: A Transdisciplinary View and Interactive Approach*, *ivi*, vol. 71, 2011, n. 3, p. 405 ss.; M.J. Moon, J. Lee, C.Y. Roh, *The Evolution of Internal IT Applications and e-Government Studies in Public Administration: Research Themes and Methods*, in "Administration & Society", vol. 46, 2014, n. 1, p. 3-36.

[4]D.lgs. 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale* (CAD).

[5]Il *Piano Triennale* è consultabile online.

[6]Ministro per l'innovazione tecnologica e la digitalizzazione, *Piano nazionale innovazione 2025* - Release stabile, 9 novembre 2020.

[7]V. d.l. 16 luglio 2020, n. 76 convertito con l. 11 settembre 2020, n. 120 recante *Misure urgenti per la semplificazione e l'innovazione digitale*.

[8]Il *Piano Nazionale di Ripresa e Resilienza* (PNRR) è consultabile sul sito del Governo.

[9]Si veda a tal proposito P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.*, in "Federalismi.it", 2018, n. 2, p. 13. Secondo l'autore «Quando tra amministrazione e cittadino si instaura – obbligatoriamente e per scelta del legislatore – un rapporto "di cittadinanza digitale", emerge l'obbligo per i pubblici poteri di rendere effettivo il diritto d'accesso alla rete come precondizione per l'esercizio di ulteriori diritti, anche costituzionalmente garantiti, nonché per la realizzazione dei principi di buon andamento ed imparzialità di un'amministrazione digitale».

[10]Si veda E. De Marco, *op. cit.*, p. 4. Secondo l'autore per la realizzazione del principio democratico assume particolare rilievo la distinzione tra democrazia rappresentativa, democrazia diretta e democrazia partecipativa o diffusa.

[11]Commissione europea, *Il ruolo dell'e-government per il futuro dell'Europa*, comunicazione del 26 settembre 2003. Fra i contributi dottrinali più recenti si segnala C.M. Arpaia, P. Ferro, W. Giuzio et al., *L'e-Government in Italia: situazione attuale, problemi e prospettive*, in "Questioni di Economia e Finanza", Banca d'Italia, n. 309, febbraio 2016; F. Bassanini, *Twenty years of administrative reforms in Italy*, in "Review of Economic Conditions in Italy", 2009, n. 3.

[12]D.U. Galetta, *Open Government, Open Data e azione amministrativa*, in "Istituzioni del Federalismo", 2019, n. 3, p. 664.

[13]Sull'*open government* D. Lathrop, L. Ruma (eds.), *Open Government: Collaboration, Transparency, and Participation in Practice*, O'Reilly Media, 2010; E. Carloni (a cura di), *L'amministrazione aperta. Regole strumenti e limiti dell'open government*, Maggioli, 2014; F. Di Donato, *Lo Stato trasparente. Linked open data e cittadinanza attiva*, Edizioni ETS, 2010; L. Sartori, *Open government: what else?*, in "Istituzioni del Federalismo", 2013, n. 3-4, pp. 753-775; F. Faini, *La strada maestra dell'open government: presupposti, obiettivi, strumenti*, in "Ciberspazio e diritto", 2013, n. 2, pp. 213-238. In merito T. Agnoloni, *Dall'informazione giuridica agli* open data *giuridici*, in G. Peruginelli, M. Ragona (a cura di), "L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze", ESI, 2014, pp. 581-602. L'autore sottolinea come il paradigma del governo aperto sia anteriore e indipendente rispetto alle tecnologie della rete: è finalizzato alla trasparenza, alla responsabilità e al controllo delle azioni da parte dei cittadini.

[14]Cfr. L. Sartori, *op. cit.*, p. 755. Secondo l'autore «I pilastri dell'*Opengov* sono individuabili nella trasparenza e nella partecipazione, cui va aggiunta la collaborazione, quale meccanismo di raccordo tra le due precedenti».

[15]V. Sforza, A. Alongi, F. Pompei et al., *Cittadinanza digitale: dal lifelong learning all'e-government*, TAB edizioni, 2021.

[16]La trasformazione digitale nel settore pubblico è fortemente relazionata al contesto sovranazionale per la funzione regolatrice che l'Unione europea svolge al fine di garantire l'interoperabilità dei sistemi nazionali e di definire un quadro normativo coerente e armonizzato.

[17]European Commission, *Digital Economy and Society Index 2021*, disponibile anche in italiano: *Indice di digitalizzazione dell'economia e della società (DESI) 2020*.

[18]Secondo l'indice DESI (2021), l'ambito strategico "capitale umano" è quello con meno miglioramenti nel decennio, tanto da collocare il Paese al 25° posto nella graduatoria europea con un punteggio di molto inferiore rispetto alla media (35,1% rispetto al valore medio del 47,1%).

[19]È importante citare il d.l. 19 maggio 2020, n. 34, *Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19 coordinato con la legge di conversione 17 luglio 2020, n. 77* e il già citato d.l. 16 luglio 2020, n. 76 convertito con l. 11 settembre 2020, n. 120 recante *Misure urgenti per la semplificazione e l'innovazione digitale*.

[20]Per approfondimenti si consulti Consiglio europeo, Consiglio dell'Unione europea, *Dispositivo per la ripresa e la resilienza: la presidenza del Consiglio e il Parlamento raggiungono un accordo provvisorio*, comunicato stampa, 18 dicembre 2020.

[21]Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240.

[22]Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il programma Europa digitale per il periodo 2021-2027, COM/2018/434 final del 6 giugno 2018.

[23]Il Piano rappresenta la strategia messa in campo dall'Italia all'interno della quale l'innovazione e la digitalizzazione del Paese «devono far parte di una riforma strutturale dello Stato che promuova più democrazia, uguaglianza, etica, giustizia e inclusione e generi una crescita sostenibile nel rispetto dell'essere umano e del nostro pianeta».

[24]Agenzia Italiana per la Cooperazione allo Sviluppo, Obiettivi di sviluppo sostenibile - SDGs.

[25]Unione europea, *NextGenerationEU*.

[26]L. Cavalli, S. Sanna, M. Alibegovic et al., *Sulla valutazione del contributo delle politiche di coesione 2021-2027 all'Agenda 2030. Una proposta metodologica*, Fondazione Eni Enrico Mattei, 30 luglio 2020.

[27]M. Pollifroni, *Open Government. I processi di reingegnerizzazione dell'azienda pubblica tra etica ed innovazione*, Giappichelli, 2020.

[28]«La transizione digitale giocherà un ruolo determinante per le traiettorie di crescita di medio-lungo periodo dell'Italia considerando che sarà proprio la Missione 1 del PNRR relativa alla digitalizzazione ("M1 digitalizzazione, innovazione, competitività, cultura e turismo") quella che avrà il maggiore impatto sulla crescita economica secondo le stime contenute nello stesso PNRR: +3,9 punti percentuali di innalzamento del PIL reale rispetto allo scenario base nell'intero periodo 2021-26, rappresentando quasi il 30% dell'intero impatto del PNRR stimato in 15 punti percentuali». Si veda V. Meliciani, M. Pini, *Digitalizzazione e produttività in Italia: Opportunità e rischi del PNRR*, Luiss, Policy Brief 14/2021, 28 luglio 2021.

[29]Il d.lgs. 7 marzo 2005, n. 82 e s.m.i. - Codice dell'Amministrazione Digitale (CAD); d.l. 22 giugno 2012, n. 83 convertito dalla legge, 7 agosto 2012 n. 134; d.l. 18 ottobre 2012, n. 179, coordinato con la legge di conversione 17 dicembre 2012, n. 221; l. 6 novembre 2012, n. 190; d.lgs. 24 gennaio 2006, n. 36 - *Attuazione della direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico*; d.lgs. 18 maggio 2015, n. 102 - *Attuazione della direttiva 2013/37/UE che modifica la direttiva 2003/98/CE, relativa al riutilizzo dell'informazione del settore pubblico*; AGID, *Linee Guida Nazionali per la Valorizzazione del Patrimonio Informativo Pubblico*, 13 febbraio 2020; Id., *Linee Guida per i cataloghi di dati*, 23 febbraio 2020.

[30]Si vedano a tal proposito: la Direttiva 2003/98/CE del Parlamento europeo e del Consiglio relativa al riutilizzo dell'informazione del settore pubblico; la Direttiva 2013/37/CE del Parlamento europeo e del Consiglio che modifica la precedente Direttiva 2003/98/CE; il Regolamento 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE Regolamento generale sulla protezione dei dati, il Rapporto 2016 sull'e-government delle Nazioni Unite nel quale si evidenzia un sensibile aumento dei Paesi che usano strumenti informatici nella pubblica amministrazione per offrire pubblici servizi online ai cittadini, la Direttiva 2019/1024 che mira a promuovere l'utilizzo di dati aperti e ad agevolare il riutilizzo, a fini commerciali e non commerciali, delle informazioni detenute da pubbliche amministrazioni, da organismi di diritto pubblico e, a determinate condizioni anche delle imprese pubbliche.

[31]A riguardo si vedano, *ex multis*, C. Alberti, *E-society e riutilizzo dell'informazione nel settore pubblico. Disciplina comunitaria e riflessi nazionali*, in "Rivista italiana di diritto pubblico comunitario", 2005, n. 5, pp. 1237-1274; B. Ponti, *Il riutilizzo di documenti del settore pubblico*, in "Giornale di diritto amministrativo", 2006, n. 8, p. 817 ss.; M. Alovisio, *Criticità Privacy nel riuso dei dati pubblici*, in "Informatica e diritto", 2011, n. 1-2, pp. 45-64; M. Maggiolino, *Il riutilizzo dell'informazione detenuta dal settore pubblico: alcune riflessioni di politica e diritto della concorrenza*, in "Concorrenza e mercato", 2012, pp. 765-802; P. Patrito, F. Pavoni, *La disciplina del riutilizzo dei dati pubblici dal punto di vista del diritto amministrativo: prime riflessioni*, in "Diritto dell'informazione e dell'informatica", 2012, n. 1, pp. 87-115; M. Ragone, *I dati aperti: l'innovazione a portata dei cittadini, pubblica amministrazione, imprese*, in "Rivista degli infortuni e delle malattie professionali", 2012, n. 3, pp. 803-812; I. Ma-

crì, *I dati delle pubbliche amministrazioni fra adempimenti e opportunità*, in "Azienditalia", 2012, n. 1, p. 7 ss.; F. Costantino, voce *Open government*, in "Digesto delle discipline pubblicistiche", UTET, aggiornamento, 2015; F. Gaspari, *L'agenda digitale europea e il riutilizzo dell'informazione del settore pubblico*, Giappichelli, 2016; G. Carullo, *Big data e pubblica amministrazione nell'era delle banche dati interconnesse*, in "Concorrenza e mercato", 2016, pp. 181-204; F. Costantino, *Lampi. Nuove frontiere delle decisioni amministrative tra* open *e* big data, in "Diritto amministrativo", 2017, n. 4, pp. 799-836; S. D'Ancona, *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo*, in "Rivista italiana di diritto pubblico comunitario", 2018, n. 3-4, pp. 587-627.

[32]L'attuale attenzione al concetto di open data nel contesto delle attività di governo si può far risalire al 2009, alle iniziative del presidente Obama negli USA. Infatti, nello stesso giorno del suo insediamento e come primo atto, il presidente Barack Obama ha pubblicato un memorandum sulla trasparenza e l'*Open Government* indirizzato ai dirigenti della sua amministrazione: «la mia amministrazione si impegna a dare vita a un grado di apertura (openness) nel governo senza precedenti. Lavoreremo assieme per assicurare la fiducia pubblica e per stabilire un sistema basato sulla trasparenza, sulla partecipazione pubblica e sulla collaborazione. L'apertura rafforzerà la nostra democrazia e promuoverà l'efficienza e l'efficacia dell'amministrazione». Al memorandum ha fatto seguito l'8 dicembre 2009 la *Open Government Directive* e la *Open Government Initiative* che, appunto, raccoglie le iniziative per l'*Open Government* dell'amministrazione federale americana in un sito progettato per favorire la partecipazione e i feedback dei visitatori. La *Open Government Directive* prevede, invece, che (ove possibile) l'amministrazione statunitense pubblichi le informazioni di cui dispone «on line, utilizzando un formato aperto (open) che possa cioè essere recuperato, soggetto ad azioni di download, indicizzato e ricercato attraverso le applicazioni di ricerca web più comunemente utilizzate. Per formato open si intende un formato indipendente rispetto alla piattaforma, leggibile dall'elaboratore e reso disponibile al pubblico senza che sia impedito il riuso dell'informazione veicolata». Per quanto riguarda il nostro Paese, bisogna attendere il 2012 con l'adesione all'*Open Government Partnership* e l'emanazione del primo piano di azione in materia di *open government*.

[33]Si veda la definizione sul sito dell'Open Knowledge Foundation.

[34]Il CAD, emanato a seguito della delega al Governo contenuta all'art. 10 della l. 29 luglio 2003, n. 229, entra in vigore nell'ordinamento italiano il 1° gennaio 2006. A pochi mesi dalla sua entrata in vigore è stato oggetto di una serie di correttivi, disposti con il d.lgs. 4 aprile 2006, n. 159 la cui emanazione era stata autorizzata dalla medesima legge delega 29 luglio 2003, n. 229. Il decreto correttivo, oltre che modificare in diversi punti la struttura del CAD, traspone al suo interno l'intero testo già compendiato nel d.lgs. 28 febbraio 2005, n. 42 – contestualmente abrogato – disciplinante il sistema pubblico di connettività e la rete internazionale delle Pubbliche Amministrazioni. In tal senso, anche l'art. 16 del decreto anticrisi (d.l. 29 novembre 2008, n. 185, convertito in l. 28 gennaio 2009, n. 2) ha modificato i commi 4 e 5 dell'art. 23, prevedendo per la copia firmata digitalmente lo stesso valore dell'originale senza obbligo di autentica da parte di notaio o di altro pubblico ufficiale, salvo i documenti da indicare con decreto del presidente del Consiglio dei ministri. Altre modifiche sono state poi introdotte dalla l. 18 giugno 2009, n. 69 e dalla l. 3 agosto 2009, n. 102. Successivamente, importanti modificazioni e integrazioni sono state introdotte dal d.lgs. 30 dicembre 2010, n. 235. Infatti, sono stati modificati 53 articoli sui 92 originari e sono stati introdotti altri 9 articoli. Il d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, inoltre, aggiorna il CAD all'ultimo orizzonte tecnologico introducendo i concetti di domicilio digitale, cloud computing e revisione dei CED. Altra modifica del CAD è stata introdotta, prima, dalla l. 23 dicembre 2014, n. 190, e successivamente con il d.lgs. 26 agosto 2016, n. 179; quest'ultima modifica rientra nel quadro normativo della legge delega 7 agosto 2015, n. 124 (riforma della PA del Ministro Madia). Successivamente il CAD è stato modificato e integrato con il d.lgs. 13 dicembre 2017, n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale. Per l'elenco completo degli aggiornamenti consultare il sito dell'Agenzia per l'Italia Digitale.

[35]Nello specifico, l'art. 1, co. 1, lett. o) del CAD chiarisce il concetto di "disponibilità dei dati", da intendersi come «possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge», mentre per "fruibilità del dato" si intende «la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione». Il successivo art. 2, co. 1, statuisce che «lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale [...]». L'art. 1, co. 1, lett. l-*ter* specifica che i dati si intendono di tipo aperto se: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato; 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti, sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati; 3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione salvo quanto previsto dall'art. 7 del d.lgs. 24 gennaio 2006, n. 36.

[36]F. Sciacchitano, *Disciplina e utilizzo degli Open Data in Italia*, in "MediaLaws", 2018, n. 1.

[37]Si veda a tal proposito F. Martines, *La digitalizzazione della pubblica amministrazione*, in "MediaLaws", 2018, n. 2, in cui l'autore osserva come «Soltanto attraverso la totale apertura verso le parti interessate potrà realizzarsi un effettivo coinvolgimento delle stesse nel processo decisionale il che, fra l'altro, responsabilizzerà maggiormente le pubbliche amministrazioni in un'ottica non soltanto giuridica (aquiliana) ma anche etica (c.d. accountability)».

[38]Il 26 giugno 2019 è stata pubblicata sulla Gazzetta ufficiale dell'Unione europea la direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico. Dopo la sua adozione nel 2003 e la significativa revisione del 2013, ora la direttiva è stata rilanciata tenendo conto dei profondi cambiamenti tecnologici e sociali avvenuti negli ultimi cinque anni, contemplando allo stesso tempo la normativa di riferimento sulla gestione dei dati.

[39]V. Zeno-Zencovich, voce *Informazione (profili civilistici)*, in "Digesto delle discipline privatistiche", vol. IX, UTET, 1993, p. 426.

[40]F. Di Mascio, A. Natalini, *Oltre il New Public Management. Le riforme amministrative tra meccanismi e contesti*, Carocci, 2018, p. 62.

[41]M.D. Wilkinson, M. Dumontier, I. Aalbersberg et al., *The FAIR Guiding Principles for scientific data management and stewardship*, in "Scientific data", n. 3, 2016.

[42]Si veda a tal proposito S. Rodotà, *Il valore dei beni comuni*, in "La Repubblica", 5 gennaio 2012, in cui l'autore definisce i beni comuni come quei beni «funzionali all'esercizio di diritti fondamentali e al libero sviluppo della personalità, che devono essere salvaguardati sottraendoli alla logica distruttiva del breve periodo, proiettando la loro tutela nel mondo più lontano, abitato dalle generazioni future». La prima definizione tecnico-legislativa dei beni comuni fu data durante i lavori della Commissione per la riforma del Titolo II del Libro III del Codice Civile, istituita dal Governo Prodi, nota come Commissione Rodotà, dall'autorevole nome di chi ne assunse la Presidenza. I lavori della Commissione si protrassero fino al Febbraio del 2008 e furono completati con un d.l. delega che mirava tra l'altro a introdurre nell'ordinamento giuridico italiano una disciplina organica dei beni comuni. Il tema è da tempo al centro di una vivace discussione, risvegliando l'attenzione di esperti di diversi settori della conoscenza, giuridica, economica, politica, filosofica e sociale. In Italia le politiche economiche di progressiva privatizzazione di beni, servizi, settori economici, avviate agli inizi degli anni '90, unite ad un progressivo disfacimento dello Stato sociale, hanno dato origine ad una crescente preoccupazione circa la concreta possibilità di accedere a beni e servizi essenziali da parte di tutti i cittadini. Si veda a questo proposito U. Mattei, E. Reviglio, S. Rodotà (a cura di), *I beni pubblici. Dal governo democratico dell'economia alla riforma del codice civile*, Accademia nazionale dei Lincei, 2010; U. Mattei, *Beni comuni. Un manifesto*, Laterza, 2011; M.R. Marella (a cura di), *Oltre il pubblico e il privato. Per un diritto dei beni comuni*, Ombre Corte, 2012.

[43]Si veda a questo proposito A. Pradi, A. Rossato (a cura di), *I beni comuni digitali*, Editoriale Scientifica, 2014. Si veda inoltre M. Lawrence, L. Laybourn-Langton, *The Digital Commonwealth: From private enclosure to collective benefit*, *discussion paper*, IPPR, 2018.

[44]I principi FAIR sono stati elaborati nel 2014 per ottimizzare la riutilizzabilità dei dati della ricerca. Essi rappresentano un insieme di linee guida e migliori pratiche sviluppate per garantire che i dati, o qualsiasi oggetto digitale, siano *Findable*/Rintracciabili, *Accessible*/Accessibili, *Interoperable*/Interoperabili e *Re-usable*/Riutilizzabili. Rintracciabili: per poter rendere i dati riutilizzabili occorre che siano per prima cosa rintracciabili dagli esseri umani e dalle macchine. Il recupero automatico e affidabile di set di dati dipende dagli identificatori persistenti (PID) utilizzati, quali ad esempio DOI, Handle o URN, e dai metadati descrittivi attribuiti ai dati, che devono essere registrati in cataloghi o in repository indicizzabili anche dalle macchine. Accessibili: i dati o almeno i loro metadati devono poter essere accessibili dagli esseri umani e dalle macchine anche attraverso sistemi di autenticazione e autorizzazione (non è necessario che i dati depositati siano open access) mediante l'uso di protocolli standard. I dati e i loro metadati devono essere depositati in archivi o repository che li rendano possibilmente persistenti nel tempo e rintracciabili in rete. Almeno i metadati dovrebbero rimanere sempre disponibili anche quando i dati non sono in open access. Interoperabili: i dati devono poter essere combinati e utilizzati insieme con altri dati o strumenti. Il formato dei dati deve pertanto essere aperto e interpretabile da vari strumenti, compresi altre basi di dati. Il concetto di interoperabilità si applica anche ai metadati. Ad esempio, i metadati dovrebbero utilizzare un linguaggio standardizzato e condiviso a livello internazionale dai diversi servizi di indicizzazione. Riutilizzabili: sia i metadati, sia i dati devono essere descritti e documentati nel migliore dei modi, a garanzia della loro qualità e perché possano essere replicati e/o combinati in contesti diversi. Il trattamento dei dati dovrebbe conformarsi agli standard o ai protocolli riconosciuti dalle comunità scientifiche di riferimento. Il riutilizzo dei metadati e dei dati dovrebbe essere dichiarato con una/o più licenze aperte chiare ed accessibili.

[45]E.T. Inau, J. Sack, D. Waltemath, A. Alamirrew Zeleke, *Initiatives, Concepts, and Implementation Practices of FAIR (Findable, Accessible, Interoperable, and Reusable) Data Principles in Health Data Stewardship Practice: Protocol for a Scoping Review*, in "JMIR Research Protocols", vol. 10, 2021, n. 2.

[46]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR). In particolare, l'art. 5 del GDPR prevede che i dati debbano essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati».

[47]Il concetto di *data revolution* è stato ideato dall'*High Level Panel Post-2020 Development Agenda*, un gruppo di esperti che è stato voluto dal segretario generale delle Nazioni Unite Ban Ki-moon all'indomani della definizione dei *Millennium Development Goals* del 2000. L'*High Level Panel* ha elaborato un report per la lotta alla povertà in cui l'uso dei dati gioca un ruolo di primo piano (*A New global parnership: Eradicate poverty and transfrom economies through sustaintable development. The Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda*, 2013, p. 23-34) e che è stato da stimolo per la nascita del progetto *Data Revolution Group*.

[48]Si veda a questo proposito M. Trapani, *Il diritto di accesso generalizzato e l'emergenza: rischi ed opportunità in uno Stato tecnologico*, in "DPCE Online", 2020, n. 3, p. 14. L'autore sostiene che sarebbe necessario in definitiva, che anche il legislatore, superando il paradigma della digitalizzazione come mero vettore di informazioni, provveda non solamente a regolarne l'utilizzo ma anche a ripensarne la governance, superando alcune criticità che hanno determinato una minore accessibilità (anche e soprattutto per le persone affette da disabilità), una minore garanzia dei diritti e un'insufficiente semplificazione dei processi della P.A., affrontando il tema in modo organico e non come mero corollario di altre discipline.

[49]Si veda a questo proposito di L. Abba, A. Alù, *Internet Governance Forum: l'evoluzione del modello multistakeholder tra criticità e prospettive future*, in questa Rivista, 2020, n. 1, p. 83. Gli autori evidenziano la necessità di realizzare un governo della rete secondo un approccio realmente *bottom-up* e *multistakeholder* e secondo un modello di *constituency* rappresentativo ove sia garantito il pieno coinvolgimento di tutti gli attori della comunità di Internet nella sua gestione trasparente e partecipativa.

[50]Nella Risoluzione dell'UNHR del 2016 *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, il diritto di accesso ad Internet è stato definito come diritto umano ed è stato affermato che gli Stati dovrebbero approntare una serie di misure finalizzate ad incrementare e migliorare la partecipazione dei cittadini e ad eliminare le cause del *digital divide*. Sulla medesima linea la più recente Risoluzione dell'UNHCR di luglio 2018 *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. È stato affermato come Internet possa essere considerato uno strumento importante per favorire la partecipazione dei cittadini e della società civile, per la realizzazione e lo sviluppo in ogni comunità e per l'esercizio dei diritti umani e che, pertanto, ogni Stato dovrebbe garantire la promozione, la protezione e il godimento dei diritti umani, compreso il diritto alla libertà di espressione su Internet e con altre tecnologie dell'informazione e della comunicazione. Il dibattito sul riconoscimento di Internet quale diritto fondamentale è fervido da tempo anche in Italia. Stefano Rodotà, in occasione del III

Internet Governance Forum, avanzò una proposta di modifica costituzionale formulando un articolo 21-*bis* in base al quale «Tutti hanno eguale diritto di accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale». Sull'accesso ad Internet come diritto sociale e fondamentale in seno al dibattitto giuridico nazionale si veda S. Rodotà, *Tecnologie e diritti*, Il Mulino, 2006; M. Cuniberti (a cura di), *Nuove tecnologie e libertà della comunicazione*, Giuffrè, 2008; P. Tanzarella, *Accesso a Internet: verso un nuovo diritto sociale?*, in E. Cavasino, G. Scala, G. Verde (a cura di), "I diritti sociali: dal riconoscimento alla garanzia. Il ruolo della giurisprudenza", Atti del Convegno annuale dell'Associazione "Gruppo di Pisa" (Trapani, 8-9 giugno 2012), pp. 517-532. Si veda, inoltre, T.E. Frosini, *L'accesso a Internet come diritto fondamentale*, in O. Pollicino, E. Bertolini, V. Lubello (a cura di), "Internet: regole e tutela dei diritti fondamentali", Aracne, 2013; P. Passaglia, *Internet nella Costituzione italiana: considerazioni introduttive*, in M. Nisticò, P. Passaglia, "Internet e Costituzione", Giappichelli, 2014, p. 18. Nel testo si elencano cinque diverse forme di esclusione da Internet: a) la determinazione autoritativa, correlata a determinate situazioni (ad es. lo stato di detenzione); b) le carenze infrastrutturali, che rendono impossibile la connessione in determinate aree; c) le difficoltà economiche che impediscono a un individuo di possedere o detenere strumenti che consentano un adeguato accesso alla rete; d) problemi di ordine fisico che precludono al soggetto la fruizione di determinati contenuti; e) un deficit culturale dell'individuo, privo delle conoscenze informatiche sufficienti per interfacciarsi con un computer.

[51]G. d'Ippolito, *La tutela dell'effettività dell'accesso ad Internet e della neutralità della rete*, in questa Rivista, 2021, n. 2, pp. 33-42.

[52]Il d.l. n. 76 del 2020 all'art. 12 co. 1 lett. b, introduce alcune modifiche al già menzionato art. 3-*bis*, stabilendo che le pubbliche amministrazioni «agiscono mediante strumenti informatici e telematici».

[53]Il *Digital divide*, letteralmente "divario digitale", è un'espressione che descrive la situazione della popolazione divisa tra chi dispone degli strumenti e delle competenze utili per accedere e usufruire appieno delle opportunità offerte dalle tecnologie della comunicazione, collegate in prevalenza all'uso di Internet, e chi non le ha. Non si tratta, tuttavia, di una mera distinzione tra "haves and have-nots", ovvero tra coloro che hanno accesso alle nuove tecnologie e coloro che non le hanno, ma descrive una condizione molto più ampia di diversità. Quest'ultima si declina sia in termini di risorse tecnologiche, sia in termini di competenze legate in maniera particolare all'alfabetizzazione informatica ed entrambi dipendenti da diversi fattori: territoriali, economici, culturali, anagrafici, di genere e tecnologici. A tal proposito si veda, S. Raveesh, *Digital Divide – "Haves" and "Have-Nots": A Modern Inequality of 21st Century*, in "European Academic Research", vol. 1, 2013, n. 7. Si veda, inoltre, P. Norris, *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, Cambridge University Press, 2001; P. Dimaggio, E. Hargittai, *From the 'Digital Divide' to 'Digital Inequality': Studying Internet Use as Penetration Increases*, Princeton University, Woodrow Wilson School of Public and International Affairs, Center for Arts and Cultural Policy Studies, Working Papers, 2001; E. Hargittai, *Second-level digital divide: Differences in People's Online Skills*, in "First monday", vol. 7, 2002, n. 4, p. 1-17. Per uno sguardo alla letteratura nazionale si veda di L. Sartori, *Il divario digitale: internet e le nuove disuguaglianze sociali*, Il Mulino, 2006; S. Bentivegna, *Disuguaglianze digitali: le nuove forme di esclusione nella società dell'informazione*, Laterza, 2009. P. Botta, *Il divario digitale nel mondo giovanile: il rapporto dei giovani italiani con le ICT*, ISFOL, 2011.

[54]R. Bracciale, *Donne nella rete. Disuguaglianze digitali di genere*, Franco Angeli, 2010; E. Hargittai, Y.P. Hsieh, *Succinct Survey Measures of Web-Use Skills*, in "Social Science Computer Review", vol. 30, 2011, n. 1, p. 95-107; S. Bentivegna, *op. cit.*

[55]A. Masera, G. Scorza, *Internet, i nostri diritti*, Laterza, 2016, p. 12.

[56]A.M. Gambino, R. Giarda, *L'accesso ad Internet come diritto*, in "MediaLaws", 2021, n. 1, p. 115.

[57]R. Bracciale, *Limiti contemporanei alla cittadinanza: la questione del* digital divide, in M. Aglietti, C. Calabrò (a cura di), "Cittadinanze nella storia dello Stato contemporaneo", Franco Angeli, 2017, pp. 184-185.

[58]A proposito di amministrazione digitale si veda: E. Belisario, *La nuova Pubblica Amministrazione Digitale*, Maggioli, 2009; L. Buccoliero, *Il governo elettronico. Modelli, strategie di innovazione ed elementi di valore per una pubblica amministrazione digitale*, Tecniche Nuove, 2009; L. De Pietro (a cura di), *Dieci lezioni per capire ed attuare l'e-government*, Marsilio, 2011; M. Iaselli (a cura di), *La nuova pubblica amministrazione. I principi dell'Agenda digitale*, Aracne, 2014.

[59]L'art. 3 del CAD dispone che chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti elencati nel CAD anche ai fini dell'esercizio dei diritti di accesso e della partecipazione.

[60]L'art. 3-*bis* del CAD stabilisce che chiunque ha il diritto di accedere ai servizi online offerti dalle amministrazioni pubbliche tramite la propria identità digitale mentre i soggetti di cui all'articolo 2, comma 2, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese, hanno l'obbligo di dotarsi di un domicilio digitale.

[61]L'art. 7 del CAD dispone che chiunque ha diritto di fruire di servizi aggiornati e resi disponibili online dalle amministrazioni pubbliche, per i quali deve essere garantita anche l'espressione del grado di soddisfazione degli utenti.

[62]A.F. Spagnuolo, E. Sorrentino, *Alcune riflessioni in materia di trasformazione digitale come misura di semplificazione*, in "Federalismi.it", 2021, n. 8, pp. 275-287.

[63]I. Korthagen, I. van Keulen, L. Hennen et al., *Le prospettive della democrazia digitale in Europa. Sintesi dello studio*, STOA, febbraio 2018, pp. 10-15.

[64]C. Colacicco, *Carta della cittadinanza digitale fra security e diritti, a che punto è la P.A.*, 5 novembre 2019.

[65]OECD, *Guiding principles for open and inclusive policy making*, su cui si veda: OECD, *Focus on Citizens: Public Engagement for Better Policy and Services*, OECD Publishing, Paris, 2009, p. 19.

[66]Una delle strategie fondamentali individuate dalla Commissione europea è l'interoperabilità delle varie banche dati delle pubbliche amministrazioni, da intendersi come la "capacità delle singole componenti del sistema P.A. di interagire orizzontalmente e verticalmente, ossia di fare rete. L'interoperabilità è infatti la capacità di due o più sistemi di connettersi fra loro e dialogare in forma automatica, scambiando informazioni e condividendo risorse". Si veda, a tal proposito C.M. Arpaia, P. Ferro, W. Giuzio et al., *op. cit.*, p. 27.

[67]C.M. Medaglia, L. Orlando, *Open government e open data: prove tecniche di trasparenza*, in "E-gov", 2011, n. 2, pp. 40-45.

[68]F. Martines, *La digitalizzazione della pubblica amministrazione*, in "MediaLaws", 2018, n. 2, p. 146-157.

Open data for e-democracy

Abstract: The Sars-CoV-2 restrictions have increased people's desire to be active citizens. In this contest digital technologies play a fundamental role. The use of organized, open and freely accessible data, gives the opportunity of implementing a transparent, participatory and collaborative governance; this improves the quality of public services, the accessibility of administrative action and its simplification. In this way it would be possible to strengthen the control of citizens and stakeholders, favoring the transition from e-government to e-democracy. In order to gain this, it's necessary that open data be protected as real common goods.

Keywords: Digital citizenship – e-Democracy – Open data – Digital transformation – Open government

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0074
Articolo sottoposto a peer review

Tutela della salute, sistemi digitali e privacy

Alessandra Pietroletti • Alessandro Nicotra

Le innovazioni e le nuove tecnologie possono contribuire enormemente, nel campo della sanità, a migliorare le cure e la ricerca, ma dovrebbero essere regolamentate sulla base di un processo multistakeholder come quello offerto dall'Internet governance. La trasformazione digitale dei sistemi in campo sanitario richiede una particolare attenzione e sensibilità sotto il profilo della protezione e del trattamento dei dati personali. Occorre costruire un ecosistema digitale funzionale, ma sicuro e rispettoso della dignità e dei diritti delle persone.

Sanità – Privacy – Protezione dati – Nuove tecnologie – Trasformazione digitale

Sommario: *1. Introduzione – 2. L'importanza della Internet governance – 3. Nuove tecnologie e sistemi digitali per la sanità – 3.1. Lo scenario italiano – 3.2. Ecosistema sanitario – 3.3. Le applicazioni – 4. La tutela dei dati personali in ambito sanitario – 4.1. Pandemia, Garante privacy e nuovo FSE – 4.2. Consenso e registro dei trattamenti – 4.3. Nuove tecnologie e valutazioni di impatto – 5.* Cybersecurity *e* data breach

1. Introduzione

Dal WSIS (*World Summit on the Information Society*[1]) del 2005 ad oggi, l'infrastruttura di Internet è cresciuta e si è sviluppata, con i suoi protocolli, trasformandosi in vera e propria spina dorsale non solo della società dell'informazione ma della nostra stessa vita quotidiana. Sarebbe arduo immaginare le nostre vite oggi, senza l'ausilio di tale strumento ed è ormai sotto gli occhi di tutti quanto le questioni legate alla Internet governance[2], che un tempo riguardavano ed appassionavano solo addetti ai lavori o attivisti, non siano più un interesse preminente ed esclusivo delle società di telecomunicazioni, degli innovatori e del mondo accademico. Ecco, quindi, che dal gTLD[3] allo sviluppo dei nomi a dominio, dalle problematiche di accesso all'anonimato, dalle Big tech a *Cambridge Analytica* oggi più che mai l'Internet governance è divenuta anche una questione di privacy, data protection e... salute.

La pandemia di Covid-19 ha reso ancora più evidenti, da un lato, i benefici che possono derivare da una trasformazione digitale dei sistemi anche in campo sanitario, ma dall'altro, ha fatto emergere anche diverse criticità e, con queste, la necessità di adottare nuovi piani e strategie per limitare i danni collaterali che da tale processo di trasformazione possono scaturire. Si pensi, in primo luogo, alla frammentarietà dei database sanitari pubblici (con le Regioni ed il Governo a contendersi le competenze) oppure ancora alle conseguenze dovute a dati mancanti o non esatti.

L'attenzione e la sensibilità verso il funzionamento dei sistemi a tutela della salute devono essere massime. Sono ormai numerosissime, infatti, le innovazioni e le sperimentazioni tecnologiche in ambito sanitario che sfruttano Internet e il digitale, ma che richiedono approfondimenti preliminari e determinate garanzie per i cittadini. Basti pensare alle ricette dematerializzate, alla telemedicina, ai dispositivi in-

A. Pietroletti e A. Nicotra sono avvocati esperti in ICT, privacy e data protection. Sono rispettivamente socio e consulente dello Studio Legale Tributario (EY).

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

dossabili o ai sensori per il monitoraggio remoto dei più svariati parametri di salute dei pazienti. Tutti questi dati, trasposti in digitale, possono essere utilmente inoltrati ai propri medici di riferimento attraverso la rete e possono essere archiviati in un dossier o fascicolo sanitario, ma vanno, in ogni caso, validati e protetti.

Le tecnologie, i sistemi ed i dati attinenti alla Sanità digitale (*eHealth*), per incrementare la loro utilità e protezione, dovrebbero convergere verso la creazione di un ecosistema digitale che, muovendo dalla ricerca (si pensi alla bioinformatica ed al sequenziamento del DNA), possa monitorare e fare arrivare in tempo reale al medico curante i parametri dell'assistito e, magari, curarlo attraverso le terapie digitali (DTx[4]) ovvero interventi terapeutici gestiti da programmi software. Si tenga presente, poi, il parallelo sviluppo di altri programmi decisamente rilevanti sul piano dell'assistenza sanitaria. Ci riferiamo a quelli sviluppati per ottimizzare la logistica e la consegna di farmaci, per lo studio e la produzione dei vaccini, per la gestione dei dispositivi medicali. Ed ancora si pensi alla chirurgia robotica o a quella a distanza, che consentono agli specialisti di operare da remoto e che sono ormai realtà consolidate, ma che necessitano di connessioni stabili e sicure.

Nonostante la sanità sia senz'altro il settore che possa trarre i maggiori benefici dai big data (ad esempio, attraverso la condivisione dei dati scientifici[5]), tutte queste innovazioni, che sono destinate ad una sempre maggiore e migliore tutela della salute, elaborano una quantità enorme di dati sensibili e richiedono, come intuibile, un preciso quadro regolatorio. Non si può che ribadire, quindi, l'importanza che assume il lecito e corretto trattamento di tali dati personali. L'analisi, la valutazione e l'adozione di misure di sicurezza realmente adeguate di dati tanto particolari e sensibili, come sono i dati sanitari, è indispensabile se si vuole evitare che i potenziali benefici offerti dalle tecnologie digitali vengano azzerati da violazioni della dignità e dei diritti delle persone. Fondamentale, in tal senso, si rivela essere il rispetto dei principi della *privacy by default* e della *privacy by design* introdotti dal GDPR ovvero dal Regolamento (UE) 2016/679.

Di fronte al vertiginoso sviluppo delle *big tech companies* e della quantità di dati personali da queste trattati, il GDPR è un prezioso e indispensabile strumento nella ricerca di un punto di equilibrio tra progresso, innovazione, sviluppo economico e rispetto dei diritti delle persone. Per dare un'idea degli interessi che gravitano attorno al settore dell'*eHealth*, si consideri che, in base a una specifica ricerca[6], nel 2016 il mercato dei Big Data nel settore sanitario veniva valutato intorno agli 11 miliardi di dollari, mentre, nel 2020, è stato stimato che tale mercato arriverà a valere 70 miliardi di dollari nel 2025. Non sorprende, dunque, il preoccupante dato che un'altra ricerca ha portato alla luce relativamente al settore sanitario in Italia: nell'ottobre del 2020 l'Italia risultava quarto paese al mondo e primo in Europa per attacchi informatici subiti[7] e il settore più colpito per numero di attacchi davanti, persino, a quello bancario e quello della pubblica amministrazione. Questo dato rende ancora più evidente l'importanza di implementare un piano di governance e data protection sia a livello di reti che di applicativi, cercando di fare tesoro degli incidenti e delle violazioni di dati già occorsi (come, ad esempio, quello subito dalla Regione Lazio nell'agosto 2021 che ne ha bloccato il Ced paralizzando i sistemi digitali regionali e la campagna vaccinale *in primis*) e approntando adeguate procedure di gestione e prevenzione di insidiosi *data breach*.

Al pari di come si sono sviluppati e si sviluppano i protocolli che rendono possibile il funzionamento di Internet, riteniamo che anche per la privacy e la *data protection* siano fondamentali il confronto e la cooperazione tra tutti gli attori coinvolti, secondo un approccio *multistakeholder*. Cercheremo di sintetizzare, qui di seguito, il percorso di alcune delle principali problematiche affrontate in seno agli *Internet Governance Forum* ove sono emersi chiaramente il rapporto e gli intrecci esistenti tra la gestione della rete Internet, l'implementazione di efficaci sistemi di sanità digitale e la necessità di guardare al funzionamento di queste tecnologie anche sotto il profilo della riservatezza e della sicurezza informatiche.

2. L'importanza della Internet governance

Per chi si occupa di Internet da più di vent'anni la tentazione ad indulgere nei ricordi su quale fosse lo spirito e gli ideali dei cd. pionieri della rete e dei suoi primi frequentatori è molto forte. Per comprendere come non sia più l'Internet elitaria, popolata da ricercatori e qualche milione di appassionati, è sufficiente il dato fornito da una ricerca che ha stimato, ad aprile del 2021, in oltre 4,72 miliardi le persone che utilizzano la rete[8]. Come spesso accade con le nuove tecnologie, però, utilizzare non significa conoscere. L'idea di libertà assoluta, di spazio aperto e senza regole, ha ingenerato in molti l'idea che l'Internet sia il *far west*, popolato da hacker cattivi che cospirano nel *dark Web*.

In verità, delle regole di base, per quanto meramente tecniche, sono sempre esistite e si chiamano protocolli. Senza l'accordo e la standardizzazione sui

protocolli[9] la connessione tra reti e dispositivi non sarebbe stata possibile. La realizzazione della *Network neutrality* ha dimostrato, di fatto, quanto siano importanti la trasparenza e l'interoperabilità tra sistemi, soprattutto quando si ha a che fare con l'informatica e le tecnologie digitali. Risulta lapalissianamente disfunzionale, infatti, avere dispositivi che utilizzano "lingue" diverse e non si capiscono fra loro, scambiandosi così documenti o file illeggibili. La neutralità della rete, costantemente messa in discussione da governi autoritari o propensi ad un controllo totale del traffico dati, ha finito in realtà con il favorire lo sviluppo del concetto di neutralità tecnologica al fine di promuovere gli scambi e le comunicazioni transfrontaliere[10].

Reti e dispositivi sono però solo meri mezzi di trasmissione attraverso i quali trasmettere, ricevere o conservare dati ed informazioni. Il problema era ed è "se" e "come" regolare le potenzialità offerte da questi strumenti. Un conto, infatti, è definire uno standard tecnico per la produzione e trasmissioni delle informazioni, altro stabilire limiti, finalità e contenuti dei dati che tali informazioni contengono.

In quest'ottica, dopo il primo boom della new economy nei primi anni del 2000, le Nazioni Unite organizzarono il *World Summit on the Information Society* che produsse una prima dichiarazione di principi[11] che esordiva così: «Noi, rappresentanti dei popoli del mondo, riuniti a Ginevra dal 10 al 12 dicembre 2003 per la prima fase del Vertice mondiale sulla società dell'informazione, dichiariamo il nostro desiderio e impegno comune di costruire una società dell'informazione incentrata sulle persone, inclusiva e orientata allo sviluppo, in cui tutti possono creare, accedere, utilizzare e condividere informazioni e conoscenze, consentendo a individui, comunità e popoli di raggiungere il loro pieno potenziale nel promuovere il loro sviluppo sostenibile e migliorare la loro qualità della vita, sulla base degli scopi e dei principi della Carta delle Nazioni Unite e nel pieno rispetto e sostegno della Dichiarazione Universale dei Diritti Umani. La nostra sfida è sfruttare il potenziale delle tecnologie dell'informazione e della comunicazione per promuovere gli obiettivi di sviluppo della Dichiarazione del Millennio, vale a dire l'eliminazione della povertà estrema e della fame; conseguimento dell'istruzione primaria universale; promozione dell'uguaglianza di genere e dell'emancipazione delle donne; riduzione della mortalità infantile; miglioramento della salute materna; combattere l'HIV/AIDS, la malaria e altre malattie; garantire la sostenibilità ambientale; e lo sviluppo di partenariati globali per lo sviluppo per il raggiungimento di un mondo più pacifico, giusto e prospero...». Nel 2003 poteva far sorridere l'obiettivo di ridurre la mortalità infantile e migliorare la salute materna con le tecnologie dell'informazione e della comunicazione, ma nel 2021 possiamo dire che parte di tali obiettivi è stata effettivamente conseguita[12].

Successivamente, nel WSIS del 2005 a Tunisi, per tentare di dare un seguito concreto a questi principi venne varata la cd. "Agenda di Tunisi per la Società dell'Informazione"[13] che invitava il Segretario Generale delle Nazioni Unite a convocare un forum per il dialogo politico *multistakeholder* denominato *Internet governance Forum* (IGF)[14]. In questi forum, che dal 2006 vengono organizzati ogni anno, si discute sui principali temi correlati alla governance di Internet.

La gestione internazionale di Internet, secondo il mandato originario e la dichiarazione di principi, dovrebbe essere multilaterale, trasparente e democratica, con il pieno coinvolgimento dei governi, del settore privato, della società civile e delle organizzazioni internazionali. Dovrebbe inoltre facilitare l'accesso per tutti e garantire un funzionamento stabile e sicuro di Internet, tenendo conto del multilinguismo. Di fatto, purtroppo, l'attenzione e la partecipazione dei governi a questi forum è divenuta nel tempo in gran parte velleitaria o di facciata. La scarsa promozione di tali eventi si è riflettuta a cascata sulla società civile, ovvero sui comuni cittadini che, non avendone magari notizia non si attivavano per la partecipazione o per farsi rappresentare (salve fortunatamente le presenze da parte di organizzazioni non governative e no profit quali ad esempio l'*Electronic Frontier Foundation*[15], ISOC Italia[16], ISOC.org[17] e molte altre) riducendo le effettive potenzialità ed i molti vantaggi in termini di conoscenza e di proposte che di solito conseguono a questi incontri.

La pandemia scoppiata all'inizio del 2020, però, imponendo tra le priorità politiche dei governi la *digital transformation* e la transizione dei servizi verso il digitale ha avuto l'effetto di ridare all'*Internet Governance Forum* una certa visibilità e di rendergli parte della sua centralità come sede deputata per la discussione ed il confronto sul futuro della rete e lo sviluppo di Internet. A dimostrazione di quanto affermato, il quindicesimo IGF tenutosi interamente online dal 2 al 17 novembre 2020 ha avuto come tema centrale l'*Internet for human resilience and solidarity* e ha registrato una partecipazione straordinaria. Anche l'IGF 2021, tenutosi anche in presenza oltre che online, è stato seguito da numerose persone facendo ben sperare, soprattutto per la forte convergenza che si è avuta tra gli argomenti in discussione nelle varie sezioni tematiche e gli obiettivi fissati con l'*Agenda 2030 per uno sviluppo sostenibile*[18]. Quest'ultima, sottoscritta nel settembre 2015 dai governi dei 193 paesi membri dell'ONU, ci inte-

ressa in particolare, perché tra i 17 obiettivi di sviluppo sostenibile (OSS/SDGs, *Sustainable Development Goals*) ha inserito specificamente quello di "Assicurare la salute ed il benessere per tutti e per tutte le età"[19]. Un obiettivo apparentemente utopistico, ma averlo fissato e sottoscritto formalmente lascia intendere che da più parti si proverà effettivamente a muoversi in tale direzione. Lo stesso Segretario delle Nazioni Unite, Antonio Guterres, ha sottolineato in più occasioni l'importanza di "fare rete", di cooperare, di innovare, ponendo l'attenzione sulla rete come infrastruttura e sulla pandemia come occasione per l'implementazione di piani di *eHealth*.

Lo sviluppo e l'attuazione di strategie e politiche sanitarie è stato un tema centrale e un argomento molto dibattuto nell'IGF del 2020. In quella sede, infatti, è stato rimarcato come ogni paese dovrebbe sfruttare le nuove tecnologie e la rete impegnandosi nell'adozione di una vera e propria strategia digitale nazionale. E tale strategia dovrebbe essere calibrata attentamente sui bisogni delle persone, sulle condizioni esistenti, sulle capacità e risorse disponibili e sugli obiettivi desiderati. Studiosi ed esperti hanno convenuto sul fatto che la definizione di una strategia nazionale facilita, di fatto, l'adozione di progetti ed azioni concrete per migliorare la tutela della salute. In primo luogo, perché tale approccio richiede una preventiva analisi ed indagine sui reali bisogni e, in secondo luogo, perché permette di mettere a fuoco le priorità di intervento. Un siffatto approccio, inoltre, avrebbe come effetto non secondario anche quello di incrementare progressivamente l'affidabilità dei sistemi e dei piani di prevenzione e, con essi, la fiducia e le possibilità delle persone nel fruirli. Chiaramente, l'elaborazione di una strategia per la sanità digitale e le relative azioni richiedono un forte investimento in infrastrutture, nell'alfabetizzazione informatica ed in competenze digitali: problemi da affrontare con partnership pubblico-privato. Del resto, solo connettendo in modo significativo ed efficace le persone, i servizi e gli strumenti sanitari digitali si può pensare di procedere concretamente verso l'ambizioso obiettivo, sopra ricordato, di "Assicurare la salute ed il benessere per tutti e per tutte le età".

Una precondizione è stata però individuata nel guadagnare e mantenere la fiducia degli utenti. In più panel si è rimarcato quanto sia essenziale poter contare su una regolamentazione di Internet che ne garantisca il funzionamento, l'interoperabilità e l'accessibilità. Tali caratteristiche sono indispensabili per l'implementazione di sistemi di sanità digitale che siano realmente efficaci e che abbiano successo. Un successo che non può prescindere da interventi normativi specifici. Da più parti, infatti, è stata segnalata la necessità che la politica ed i legislatori, nel rispetto dei diritti e delle libertà di tutti gli attori, definiscano meglio il quadro delle regole e stabiliscano affidabili meccanismi di convalida e di verifica delle tecnologie destinate alla prevenzione ed alla tutela della salute. Cosa, per esempio, può essere considerato dispositivo medico? Chi lo certifica come tale? Quanto è legittima la raccolta di big data e la profilazione da parte di soggetti privati e commerciali? Quali tutele e protezioni possono considerarsi adeguate?

Il funzionamento stesso di sistemi e applicazioni dovrebbe essere quanto meno trasparente ed occorre renderli accessibili e semplici da usare, in modo da garantire anche un controllo diffuso, non solo da parte di autorità o agenzie all'uopo preposte, ma anche da parte di singoli appassionati ed esperti.

Se si vuole garantire che più persone abbiano accesso a prestazioni e servizi sanitari migliori e più efficienti, la digitalizzazione dei sistemi sanitari deve diventare una priorità in tutto il mondo. E le azioni da intraprendere non riguardano solo gli investimenti e piani strategici... Non vanno infatti ignorate altre precondizioni essenziali quali: il diritto di accesso alla rete, il contrasto al divario digitale, la lotta alla disinformazione sanitaria ed alla disinformazione in generale (le cd. fake news[20]). Occorre, infine, una maggiore sensibilizzazione e responsabilizzazione delle singole persone. Dopo tutto, i social network e la rete sono sempre stati, nel bene e nel male, uno specchio del mondo reale e rimangono degli strumenti da saper utilizzare. Tutte le proposte ed i progetti ideati e portati avanti per creare fonti di informazione e di condivisione affidabili sono, in definitiva, orientati ad aiutare le persone a scegliere, liberamente e con cognizione di causa, in chi aver fiducia ed a filtrare lo tsunami di informazioni cui hanno accesso.

3. Nuove tecnologie e sistemi digitali per la sanità

Occorre alimentare una cultura digitale che, per formarsi, ha comunque bisogno di verifiche empiriche. Oggi assistiamo a persone che per curarsi si affidano indiscriminatamente ai motori di ricerca sul Web o ai social network ed è del tutto evidente quanto sia necessaria un maggior spirito critico circa le fonti e le informazioni consultate o, per esempio, su che fine facciano i propri dati sanitari immessi nelle app dello smartphone o pubblicati in rete.

Guardando alla storia della medicina[21], è possibile constatare come solo negli ultimi due secoli le procedure mediche abbiano iniziato a fondarsi su conoscenze e metodologie in grado di rendere le cure

più sicure ed efficaci per tutti. Negli ultimi vent'anni l'informatica ha accelerato esponenzialmente queste procedure grazie all'aumento della capacità e della velocità di elaborazione dei dati che ha permesso di introdurre e sperimentare nuove metodologie e nuove tecnologie. Parlare di algoritmi, robot ed intelligenza artificiale applicati alla sanità non è più fantascienza, ma una realtà consolidata ed imprescindibile, destinata a espandersi ed a svilupparsi ulteriormente negli anni a venire. Un esempio concreto, a questo riguardo, ci è stato dato durante la pandemia di Covid-19 con l'approntamento di appositi vaccini. Normalmente la produzione e la commercializzazione di un nuovo vaccino richiedono anni[22]. Si consideri che il vaccino sviluppato più velocemente, nel passato, è stato quello contro la parotite, realizzato, negli anni '60, in quattro anni[23] (dal sequenziamento virale all'approvazione finale). Per fronteggiare il Covid-19, invece, in meno di un anno si è assistito allo sviluppo di oltre 200 potenziali vaccini, di cui 5, dopo aver completato le diverse fasi di sperimentazione e controlli, sono risultati pronti per l'uso. Un risultato straordinario reso possibile dalle ingenti risorse economiche messe a disposizione dei ricercatori e dagli interessi in gioco, certo, ma anche e soprattutto grazie ad un processo di sviluppo e di elaborazione dei dati preesistenti e condivisi a livello globale. Con i vaccini anti-Covid, «nessuna tappa del processo è venuta meno, grazie al concorso di diversi fattori:

- ricerche già condotte in passato sulla tecnologia a RNA messaggero (mRNA);
- studi sui coronavirus umani correlati al SARS-CoV-2, per esempio quelli che hanno provocato SARS (Severe acute respiratory syndrome) e MERS (Middle East respiratory syndrome);
- ingenti risorse umane ed economiche messe a disposizione in tempi stretti;
- conduzione parallela delle varie fasi di valutazione e di studio;
- produzione del vaccino parallelamente agli studi e al processo di autorizzazione;
- ottimizzazione della parte burocratica/amministrativa;
- valutazione da parte delle agenzie regolatorie dei risultati ottenuti, man mano che questi venivano prodotti (rolling review) e non, come generalmente si usa fare, solo dopo il completamento di tutti gli studi»[24].

Poter elaborare digitalmente e sinergicamente tutti i dati relativi a ricerche e studi condotti in precedenza e poterli verificare e valutare telematicamente, in tempo reale, rappresenta una dimostrazione lampante dei benefici che possono derivare dalla cd. *digital transformation*. Una vera e propria rivoluzione che avviene modificando le modalità di trattamento del dato biologico e sanitario; modalità che, da analogiche e cartacee, non solo diventano digitali ma vengono elaborate da algoritmi sempre più complessi sino ad arrivare a strabilianti applicazioni di intelligenza artificiale come dimostrato dal progetto *Alphafold*: un software creato dalla Deepmind per la previsione della struttura delle proteine (CASP), usato anche in uno studio per predire le strutture delle proteine di SARS-CoV-2, l'agente eziologico di Covid-19.

Come già accennato, tutto questo è reso possibile sia dalla velocità di elaborazione dei nuovi processori, sia dalla straordinaria quantità di dati disponibili. Attraverso la progressiva ed incrementale trasformazione digitale in corso si assiste ad una accelerazione negli studi e nelle ricerche di nuove terapie e di migliori cure, si possono offrire nuovi servizi ed erogarli telematicamente con notevole risparmio di risorse e dei costi (anche ambientali) legati agli spostamenti. Chiaramente, una simile trasformazione non è immediata e mondo accademico ed esperti sono unanimi nel sottolineare quanto sia indispensabile un'adeguata programmazione: occorre, giova ribadirlo ancora una volta, che i governi si dotino di un piano di sviluppo strategico che consenta di superare problemi culturali, problemi di connessione e di accesso ovvero il già citato *digital divide*. Per restare in ambito salute, poi, serve nello specifico una governance che regolamenti l'uso delle nuove tecnologie e dei dati sanitari digitalizzati per evitare futuri distopici nei quali tali informazioni anziché avvantaggiare le persone le discriminino.

3.1. Lo scenario italiano

L'Italia, grazie ai suoi ricercatori ed imprenditori, può legittimamente annoverarsi tra le prime nazioni ad avere contribuito alla diffusione dell'informatica (si veda la storia di Olivetti) ed allo sviluppo della rete (si veda lo straordinario archivio sull'Internet italiano a cura del compianto Giorgio Giunchi[25]. La politica ed i legislatori hanno, però, dovuto sempre inseguire poiché innovazioni e tecnologie evolvono più velocemente della possibilità e della capacità di regolamentarle. Negli ultimi trenta anni si è assistito ad un susseguirsi di leggi, decreti, circolari in materia di informatica e telecomunicazioni: un dedalo di norme nel quale anche gli esperti a volte faticano a districarsi. Basta guardare all'originaria identificazione obbligatoria per sottoscrivere un abbonamento ad Internet, all'istituzione della Posta Elettronica Certificata e la sua evoluzione con relativi registri pubblici ed assunzione a domicilio digitale, alle firme

e certificati digitali ed alla conservazione sostitutiva, oppure ancora al baluardo rappresentato dal Codice dell'amministrazione digitale, modificato e integrato più volte dal suo varo con il d.lgs. 7 marzo 2005, n. 82, alla fatturazione elettronica, ai provvedimenti per alterare i DNS ed oscurare siti... Anche il percorso degli organismi creati dal nostro Governo per lo sviluppo e la regolamentazione del digitale è stato piuttosto travagliato: quanti si ricordano dell'Autorità per l'informatica nella pubblica amministrazione (AIPA) istituito nel febbraio del 1993 e le cui competenze furono parzialmente ereditate dal Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA)? Da notare che il CNIPA venne istituito dall'art. 176 del d.lgs 30 giugno 2003, n. 196 (il Codice italiano per la protezione dei dati personali) in sostituzione dell'Autorità per l'informatica nella pubblica amministrazione (AIPA), della quale conservava le attribuzioni. Il CNIPA si trasformò in DigitPA per confluire, poi, nell'attuale Agenzia per l'Italia Digitale (AgID).

Paradossalmente, proprio l'emergenza pandemica, ha dato ulteriore impulso allo sviluppo ed alla regolamentazione della sanità digitale. Ai contenuti del *Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022*[26], infatti, si è aggiunto quanto previsto dal *Piano Nazionale di Ripresa e Resilienza*[27]. I punti salienti per quanto riguarda l'attuale Piano Triennale in ambito salute riguardano l'implementazione del FSE (Fascicolo sanitario elettronico), dei CUP (Centri unici di prenotazione) e dei progetti di telemedicina, mentre gli obiettivi fissati dal PNRR Salute[28] sono ancora più ambiziosi: «potenziare la capacità di prevenzione e cura del sistema sanitario nazionale a beneficio di tutti i cittadini, garantendo un accesso equo e capillare alle cure e promuovere l'utilizzo di tecnologie innovative nella medicina».

L'auspicio è che si riesca a passare da progetti sperimentali e scollegati tra loro ad un vero e proprio ecosistema sanitario all'interno del quale poter sfruttare tutti i collegamenti possibili tra le varie banche dati, usando le migliori tecnologie disponibili ed implementando una solida governance che oltre alla salute tuteli anche la sicurezza ed il trattamento dei dati.

3.2. Ecosistema sanitario

La creazione di un ecosistema sanitario vede come attori principali il Ministero della Salute, il Ministero dell'Economia e delle Finanze, il Garante per la protezione dei dati personali, AgID ed ovviamente gli ospedali, i laboratori, le case di cura ed i cittadini. La finalità principale è quella di arrivare all'adozione di soluzioni e di azioni finalizzate a migliorare i servizi sanitari, limitare gli sprechi e le inefficienze, migliorare il rapporto costo-qualità dei servizi sanitari e garantire a tutti i cittadini le medesime possibilità di cura e di accesso ai servizi riducendo le differenze tra i territori[29]. Vanno considerati come parte integrante di questa piattaforma anche i servizi relativi all'identità (CIE, SPID) ed ai pagamenti digitali (PagoPA) che consentono di accedere ai propri dati e di pagare quanto dovuto per le prestazioni fruite.

Senza avventurarci troppo nei dettagli dei singoli progetti, la cui documentazione comunque è facilmente reperibile in rete[30], possiamo affermare che il sistema di base prevede che il cittadino sia dotato della Tessera sanitaria (TS) che abilita all'accesso delle prestazioni sanitarie erogate dal Servizio Sanitario Nazionale. La TS è strutturalmente connessa al codice fiscale ed a questo viene associato per ciascun individuo un fascicolo sanitario elettronico. Quest'ultimo è lo strumento attraverso il quale il cittadino può tracciare, consultare e condividere la propria storia sanitaria.

La base dati costituita da TS e FSE rende possibili ulteriori implementazioni dell'ecosistema quali l'adozione di un sistema centralizzato informatizzato per la prenotazione unificata delle prestazioni (il CUP) e la dematerializzazione di referti e ricette, che possono essere archiviati e resi direttamente accessibili ai cittadini attraverso diversi canali telematici. Questi dati, tra l'altro, essendo digitalizzati possono essere riutilizzati per diverse finalità e con diverse modalità, purché lecite e conformi alla normativa vigente sulla protezione dei dati personali. Anche per i cittadini la situazione critica della pandemia ha determinato un impulso a dotarsi delle conoscenze e degli strumenti necessari per beneficiare dei servizi sanitari a distanza: non solo sono aumentati esponenzialmente gli accessi telematici ai referti e le ricette dematerializzate, ma si sono avute anche le prime sperimentazioni di tele-visite. L'integrazione e l'interoperabilità di tutte queste piattaforme non è cosa semplice, sia per quanto riguarda gli aspetti tecnici che per quelli legati alla riservatezza, come si è visto in occasione degli applicativi utilizzati per gestire la prenotazione dei vaccini o di quelli creati per il Green Pass e financo per il tracciamento e per avvertire gli utenti che avessero avuto un'esposizione a rischio (app Immuni[31] era stata creata per acquisire e visualizzare la Certificazione verde COVID-19).

3.3. Le applicazioni

In molte strutture ospedaliere si utilizzano già oggi dispositivi certificati che consentono il tele-

monitoraggio ovvero l'osservazione a distanza dello stato di salute dei pazienti assistiti, grazie a dispositivi di misurazione integrati, interfacciati tramite apposite applicazioni con il personale medico. Le evidenze dei benefici dati dalla telemedicina sono evidenti da anni[32], ma lo sviluppo e la diffusione delle sottostanti tecnologie, che la rendono possibile, richiedono un quadro normativo che fatica a delinearsi. Accanto alle sperimentazioni di alcuni ospedali e centri di ricerca od alle iniziative istituzionali di applicazioni per cellulari quali Immuni, quella del Fascicolo Sanitario Elettronico e quella dei servizi pubblici IO, non bisogna dimenticare il fenomeno legato alla diffusione di dispositivi *wearable* e della miriade di applicazioni sviluppate per monitorare la salute o l'attività fisica: la cosiddetta *mobile health* (*mHealth*).

Molti dei più diffusi dispositivi cellulari sono ormai in grado di rilevare battito cardiaco, pressione, quantità e qualità del sonno, ossigenazione, ed i loro applicativi possono essere integrati con altri dati inseriti dagli utenti o acquisiti via Bluetooth da altri dispositivi quali: peso, consumo calorico, glicemia, ciclo mestruale e tutta una serie di altri parametri per monitorare il proprio stato di salute. Per quanto in tutte queste applicazioni in uso sugli smartphone siano presenti precise avvertenze sulla tutela della privacy e su come i parametri rivelati non siano certificati né possano costituire una vera e propria diagnosi, non sfuggirà ai più che le modalità di utilizzo e di controllo di questi dispositivi e di queste app siano totalmente rimesse ai singoli utenti. In assenza di una diffusa cultura digitale e di una maggiore consapevolezza degli utenti è praticamente impossibile determinare il giusto compromesso tra benefici e rischi, fra tutela della salute e corretto trattamento dei propri dati personali[33]. Se da un lato abbiamo app in grado di rivelare aritmie o cadute e di salvare così delle vite, dall'altro abbiamo delle app studiate per facilitare la diagnosi delle malattie che potrebbero indurre a sentirsi tranquillizzati a fronte di una previsione o diagnosi errata. Ritorna qui il tema della fiducia e delle fonti affidabili, emerso anche nel corso di vari panel degli IGF, sia sotto il profilo della certificazione di software e dispositivi, sia sotto il profilo delle garanzie necessarie al loro corretto trattamento ai fini della privacy. Uno spiraglio lo si sta intravedendo grazie al diffondersi del principio della *Evidence Based Medicine* ovvero di un utilizzo verificato e verificabile delle risultanze dei dati raccolti attraverso i diversi dispositivi ed alle discussioni sui modelli predittivi che possono, chiaramente, avere effetti eterogenei su soggetti diversi[34].

4. La tutela dei dati personali in ambito sanitario

Al centro di tutto quanto sinora illustrato vi è il dato personale di carattere sanitario ovvero una particolare categoria di dato considerato molto sensibile in quanto in grado di rivelare lo stato di salute con potenziali conseguenze dirette sulla libertà, sulla dignità e nella vita concreta delle persone. A distanza di quasi vent'anni sono ancora di straordinaria attualità le parole di Stefano Rodotà (di cui consigliamo la lettura integrale al link in nota[35]) nel suo intervento del 2004 alla ventiseiesima Conferenza internazionale sui commissari per la protezione dei dati e la privacy: «Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro. [...] Emerge un legame profondo tra libertà, dignità e privacy, che ci impone di guardare a quest'ultima al di là della sua storica definizione come diritto ad essere lasciato solo. Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale dalla società dell'eguaglianza. [...] Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo, diventa così evidente che: la privacy è uno strumento necessario per difendere la società della libertà, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale».

Ogni volta che viene messa in dubbio l'importanza della privacy o la si voglia considerare una cosa astratta e secondaria andrebbero rilette le parole sopra riportate. Ancora oggi, purtroppo, molti vedono la tutela della riservatezza come un farraginoso e fastidioso orpello che ostacola il libero mercato e la stessa azione della pubblica amministrazione. Il periodo pandemico è stato abbastanza eclatante sotto questo aspetto ed ha messo a dura prova il Garante italiano, tutti i *data protection officer* (DPO) e quanti si occupano della materia professionalmente o per motivi di studio e ricerca. La situazione di emergenza ha indotto molti, persino a livello legislativo, a ritenere che, in nome della tutela alla salute, si potesse e si dovesse mettere in secondo piano la tutela dei dati personali.

A questo riguardo, vale la pena ricordare come la normativa dettata del Regolamento UE 2016/679[36] meglio noto come GDPR (*General Data Protection Regulation*) abbia riconosciuto e sancito che la protezione delle persone fisiche con riguardo al trattamen-

to dei dati di carattere personale sia un diritto fondamentale. Ma ha anche precisato come tale diritto non sia assoluto, ma vada considerato alla luce della sua funzione sociale e vada contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (considerando 1 e 4 del GDPR). Più che creare una contrapposizione o invocare una scelta tra la tutela della salute e quella della privacy, occorre cimentarsi in un'operazione di costante bilanciamento tra valori e diritti: diversi, ma ugualmente fondamentali. Vanno lette in quest'ottica alcune delle principali problematiche verificatesi ed affrontate durante il periodo pandemico e riportate brevemente di seguito.

4.1. Pandemia, Garante privacy e nuovo FSE

L'individuazione o la realizzazione, via via, di specifiche piattaforme software per gestire la prenotazione e l'erogazione dei vaccini, per tenere traccia dei contatti, oppure ancora per ricevere ed aggiornare il cd. Green Pass ha sollevato diversi problemi operativi ed infinite discussioni sotto il profilo delle funzionalità, della protezione dei dati e della tutela della riservatezza.

Non si vuole entrare qui nel merito di politiche e scelte legislative, ma solo sottolineare alcune peculiari criticità che si sono verificate. È il caso, per esempio, di soggetti fragili che avrebbero avuto diritto a prenotarsi per la vaccinazione e non hanno potuto farlo in prima battuta a causa di database incompleti e di piattaforme poco flessibili. Vi sono stati poi casi in cui la non esattezza dei dati riguardanti i codici fiscali ha portato a mancate certificazioni o scambio di identità nei referti di positività al virus e a tanti altri disguidi. Mai come in questo caso è diventato evidente quanto il trattamento dei dati personali possa incidere sulle libertà e nella vita quotidiana degli individui e di quanto siano importanti i principi declinati, in particolare, dall'art. 5 del GDPR sulla minimizzazione, esattezza e conservazione dei dati personali.

Altrettanto lungimirante si è rivelato il regolamento europeo laddove ha introdotto con i commi 4 e 5 dell'art. 36 un obbligo di consultazione preventiva delle Autorità garanti da parte dei singoli legislatori europei per tutti gli atti legislativi o regolamentari che incidano sul trattamento di dati personali: «4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento» e «5. ... il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica».

Di fronte all'emergenza medica, al grande impegno del personale sanitario è corrisposto pari impegno, non sempre compreso, da parte del Garante Privacy e dei responsabili per la protezione dei dati personali per salvaguardare diritti e riservatezza degli interessati, ma anche per ridurre i rischi e le responsabilità connesse al trattamento di dati tanto sensibili.

Durante l'emergenza pandemica il Garante della privacy italiano è dovuto intervenire più volte[37] e su più fronti: un'attività poderosa, non sempre compresa o accettata di buon grado.

Uno dei progetti che verrà sostenuto e finanziato dal PNRR Salute è la messa a punto del nuovo Fascicolo Sanitario Elettronico, che sarà basato su un repository centrale HL7 FHIR[38] per la gestione dei dati strutturati oltre che sul protocollo XDS[39] per i documenti. Un progetto molto complesso che richiederebbe una discussione allargata (sul modello IGF) con tutti gli stakeholder ed il coinvolgimento di diverse professionalità, cominciando proprio dai medici, e che dovrà senz'altro coinvolgere il Garante per le implicazioni legate alla sicurezza ed alla protezione dei dati personali[40].

Si deve prendere atto che, se le finalità perseguite con il trattamento dei dati personali sono spesso nobili ed importanti, non si deve mai ignorare, però, il come i dati vengano elaborati. È di fondamentale importanza valutare l'intero ciclo di vita dei dati, dalla raccolta alla cancellazione/distruzione, affinché questo avvenga lecitamente e nel rispetto delle cautele e della normativa dettate in materia di privacy e *data protection*. Il sistema che si vuole adottare prevede la geolocalizzazione? I dati che tratta sono tutti necessari per le finalità che ci si propone? È stata definita la base giuridica che rende legittimo il trattamento? Chi avrà accesso al sistema viene autorizzato, tracciato e (in)formato sui vincoli a tutela della riservatezza degli interessati? Si prevede di comunicare i dati a terzi o che propri fornitori/collaboratori esterni vi abbiano accesso? Il sistema è *on premise* o in cloud e adotta misure di sicurezza adeguate? È previsto trasferimento dati diretto od indiretto all'estero? Per quanto tempo i dati verranno conservati ed è stata messa a disposizione degli interessati un'informativa dettagliata e completa? Queste sono solo alcune delle domande e degli adempimenti che si devono affrontare per una corretta governance ed una reale tutela di tutti i diritti dei cittadini.

4.2. Consenso e registro dei trattamenti

Va ribadito, una volta per tutte, che le finalità di cura non necessitano di consenso e che il consenso informato è cosa diversa dal consenso privacy. Il consenso informato riguarda il trattamento sanitario ed il tipo di cure, il consenso privacy attiene all'autorizzazione a che i propri dati possano essere trattati per le finalità indicate nell'informativa. I dati relativi alla salute, i dati genetici e biometrici, possono del pari essere lecitamente trattati per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria e per finalità sociali quali la gestione dei servizi sociosanitari, nonché per motivi di interesse pubblico nel settore della sanità pubblica. Discorso diverso per tutte le altre finalità che richiedono l'esplicita espressione di apposito e libero consenso.

L'inserimento di dati, ovvero l'alimentazione del Fascicolo Sanitario Elettronico, per esempio, richiedeva il consenso. Nel 2020, poi, al fine di accelerare l'attivazione e l'utilizzo del FSE da parte di tutti gli assistiti, l'articolo 11 del d.l. 19 maggio 2020, n. 34 ha previsto che l'alimentazione del fascicolo avvenga in maniera automatica eliminando la necessità di ottenere il consenso[41]. Sul punto, però, il Garante, che già si era espresso favorevolmente nel 2019 quando aveva fornito dei primi importanti chiarimenti sull'applicazione del GDPR nel trattamento dei dati relativi alla salute in ambito sanitario[42], ha stabilito che, al fine di garantire i diritti degli interessati, venisse effettuata un'adeguata campagna informativa a livello nazionale e regionale e che venisse comunque garantito di poter esercitare il diritto di opposizione all'alimentazione del FSE con i dati sanitari generati da eventi clinici anteriori alla nuova norma, entro un termine prestabilito, non inferiore a 30 giorni.

Non va sottaciuto, però, quanto sia complessa la concreta applicazione del GDPR e l'elaborazione di misure tecnico-organizzative pienamente conformi al Regolamento all'interno delle strutture che caratterizzano il nostro Sistema Sanitario Nazionale (SSN). L'esperienza sul campo ci ha dimostrato quanto siano importanti le competenze, le risorse, la buona volontà e la formazione di tutti i soggetti coinvolti ai quali, spesso, difetta il tempo. Eppure, nonostante l'ostacolo e le urgenze dettate dalla pandemia, abbiamo personalmente constatato un generale e notevole innalzamento della sensibilità e dell'attenzione nella tutela della riservatezza delle persone.

Una vera e propria pietra angolare nel costante percorso di adeguamento alla normativa vigente si è rivelato essere il registro dei trattamenti che, previa adeguato *assessment*, permette di fotografare quali dati vengano raccolti e trattati, da quali unità operative, per quali finalità e con quali misure di sicurezza, censendo anche i fornitori ed i relativi contratti in essere. Un registro organizzato, completo ed aggiornato correttamente rende molto più semplice la messa a punto di adeguate procedure e l'introduzione di un sistema di gestione della privacy sia dal punto di vista documentale (incarichi, nomine, informative, regolamenti interni, etc.), sia dal punto di vista tecnico ed organizzativo (chi fa cosa e con quali strumenti). Per un DPO o responsabile della protezione dei dati la stessa gestione di un *data breach* non sarebbe possibile nella finestra di tempo prevista dall'ordinamento (72 ore) senza i riferimenti contenuti nel registro.

4.3. Nuove tecnologie e valutazioni di impatto

Abbiamo già osservato come la sanità strizzi l'occhio alle nuove tecnologie. Riteniamo opportuno, però, seppur brevemente, mettere in guardia dall'ideazione e dall'avvio di progetti o di sperimentazioni che non tengano in debito e preventivo conto della tutela dei dati personali. Introducendo i principi di *privacy by default* e *privacy by design* il GDPR ha giustamente imposto che nessun trattamento di dati personali avvenga senza che ne sia stato valutato il rischio e senza che siano state adottate adeguate misure di sicurezza.

«Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l'autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti – cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato»[43].

Quanto sopra non deve essere visto come un freno all'innovazione o alla possibilità di cambiare il modo di erogare determinati servizi, è invece una doppia tutela sia per gli interessati, i cui dati si intendono trattare, sia per gli stessi titolari dei trattamenti che, in base al principio dell'accountability, devono essere in grado di dimostrare che le misure di sicurezza da loro adottate sono "adeguate", se non vogliono andare incontro a responsabilità e sanzioni.

5. *Cybersecurity* e *data breach*

Merita, da ultimo, un capitolo a parte il tema della sicurezza informatica dei dati personali in grado di

rivelare lo stato di salute trattati da ospedali, centri di cura, laboratori, centri vaccinali, pubbliche amministrazioni, case farmaceutiche e da tutti gli attori del sistema sanitario.

In generale, il principio di accountability introdotto dal GDPR ha correttamente spostato l'attenzione da mere check list di adempimenti (approccio formale) alle indicazioni contenute negli artt. 24-25 e 32 del Regolamento: titolare e responsabili del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato ai rischi e, in particolare, a quelli che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (approccio sostanziale). Un adeguato livello di sicurezza non potrà prescindere da una verifica costante delle misure di sicurezza approntate rispetto allo "stato dell'arte", anche in considerazione della rapida evoluzione tecnologica. E nel caso di trattamenti di dati sanitari, il livello di sicurezza dovrà sempre essere il più elevato possibile, specie qualora si trattino dati genetici o dati biometrici.

All'interno del summenzionato art. 32 del GDPR vengono indicate, a titolo esemplificato, alcune misure di sicurezza quali la pseudonimizzazione e la cifratura dei dati personali. Altro strumento indispensabile per la conformità alla normativa vigente in materia di protezione dei dati personali sono le linee guida, le raccomandazioni e le *best practices*[44] pubblicate dallo *European Data Protection Board* (EDPB) Comitato europeo per la protezione dei dati, che è composto da rappresentanti delle autorità nazionali per la protezione dei dati dell'UE e dal Garante europeo della protezione dei dati. Dal punto di vista tecnico, invece, il punto di riferimento e di supporto nella definizione delle misure di sicurezza è dato dall'ENISA[45], l'Agenzia dell'Unione europea per la cybersecurity dedicata al raggiungimento di un livello, comune ed elevato, di sicurezza informatica in tutta Europa. Da segnalare che l'ENISA aveva pubblicato già nel 2017 delle linee guida tecniche per l'attuazione delle misure minime di sicurezza per i fornitori di servizi digitali[46] e messo a disposizione, agli inizi del 2020, un tool per valutare il livello di rischio nei trattamenti dei dati personali[47]. Di ancora maggiore interesse, però, sono le iniziative prese da ENISA nello specifico ambito salute: ha infatti lanciato l'*Health Security Experts Group*[48] per garantire la sicurezza e la resilienza del settore sanitario in Europa, ha pubblicato le linee guida per gli appalti per la sicurezza informatica negli ospedali[49] e uno strumento online per aiutare le organizzazioni sanitarie a identificare rapidamente le linee guida più rilevanti per il loro contesto di approvvigionamento, come i beni acquistati o le relative minacce[50] ed ha pubblicato un rapporto sulla sicurezza cloud per i servizi sanitari nel gennaio 2021. L'ENISA, inoltre, organizza ciclicamente l'*eHealth Security Conference* per discutere temi essenziali di cybersecurity per il settore sanitario[51].

A completare il quadro non si può non citare anche la direttiva (UE) 2016/1148[52], meglio nota come direttiva NIS (*Network and Information Security*) che concerne le misure per garantire un livello comune ed elevato di sicurezza delle reti e dei sistemi informativi in tutta l'Unione europea. Nel recepirla con il d.lgs. 18 maggio 2018, n. 65, sono stati individuati cinque Ministeri (sviluppo economico, infrastrutture e trasporti, economia, salute e ambiente) presso i quali sono state designate le "Autorità competenti NIS". Il Ministero della Salute che è Autorità competente NIS per l'attività di assistenza sanitaria, prestata dagli operatori dipendenti o incaricati dal Ministero o convenzionati con il medesimo, ha poi individuato degli Operatori di Servizi Essenziali (OSE), ovvero soggetti i cui servizi dipendono dalla rete e dai sistemi informativi e per i quali un incidente avrebbe effetti negativi rilevanti sulla fornitura di tali servizi. Questi ultimi sono secretati, hanno degli obblighi particolari in materia di sicurezza e di notifica degli incidenti e devono seguire delle apposite linee guida basate sul Framework nazionale per la cyber security e la data protection.

Purtroppo, i numerosi *data breach* informatici occorsi hanno dimostrato che, pur in presenza di procedure e politiche per la gestione delle informazioni, il fattore umano risulta sempre determinante. Anche per questo continue procedure di *assessment*, formazione ed audit sono indispensabili così come il supporto di team e professionisti esperti in IT, sicurezza informatica e protezione dei dati.

Concludendo, una delle sfide più grandi, in termini di governance, è quella di riuscire a rendere Internet ed i sistemi per la tutela della salute più sicuri ed affidabili, mantenendoli però aperti, interoperabili ed accessibili, tramite una riduzione del divario digitale e l'aumento di fonti *trustable*, ovvero affidabili, senza con ciò sottovalutare la tutela della privacy degli utenti.

Note

[1] World Summit on the Information Society (WSIS), Geneva 10-12 December 2003, and Tunis 16-18 November 2005.

[2] Ministero dello sviluppo economico, *Internet Governance e Attività Internazionali*.

[3]V. L. Abba, A. Nicotra, *Generic Top Level Domain di Internet*, in "Informatica e diritto", 2006, n. 1, pp. 125-147.

[4]Le *Digital Therapeutics*, abbreviato all'americana DTx, sono terapie digitali basate su software ed algoritmi che prendono la forma di videogiochi, sensori o realtà virtuale ed agiscono sia come terapia comportamentale sia come cura specifica per determinate patologie. Si tratta di vere e proprie terapie che necessitano di prescrizione medica e devono essere accompagnate da adeguate istruzioni, esattamente come coi farmaci.

[5]Si veda il progetto per l'hosting e l'elaborazione dei dati della ricerca a sostegno della scienza dell'UE varato con lo *European Open Science Cloud* (EOSC).

[6]*Global healthcare big data market size in 2016 and a forecast for 2025*.

[7]Anitec-Assinform, *Italia quarta al mondo e prima in Europa per attacchi Malware*.

[8]S. Kemp, *Digital 2021 April Global Statshot Report*, 21 April 2021.

[9]*Reti di calcolatori. Protocolli e standard*.

[10]Si veda, ad esempio, il Regolamento (UE) n. 283/2014 del Parlamento Europeo e del Consiglio dell'11 marzo 2014 sugli orientamenti per le reti transeuropee nel settore delle infrastrutture di telecomunicazione.

[11]World Summit on the Information Society, *Declaration of Principles. Building the Information Society: a global challenge in the new Millennium*, 12 December 2003.

[12]Unicef, Mortalità infantile ancora in calo nel mondo, ma il COVID minaccia i progressi, 9 settembre 2020: «Secondo le nuove stime sulla mortalità pubblicate oggi da UNICEF, Organizzazione Mondiale della Sanità (OMS), Divisione per la Popolazione del Dipartimento per gli Affari Economici e Sociali delle Nazioni Unite (UNDESA) e Banca Mondiale, il numero di decessi tra 0 e 5 anni a livello globale nel 2019 è sceso al punto più basso mai registrato nella storia. I decessi sono stati infatti 5,2 milioni, con un calo di quasi il 60% rispetto ai 12,5 milioni del 1990».

[13]World Summit on the Information Society, *Tunis Agenda for the Information Society*, 18 November 2005.

[14]Si veda il sito ufficiale dell'Internet Governance Forum.

[15]L'*Electronic Frontier Foundation* è un'associazione internazionale no profit.

[16]*Società Internet* è l'associazione ed il capitolo italiano di ISOC.

[17]*Internet Society* (ISOC) è l'associazione costituita nel 1992 da Vint Cerf, Bob Kahn e da altri primi pionieri che hanno guidato lo sviluppo tecnico di Internet.

[18]ONU - Assemblea generale, *Trasformare il nostro mondo: l'Agenda 2030 per lo Sviluppo Sostenibile*, 21 ottobre 2015.

[19]Agenzia italiana per la cooperazione allo sviluppo, *Obiettivi di sviluppo sostenibile - SDGs*.

[20]Da elogiare, in tal senso, il nostro Ministero della Salute che, per esempio, ha ritenuto opportuno pubblicare delle FAQ ed una risposta alle fake news circolanti sui vaccini e sul Covid-19.

[21]Si veda per esempio il contributo di Gilberto Corbellini, professore ordinario di Storia della medicina e docente di Bioetica presso la Sapienza Università di Roma, ripreso dalla Encilopedia Treccani, alla voce *Storia della Medicina*.

[22]Istituto Superiore di Sanità, *Come viene sviluppato e commercializzato un vaccino*, aprile 2017.

[23]Ospedale pediatrico Bambin Gesù, *Nuovo Coronavirus: come si è riusciti a produrre rapidamente vaccini sicuri*, agosto 2021.

[24]Istituto Superiore di Sanità, *Sviluppo, valutazione e approvazione dei vaccini contro COVID-19*, gennaio 2021.

[25]Giorgio Giunchi è stato l'ideatore ed il curatore del più completo portale contenente fonti e ricerche sulla storia dell'informazione automatica e dell'Internet in Italia).

[26]AGID, *Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022*, luglio 2020.

[27]Presidenza del Consiglio dei ministri, *PNRR, gli obiettivi e la struttura*, novembre 2021.

[28]Id., *PNRR: salute*, novembre 2021.

[29]AGID, *Sanità digitale*.

[30]Il Ministero della Salute ha reso disponibile il sito *eHealth - Sanità digitale*, con collegamenti e normativa aggiornati.

[31]L'app Immuni

[32]Si veda a questo riguardo la ricerca presentata dalla Dr.ssa Diana Lelli nell'ambito del 63esimo Congresso Nazionale della Società Italiana di Gerontologia e Geriatria (Roma, 28 novembre-1 dicembre 2018).

[33]E. Santoro, *Tutti i problemi delle app mediche: vantaggi dubbi, privacy a rischio*, in "AgendaDigitale.eu", 23 gennaio 2017.

[34]D.M. Kent, E. Steyerberg, D. van Klaveren, *Personalized evidence based medicine: predictive approaches to heterogeneous treatment effects*, 2018.

[35]S. Rodotà - *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, settembre 2004.

[36]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[37]Fra i numerosissimi interventi, si segnala il parere favorevole sullo schema di decreto attuativo, che attiva la Piattaforma nazionale-DGC per il rilascio del *green pass*, prevedendo adeguate garanzie per l'utilizzo delle certificazioni verdi. V. Garante per la protezione dei dati personali, *Certificazioni verdi: via libera del Garante, con adeguate garanzie. Disposto il blocco provvisorio per l'App IO*, 10 giugno 2021.

[38]FHIR è uno standard per lo scambio di dati sanitari, pubblicato da HL7.

[39]Un documento XDS è un qualsiasi tipo di informazione clinica indipendente dal contenuto e rappresentazione con una precisa struttura che si avvale degli standard informatici sanitari.

[40]*Anteprima: ecco come sarà il Fascicolo Sanitario Elettronico 2.0*, 16 novembre 2021.

[41]Ministero della Salute, *L'attivazione e l'alimentazione del FSE*, 4 maggio 2021.

[42]Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, 7 marzo 2019.

[43]Id., *Valutazione d'impatto della protezione dei dati (DPIA)*.

[44]European Data Protection Board, *Guidelines, Recommendations, Best Practices*.

[45]L'*Agenzia dell'Unione europea per la cybersecurity* (ENISA) è incaricata di creare le condizioni per un elevato livello comune di cibersicurezza in tutta Europa.

[46]ENISA, *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*, 16 February 2017.

[47]Id., *Evaluating the level of risk for a personal data processing operation*.

[48]Sul portale dell'ENISA è presente una sezione dedicata alle misure di sicurezza ed infrastrutturale per il settore sanitario.

[49]ENISA, *Procurement Guidelines for Cybersecurity in Hospitals*, 24 February 2020.

[50] Id., *Good practices for the security of healthcare services*.
[51] Id., *Cloud Security for Healthcare Services*, 18 January 2021.
[52] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

* * *

Health protection, digital systems and privacy

Abstract: Innovations and new technologies can greatly contribute to improve care and research, but they should be regulated on the basis of a multistakeholder process such as that offered by Internet Governance. The systems digital transformation in the healthcare requires particular attention and sensitivity in terms of protecting and processing of personal data. It is central to build a functional digital ecosystem, yet safe and respectful of people's dignity and rights.

Keywords: Health – Privacy – Data protection – New technologies – Digital transformation

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0072
Articolo sottoposto a peer review

Relazioni e solitudini nella Rete. #Social_relation_&_società_confessionale

Maria Novella Campagnoli

Entro la più ampia e variegata cornice di una trattazione dedicata alla Internet governance, un'osservazione specifica non può non essere riservata alle particolari forme di comunicazione e di relazione che si sviluppano all'interno delle piattaforme social. Teatro, non soltanto di interazioni fluide e frettolose, ma anche di narrazioni solipsistiche e monadiche. Aspetti che, oggi più che mai, necessitano di essere ripensati e, laddove necessario, regolamentati.

Social network – Comunicazione – Relazione – Mipiacismo – Società confessionale

Sommario: *1. Tre* breadcrumbs *a mo' di introduzione – 2. Dal World Wide Web... ai social network – 3. Caratteristiche ed elementi di fascinazione – 4. Tra costruzioni e continue ri-configurazioni di sé e della relazione con gli altri – 5.* Les Fleurs du mal. *Brevi suggestioni conclusive*

1. Tre *breadcrumbs* a mo' di introduzione

Entro la più ampia e variegata cornice di una trattazione dedicata alla Internet governance, un'osservazione specifica non può non essere riservata alle particolari forme di comunicazione e di relazione che si sviluppano all'interno delle piattaforme social, oramai, da alcuni anni, teatro non soltanto di interazioni fluide e frettolose, ma anche di narrazioni solipsistiche e monadiche. Aspetti, che, oggi più che mai, necessitano di essere ripensati e regolamentati.

Muoviamo, in questa nostra ricostruzione, da alcune singolari *breadcrumbs*[1] fotografiche. Immagini che, con eloquenza ed efficacia, danno l'idea dell'impatto che la diffusione dei social network ha avuto – e tuttora sta avendo – sulle nostre vite: modificando le abitudini[2], trasformando gli atteggiamenti[3], alterando i linguaggi e ridisegnando le interazioni e le relazioni[4].

Una prima indicazione proviene da *Removed Social*[5], l'originale progetto realizzato, nel 2012, dall'americano Eric Pickersgill, che illustra con lucida ironia la solitudine e l'isolamento di chi è iperconnesso. *Removed Social* propone una nutrita photo-gallery nella quale sono ritratte scene di vita quotidiana: persone attorno ad un tavolo, sul divano, in salotto, in barca, in poltrona, a letto, dal barbiere, alla guida e perfino al cimitero. Tutti frangenti che, solitamente, vengono vissuti con lo smartphone (o con un qualunque altro device) a portata di mano[6]. Pur nella varietà delle scene e nella diversità dei contesti e dei soggetti, in ogni foto si rinviene un denominatore comune: il dispositivo elettronico del caso non compare, è stato infatti rimosso. Scelta che simboleggia l'invettiva di Pickersgill contro l'uso smodato dei

M.N. Campagnoli è avvocato e ricercatrice di Filosofia del diritto, informatica giuridica e biogiuridica presso il Dipartimento di Giurisprudenza dell'Università di Roma "Tor Vergata", dove insegna Teoria e pratica dei diritti umani.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

tool digitali e della mania di essere connessi alla Rete in ogni momento della nostra giornata. Fra le raffigurazioni più significative: quella che immortala due novelli sposi appoggiati al cofano di un'autovettura bardata per l'occasione: lo sposo da un lato, la sposa dall'altro. Entrambi mimano l'atteggiamento di chi è intento a controllare il proprio smartphone. Il paradosso è evidente: i due sono *appena sposati* (come è scritto sul cartello affisso alla vettura) eppure si comportano come se fossero *già separati*[7].

Un secondo spunto è fornito dallo stravagante ritratto, a firma di Oliviero Toscani, che è apparso su *Elle Man France* nell'aprile del 2014[8]. La fotografia – che come vuole lo stile dell'artista è spregiudicata, irriverente e provocatoria – ritrae un ragazzo e una ragazza distesi su un letto e completamente nudi. Sensualità e imbarazzo sono, però, scongiurati dalla presenza dei dispositivi tecnologici, che dominano il campo visivo e polarizzano l'attenzione dello spettatore. La ragazza regge in grembo un pc e indossa delle vistose cuffie, mentre il ragazzo tiene in mano uno smartphone collegato a degli auricolari. Il contrasto è particolarmente forte. Al contesto e alla mancanza di indumenti (che di per sé stessi presupporrebbero una certa confidenza ed intimità tra i due) fa da contraltare l'assenza di ogni forma di prossimità, di contatto e/o di comunicazione.

Una terza occasione di riflessione, infine, è suggerita da *Sur-Fake*[9]. La serie di scatti realizzati dal fotografo francese Antoine Geiger nel 2015, dove a venir meno sono addirittura i volti, attratti e letteralmente risucchiati dallo smartphone. Professionisti che vanno al lavoro, giovani che si fanno un selfie, persone che camminano, che sono in bicicletta o che si trovano nel bel mezzo di una mostra, da un'immagine all'altra, cambiano le situazioni ma la scena in sé è la medesima. I soggetti ritratti hanno sempre la stessa postura: tengono la testa china e hanno in mano un dispositivo che catalizza il loro interesse e che attrae e inghiotte il loro volto.

Fotografie *della* e *dalla* realtà, quelle realizzate da Pickersgill, da Toscani e da Geiger. Suggestioni distinte eppure concordi che – oltre ad essere particolarmente intense, disincantate e, a tratti, persino crude – hanno il pregio di cogliere e di mettere bene in evidenza alcuni dei nodi critici attorno ai quali orbita l'attenzione degli scienziati della Rete e di chi, a vario titolo, si interessa allo studio dei social e dei loro tanti riverberi (informatici, sociologi, filosofi, psicologi, matematici, ingegneri sociali, giuristi ed economisti). Ripercorrendo l'ordine delle immagini, possiamo, così, sintetizzare gli aspetti salienti messi a fuoco.

(i) *I social network sono parte integrante della nostra quotidianità.* È un dato di fatto. Abbiamo sviluppato un'abitudine compulsiva, una vera e propria ossessione, quella di avere lo smartphone sempre con noi e di controllarlo di continuo. Per la precisione – stando al documentario *It's people like us*[10] – lo controlliamo in media circa centocinquanta volte al giorno, in pratica, ogni sette minuti[11]. Inseparabile protesi, sempre connessa alla Rete e ai social, lo smartphone è come una finestra alla quale ci affacciamo ogniqualvolta ne sentiamo l'esigenza (per pubblicare un contenuto, per aggiornare e/o modificare il nostro stato, oppure, semplicemente, per distrarci curiosando fra i profili e le pagine altrui). Il rovescio della medaglia – come nota Manfred Spitzer – è che quando i nostri device non sono con noi, o quando non abbiamo la possibilità di connetterci alla Rete, «ci sentiamo come un insetto girato sulla schiena, che dimena impotente le zampe, del tutto inutilmente»[12].

(ii) *I social network comportano una riconfigurazione profonda della comunicazione e delle relazioni*[13]. La perdita dell'interazione vis-à-vis – nella quale sia io che l'altro siamo il nostro corpo – e il passaggio a una comunicazione in cui l'oggettività del corpo è assente e il soggetto-comunicante è ridotto al contenuto del suo messaggio, infatti, porta con sé tutta una serie di ripercussioni sulla sfera emotiva[14]. Ciò che ne consegue è il possibile sviluppo di dipendenze[15] e anche di vere e proprie patologie[16]. Fra le più recenti e allarmanti, senza dubbio, la c.d. *sindrome da ritiro sociale*, meglio nota come sindrome da *hikikomori*. Una situazione patologica che coinvolge soprattutto i più giovani (ne sono colpiti prevalentemente gli adolescenti) e che prevede l'azzeramento delle relazioni sociali e il ritrarsi del soggetto fra le mura domestiche, dove resta letteralmente incollato ad uno schermo anche per diciotto ore filate[17]. Isolato dalla società, l'*hikikomori* è un Neet (ossia uno di quei giovani "neither in employment nor in education or training"), immerso nel *mondo manga*[18] o prigioniero delle *virtual communities*[19].

(iii) *I social network ci permettono di scegliere come vogliamo apparire agli occhi degli altri, consentendoci di avere il profilo e le parvenze che più ci piacciono.* Disincarnati e svincolati dalla dimensione fisica, siamo – come afferma Sherry Turkle – ciò che appare sullo schermo[20] o, meglio, «ciò che le nostre dita fanno trapelare di noi attraverso lo schermo»[21]. Sempre in divenire, fluida e pronta ad essere ridisegnata quando vogliamo la nostra identità online, è un'identità che, però, non sempre rispecchia fedelmente la realtà e che – come ci avverte a suo modo Antoine Geiger – può anche venirci sottratta assieme alle informazioni che ci riguardano[22].

Tre snodi importanti, questi, sui quali si avrà modo di ritornare nel corso della trattazione.

2. Dal World Wide Web... ai social network

La storia dei social network assomiglia ad una parabola dall'ascesa rapida ed intensa. Per quanto veloce e significativa, però, si tratta di una storia relativamente recente, che trae avvio dalla convergenza sinergica di due fattori, reciprocamente collegati. Vale a dire: a) la diffusione del computer e la sua trasformazione da strumento per eseguire calcoli a strumento di scrittura (prima) e di comunicazione (poi); b) l'avvento, nel 1991, del World Wide Web[23], che – a detta del suo ideatore Tim Berners-Lee – più che un'innovazione tecnologica avrebbe dovuto rappresentare un'innovazione sociale, destinata ad aiutare le persone a comunicare e a migliorare la loro esistenza reticolare nel mondo[24].

Diversamente da quanto si potrebbe pensare, quindi, la primissima tappa dello sviluppo e dell'evoluzione dei nuovi network non si colloca nel 1997 – anno in cui si assiste alla comparsa della piattaforma *SixDegrees.com*[25] – ma risale a qualche anno prima. È, infatti, concomitante all'invenzione del Web o – mutuando le parole di Manuel Castells – di quel nuovo ambiente di interazione e di condivisione delle informazioni che è la *Galassia Internet*[26]. Il perché è presto detto. Internet ha ampliato e stravolto l'uso e le funzioni del computer, convertendolo in un mezzo di comunicazione di massa o, più correttamente, in un nuovo *medium*[27]. Ovverosia, in uno strumento che – superando i limiti spazio-temporali e interponendosi fra gli interlocutori – trasforma l'interazione da *esperienza diretta* dell'Altro ad *esperienza indiretta* (poiché, per l'appunto, mediata)[28].

Affinché i social network potessero fare la loro comparsa è stato, però, necessario un ulteriore e fondamentale passaggio. Dal Web (Web 1.0) – e dunque da un'interfaccia che consentiva di trasmettere lo stesso messaggio ad un consistente numero di riceventi, ma nella quale l'accesso alla produzione comunicativa era riservato a pochi e, in generale, a quegli stessi colossi che già controllavano l'editoria, la radio o la televisione[29] – si è dovuti passare al Web 2.0[30]. Vale a dire, ad un ambiente digitale ancor più aperto, nel quale ogni utente, oltre alla possibilità di accedere alle informazioni e ai contenuti, avesse anche quella di crearne e diffonderne di nuovi.

Con il Web 2.0 (web *partecipativo*), difatti, chiunque abbia accesso alla Rete e alle piattaforme social può – *ipso facto* – realizzare e pubblicare testi, immagini, audio e video, rendendoli visibili agli altri utenti che, oltre a guardarli e a commentarli, possono anche condividerli e divulgarli a loro volta. Altrimenti detto, se con il Web 1.0 ci trovavamo ancora di fronte ad un mezzo di comunicazione di massa (ossia rivolto alla massa), che presentava parecchie limitazioni nell'accesso alla creazione e alla divulgazione dei contenuti, con il Web 2.0 queste limitazioni vengono meno.

È, così, che si assiste al profilarsi dei social network: piattaforme che possono assolvere a diverse funzioni e che fungono anche da mezzi di comunicazione *di* e *per* la massa[31]. E cioè, media che si *rivolgono alla* massa e che *sono a disposizione della* massa: con i quali quest'ultima comunica e – a seconda dei casi e delle situazioni – diffonde informazioni e notizie. Nuovi vettori che sono alla portata di chiunque abbia accesso a Internet e ai tantissimi social che, in questi anni, sono nati. Un elenco in continua crescita[32] di cui YouTube, Facebook, Instagram, Pinterest, LinkedIn, Twitter, Skype, Messenger, Viber, Telegram, Signal, Snapchat e WhatsApp sono soltanto alcuni dei più noti e diffusi.

Figli di Internet e dell'evoluzione della sua interfaccia resa possibile grazie al Web 2.0 e alle app, i social network[33] non ci permettono soltanto di condividere esperienze, sentimenti, punti di vista e stati d'animo – come in una sorta di diario aperto alla lettura degli altri utenti[34] – ma ci consentono anche di raggiungere un triplice risultato:

- quello di avere un ruolo attivo-creativo nella definizione della nostra identità sociale (cioè della nostra posizione nell'ambito del network e/o del gruppo di cui facciamo parte)[35];
- quello di poter visionare, monitorare e controllare i profili altrui[36];
- e, infine, quello di estendere la nostra rete sociale, ad esempio, ampliando il numero dei nostri amici (nel caso di Facebook), dei nostri followers (in quello di Twitter) degli iscritti (nel caso di YouTube), oppure delle persone collegate e in contatto (nel caso di LinkedIn).

Tutto ciò, nell'ambito del cyberspazio[37] (quel particolare ambiente virtuale e interattivo che Geert Lovink definisce *spazio tecnosociale*[38]) e sullo sfondo di continue e vorticose trasformazioni che, passando per il Web 3.0 (web *semantico*[39]), sembrano averci già proiettato verso altri ed ulteriori scenari.

È il caso dell'attuale Web 4.0 (web della *realtà aumentata* e dei *big data*[40]) e dell'imminente Web 5.0[41] (il cosiddetto web emotivo). Uno spazio basato sull'interazione uomo-macchina/uomo-IA, del quale *R.E.A.D. System* (presentato al "CES" di Las Vegas nel gennaio del 2019[42]), così come, gli esoscheletri, i droni e i robot-chirurghi mostrati al "World Robot Conference"[43] di Pechino, ci offrono già qualche affascinante anticipazione[44].

3. Caratteristiche ed elementi di fascinazione

Reti informazionali alimentate da Internet e basate sui nuovi media, i social network sono piattaforme che consentono all'utente di scegliere e di gestire la propria identità e la propria rete sociale[45]. Piattaforme che, grazie alla loro intrinseca flessibilità e adattabilità, comportano parecchi vantaggi sotto il profilo organizzativo[46], ma che, al contempo, modificando radicalmente il nostro modo di comunicare, determinano anche una trasformazione (e, per certi versi, una vera e propria rivoluzione) sul piano antropologico[47].

Indissolubilmente legati all'avvento della digitalizzazione (e, cioè, al passaggio dalla rappresentazione analogica-continua[48] a quella digitale-discontinua[49] e alla successiva codifica delle informazioni[50]), i social network si contraddistinguono per la presenza di alcune particolari caratteristiche strutturali, quali:

a) la *modularità*, ossia la possibilità di scomporre tutti i contenuti in moduli dotati di un'identità distinta e separata rispetto all'oggetto di cui fanno parte. È il caso dei pixel di un'immagine, dell'audio di un filmato o degli script di una pagina web. In pratica, ciascun modulo può essere cambiato, sostituito, unito ad altri oppure estrapolato e riutilizzato. Si pensi alla possibilità di scaricare un'immagine da un sito per poi inserirla nell'ambito di un altro contesto o di un altro sito[51];
b) la *variabilità*, ovvero, la facoltà di modificare a piacimento tutti i contenuti multimediali. Emblematiche le variazioni che si possono apportare alle fotografie: da un'unica immagine iniziale, infatti, se ne possono ricavare parecchie semplicemente applicando dei filtri, ritagliandone delle parti, oppure ricorrendo a programmi come photoshop;
c) l'*interattività*, caratteristica connessa all'ipertestualità, grazie alla quale il lettore può interagire con l'autore, in un continuo scambio di ruoli[52]. Basti pensare al funzionamento di Wikipedia, basata proprio su di un costante "passaggio di testimone" tra chi scrive e chi legge;
d) l'*automazione*, grazie alla quale alcune operazioni possono essere svolte in maniera automatica. Paradigmatiche alcune applicazioni ludiche di Facebook, come Farmville e Bubble Island, che seguitano a funzionare anche quando l'utente non è connesso.

Alla modularità, alla variabilità, all'interattività e all'automazione, si aggiungono altresì: e) lo *spazio virtuale* all'interno del quale gli utenti possono costruire e mostrare il proprio profilo, visibile agli altri; f) la *lista* (*rete*) *di utenti* (*contatti*) con i quali è possibile comunicare, scambiare informazioni e condividere contenuti multimediali; g) la *facoltà di monitorare e di analizzare* l'andamento del proprio profilo e della propria rete (i messaggi, il numero di contatti, le condivisioni, i like, ecc.); h) la *notevole facilità di utilizzo*, dovuta al fatto che tutte le piattaforme social, grossomodo, presentano la medesima impostazione grafica e lo stesso approccio, cosa che le rende immediatamente accessibili e utilizzabili senza bisogno di particolari spiegazioni e/o istruzioni; i) la *dimensione espressiva*, che consente agli utenti di generare nuovi contenuti multimediali; l) la *dimensione comunicativa*, grazie alla quale tutto ciò che viene pubblicato nel social è visibile (salvo limitazioni) a tutti gli altri utenti della piattaforma; m) la *dimensione comunitaria*, che fa sì che la versione finale delle informazioni sia frutto dell'interazione con la comunità, che visualizza i contenuti, li valuta, concorre alla loro circolazione e contribuisce al loro eventuale successo[53]. Sempre guardando alle caratteristiche strutturali, ma con specifico riferimento alle interazioni e ai legami che si possono instaurare fra gli utenti, va detto che – a seconda delle situazioni e dei network – si possono avere:

- *legami bidirezionali*, individuati dalle c.d. *amicizie*, particolari rapporti che permettono di accedere in maniera completa al profilo dell'amico e che rendono possibile contattarlo direttamente, vederne le attività realizzate sulla piattaforma, nonché commentarne, condividerne e/o modificarne i contenuti pubblicati. Una forma d'interazione, questa, che è diffusa soprattutto su Facebook;
- *relazioni di gruppo*, basate su reti create *ad hoc* e volte a consentire ad un novero ristretto e chiuso di utenti di scambiarsi foto, video, collegamenti e messaggi, elementi la cui visione resta del tutto preclusa agli "esterni". Modalità molto in voga, ad esempio, su WhatsApp;
- *interazioni a stella*, legami c.d. *uno-a-molti*, in quanto, potenzialmente aperti a tutti gli utenti del network. Interazioni in cui, un unico emittente può scegliere se rivolgersi ad un destinatario solo (tramite l'invio di un messaggio individuale-privato), oppure a molti, come avviene con il Tweet.

Al di là degli aspetti strutturali e dei numerosi vantaggi che ne conseguono, è interessante sottolineare che l'*appeal* dei social network – la chiave del loro successo e la ragione della loro diffusione trasversale[54] e intergenerazionale[55] – risiede nella loro singolare capacità di rispondere alle diverse attese degli utenti: quelle di chi li utilizza come mezzo espressivo, per condividere pensieri e frangenti

di vita; quelle di chi se ne avvale come strumento professionale per farsi conoscere e/o per soddisfare esigenze di marketing; e, non da ultimo, anche quelle di chi, attraverso i social, instaura, realizza e sviluppa la propria sfera relazionale.

Più in particolare – ricordando la *teoria degli usi e delle gratificazioni*[56] e riproponendo l'ordine dei *bisogni sociali* individuato dalla *piramide* di Abraham Maslow[57] – si può affermare che i social appagano:

- il *bisogno di sicurezza*, ossia il desiderio di protezione e tranquillità. Non a caso, all'interno delle piattaforme social e nell'ambito della rete di contatti che ogni utente si costruisce, non ci sono persone estranee o ostili, ma soltanto amici che – nel caso in cui non si dimostrino tali oppure divengano indesiderati e molesti – possono essere cancellati e/o persino bloccati;
- il *bisogno associativo*, vale a dire l'esigenza di sentirsi parte di un gruppo, di essere apprezzati, amati e di interagire e collaborare con gli altri. È sufficiente pensare ai frequenti scambi di opinioni e risorse multimediali che i social permettono, indipendentemente dagli orari, dalle distanze, dal luogo in cui ci troviamo e da cosa stiamo facendo;
- il *bisogno di autostima* e, dunque, la necessità di sentirsi apprezzati, rispettati e tenuti in considerazione. Necessità alla quale i social rispondono offrendo la possibilità di scegliere di continuo a chi si desidera chiedere l'amicizia e di chi si intendono accettare le rispettive richieste. Va da sé che se le persone che ci chiedono (o che ci hanno chiesto) l'amicizia sono parecchie vuol dire che valiamo e che godiamo dell'interesse e dell'apprezzamento degli altri utenti;
- il *bisogno di autorealizzazione*, ovvero l'esigenza di sviluppare e di esternare la propria personalità, realizzare le proprie aspettative e raggiungere una posizione gratificante e pregevole all'interno del gruppo sociale. Aspirazioni che i social soddisfano dotandoci di un profilo sempre in divenire e di una cerchia più o meno ampia di "amici" (nel caso di Facebook) o di "seguaci" (nel caso di Twitter).

Le cose, però, non sono così semplici. Il desiderio di sicurezza, la voglia di essere accettati e di far parte di un gruppo, la necessità di dimostrare il proprio valore, l'esigenza di affermarsi sono, sì, bisogni eterogenei che i social network soddisfano, ma – paradossalmente – sono anche necessità che vengono accresciute in maniera esponenziale proprio dagli stessi social.

Vetrine virtuali che ospitano *esplosioni autobiografiche*[58], i nuovi network, infatti, prestano il fianco alle inclinazioni narcisistiche[59] e alimentano quella particolare smania di consenso e di approvazione che – con un'insolita ma efficace formula – viene definita *mipiacismo*[60]. Non a caso, una delle prime e delle maggiori preoccupazioni di chi pubblica un post, o un qualsiasi altro contenuto, è quasi sempre quella di riuscire ad "accaparrarsi" quanti più like possibile[61], anche se per far ciò è necessario "dire tutto di sé"[62].

Ed è proprio questo il motivo per cui – Bauman sostiene – che la società odierna è una *società confessionale*, dove tutti e, in modo particolare i ragazzi, non avvertono più alcuna gioia nell'avere dei segreti: «[...] I teenager muniti di confessionali elettronici portatili non sono che apprendisti che si formano e vengono formati all'arte di vivere in una società-confessionale, una società contraddistinta dal fatto di aver cancellato il confine che separava un tempo pubblico e quello privato, di aver trasformato l'esibizione pubblica del privato in una pubblica virtù e in un pubblico dovere e di aver spazzato via dalla comunicazione pubblica tutto ciò che non si lascia ridurre a confidenza privata e tutti coloro che rifiutano di confidarsi». «[...] [Così si] mettono in mostra avidamente ed entusiasticamente le proprie qualità sperando di attirare l'attenzione e possibilmente di ottenere il riconoscimento e l'approvazione necessari per non essere esclusi dal gioco della socializzazione [...]»[63].

4. Tra costruzioni e continue ri-configurazioni di sé e della relazione con gli altri

Diversi anni fa, in un noto lavoro pubblicato su *New Media & Society*, Roger Silverstone – fra i primi ad occuparsi di questi temi – si chiedeva quali fossero gli aspetti inediti dei nuovi media[64]. Pur nell'ambito di studi e di approcci fra loro molto differenti[65], questo stesso interrogativo si è poi riproposto con una certa ciclicità e – ancora oggi – può rivelarsi un utile spunto per ragionare sulle prerogative e sugli aspetti inconsueti dei social network[66].

Dei nuovi network all'inizio del nostro percorso s'è detto che: (i) *fanno parte della nostra quotidianità*; (ii) *determinano una riconfigurazione della comunicazione e dei rapporti*; (iii) *ci permettono di scegliere il nostro profilo e la nostra identità*. Osservazioni senza dubbio significative, ma che – da sole – non sono sufficienti a rispondere e a soddisfare pienamente il quesito posto da Silverstone. Proviamo, seppur in maniera molto sintetica e per punti, a ricostruire.

(i) È vero: *i social permeano la nostra vita*. E pressoché ogni giorno siamo subissati da messaggi che ci ricordano quanto siano utili, e che ci suggeriscono quali siano i network e le soluzioni tecnologiche più adatte a soddisfare le nostre esigenze. Messaggi, che suonano più o meno così:

«*Ti senti solo?* – Perché non sei su Facebook?
Single? – Perché non provi con gli incontri online?
Problemi a scuola? – Ti manca solo la giusta App per studiare!
Vuoi recuperare la linea? – Non hai ancora la App per la dieta?
Non hai tempo? – Metti la tua agenda su cloud!
Malato? – Watson ti aiuta nella diagnosi e nella terapia!
Fame? – Dai fast food alle ricette gourmet: tutto online!
Niente soldi? – Il credito online è più veloce di qualsiasi altra banca!
Sei svogliato? – Prova la giusta App motivazionale!
Dedichi troppo tempo al tuo smartphone? – Basta un'App per lo spegnimento automatico!»[67].

Malgrado ciò, però, non si può non ammettere che tutti i media, che via via si sono succeduti nel corso della storia[68], hanno sempre comportato profondi mutamenti non solo nello svolgimento e nella gestione delle attività quotidiane, ma anche nel nostro stesso modo di pensare e di rapportarci al mondo. Emblematici – come avverte Lévy – i tanti cambiamenti legati all'invenzione della scrittura e, più di quattromila anni dopo, a quella della stampa.

«All'interno delle culture prettamente orali, che hanno caratterizzato il 95% del tempo che la nostra specie ha trascorso su questo pianeta, la memoria umana era circoscritta alla capacità di ricordare dei gruppi di anziani. Gli strumenti, i gioielli, le statue, i monumenti di pietra e le immagini dipinte erano i soli supporti capaci di trasmettere concetti astratti. Con la scrittura [...] le conoscenze hanno cominciato ad essere registrate in maniera più efficace. [...] La nuova abbondanza di testimonianze [...] permise di mettere in prospettiva le conoscenze legate al presente, così come i progetti legati al futuro [...] [abituando] lo spirito umano ad utilizzare uno sguardo analitico, logico, critico e comparativo nei confronti della realtà»[69].

Una vera e propria rivoluzione culturale, alla quale, anche Victor Hugo non manca di dedicare un significativo rimando. Celebre l'espressione dell'arcidiacono di Notre-Dame, Claude Frollo: "*ceci tuera cela*". Formula con la quale Hugo accenna proprio ai riverberi connessi all'invenzione di Gutenberg[70].

(ii) È altresì vero: *i social trasformano la comunicazione e le relazioni*. Non solo, Internet e i nuovi network trasformano anche lo spazio e il tempo[71]. Assistiamo, così, all'emergere di quella particolare dimensione che Paul Virilio definisce *dromosfera*[72]. Una dimensione che è contraddistinta dall'accelerazione continua e, all'interno della quale, il tempo risulta per così dire contratto (grazie alla riduzione delle durate necessarie al compimento delle diverse attività), mentre la geografia (intesa come spazio fisico fatto di confini, frontiere e distanze) sembra condannata a perdere qualunque significato.

«Più che alla "fine della storia" assistiamo dunque a quella della geografia. [...] il GLOBALE è l'*interno* [...] e il LOCALE è l'*esterno*. [...] i semi non sono più all'interno delle mele, né gli spicchi al centro dell'arancia: *la scorza è rovesciata*»[73].

Tuttavia, non si può fare a meno di osservare che il principale scopo dei media (*di tutti i media! vecchi e/o nuovi che siano!*) è quello di "mediare la comunicazione". Vale a dire, proprio quello di superare i vincoli spazio-temporali e di rendere possibile il passaggio dall'interazione sincronica e contingente a quella diacronica e differita. Altrimenti detto, anche in questo caso, così come per il precedente, non si può dunque dire di aver individuato una vera e propria novità.

(iii) Ed è pure vero: *i social ci permettono di scegliere come mostrarci*[74]. Eccellenti strumenti di *impression management* e di *self-empowerment*, i social network ci consentono di scegliere come presentarci, cosa mostrare di noi e, soprattutto, ci permettono di creare dei *nuovi sé sociali*. Non a caso, Floridi osserva che «il sé sociale [...] [costituisce] il principale canale attraverso cui le ICT e, in particolar modo i social media interattivi, esercitano il loro profondo impatto sulle nostre identità personali. [...] [Basta infatti che] cambiamo le condizioni sociali in cui viviamo, mutiamo le reti di relazioni e il flusso di informazioni di cui godiamo e ridisegniamo natura e novero dei limiti e delle possibilità che regolano come ci presentiamo al mondo e indirettamente a noi stessi, [...] [perché] il nostro sé sociale [...] [possa] essere radicalmente aggiornato [...]»[75].

Un fenomeno, questo della costruzione e della *micronarrazione* del sé, al quale James[76] e Proust[77] hanno dedicato particolare attenzione, e che – seppur con tecniche e modalità molto meno penetranti rispetto a quelle dei social media – ha sempre accompagnato la storia dell'uomo. A riprova di ciò, e semplicemente a titolo d'esempio, si può ricordare quanto osservato da Rifkin a proposito di quella straordinaria "finzione" che, fra il Settecento e l'Ottocento, è stata il romanzo. Una finzione che – come nota il celebre economista e sociologo statunitense – ha infatti permesso a «milioni di persone [...] di definire i propri sentimenti più intimi e di manifestarli»[78].

Ma, se così, è evidente che si deve compiere un passo ulteriore, tornando a domandarsi – con Silverstone – *what's new about new media?* Per rispondere, è necessario soffermarsi sull'aspetto sociale che con-

traddistingue i nuovi network. Una scelta che, parlando di media – e cioè di strumenti di mediazione volti a favorire i rapporti sociali – potrebbe anche apparire auto-evidente[79], o persino banale, e che, invece, ci permette di mettere a fuoco alcuni elementi di nodale importanza.

Nati per abilitare le collaborazioni partecipative e per incentivare le comunicazioni orizzontali "dal basso"[80] (secondo la logica *peer-to-peer*), i social network hanno portato a maturazione quella trasformazione che aveva già avuto inizio con l'avvento di Internet[81], favorendo la comparsa di nuove forme di aggregazione, basate solo ed esclusivamente sull'interazione online: le community. Più in particolare, i social media hanno contribuito ad avvicinare la nostra vita quotidiana al cyberspazio[82], generando un nuovo ed inedito spazio, quello dell'*inter-realtà*[83]: un ambiente sociale ibrido, contraddistinto dalla commistione e dalla sovrapposizione di esperienze reali (offline) e di esperienze digitali (online).

Si assiste così – *ed è questa la più significativa novità dei social!* – al passaggio dalla comunità tradizionalmente intesa (radicata nel territorio)[84] alla Rete[85], o meglio ai nuovi network che, invece, sono del tutto affrancati dalla dimensione spaziale[86]. Inedite forme di aggregazione sociale, che – con Castells – possiamo definire comunità *specializzate* e/o *di scelta*, occasionate dalle preferenze, dalle necessità e dalle strategie degli utenti e degli attori sociali[87]. Comunità sempre *in fieri*, all'interno delle quali la parola d'ordine è *flessibilità* e in cui i legami sono, sì, meno impegnativi e più liberi, ma, al contempo, si fanno anche più fragili ed incerti.

Si noti, questa sorta di "transizione" dalla comunità al network suggerisce anche due possibili considerazioni. La prima è che con i social network sembra realizzarsi quella particolare forma di *sociazione* che – per Simmel – è rappresentata dalla *socievolezza*. Una singolare modalità d'interazione, nell'ambito della quale il processo di associazione integra un valore *in sé*: una relazione sviluppata nella modalità del gioco, che si contraddistingue per l'assenza di tutte quelle tensioni che, invece, sono proprie dei rapporti e dei vincoli politici, economici e giuridici. In base alla ricostruzione del celebre sociologo tedesco, infatti, la socievolezza sarebbe il frutto della *libera interdipendenza degli individui* che interagiscono fra di loro, mossi unicamente dal *desiderio di stare insieme*, senza contenuti o obiettivi ulteriori[88].

La seconda considerazione è che, contrariamente alle finalità per le quali sono stati pensati (*semplificare le comunicazioni e i contatti fra gli utenti ed agevolare la condivisione di contenuti e informazioni*), i social stanno diventando sempre più autoreferenziali[89], determinando lo sviluppo di vere e proprie comunità *personalizzate* e *io-centriche* modellate sui gusti e sulle preferenze dell'individuo[90].

Di qui, come avvertono in molti[91], il pericolo che si assista ad una sorta di reviviscenza dell'individualismo[92], sotto forma di individualismo *in e/o di rete*[93]. Non di rado, infatti, i network si conformano ai valori, agli interessi, ai desideri e ai progetti dei singoli. Inclinazioni che, tra l'altro, vengono poi adoperate per mettere a punto strategie commerciali[94], per orientare i comportamenti e, non da ultimo, anche per condizionare le scelte politiche[95]. E, sempre di qui, anche tutta una serie di rischi che possono investire proprio l'individuo e, in maniera particolare, la sua percezione del mondo, le relazioni con gli altri e le sue stesse condizioni psico-fisiche[96].

Entro questa cornice, si inseriscono quello che può essere considerato come *il paradosso dei social network*, ovvero: l'emergere di forme di isolamento sociale[97] o – per dirla con Anders – di *eremiti di massa*[98] e la conseguente diffusione di forme di rifiuto della vita reale[99]. Un rifiuto analogo a quello dei turisti giapponesi affetti dalla c.d. *sindrome di Parigi*[100], che, una volta arrivati nella capitale francese e vedendo disattesa la loro percezione idealizzata e romanzata della città, manifestano condizioni di disagio.

Abituati alle opportunità e agli scenari ottimizzati proposti dal mondo virtuale e dai social, nel momento in cui ritorniamo alla dimensione reale, decisamente meno piacevole ed accattivante[101], avvertiamo una sorta di malessere[102] che ci porta a rifugiarci nella vita offertaci dallo schermo[103]. Un po' come accade agli *i-Gen*, l'attuale generazione di nativi digitali iperconnessi: ragazzi del tutto incapaci di concepire un mondo senza Internet, e che – rispetto alle esperienze reali – prediligono di gran lunga quelle digitali[104], più semplici e più gratificanti.

5. *Les Fleurs du mal*. Brevi suggestioni conclusive

È innegabile: con le loro interfacce intuitive e decisamente friendly, i social, non ci offrono semplicemente occasioni di svago, o spensierate digressioni dalla realtà, ma ci accompagnano e ci agevolano quotidianamente anche nello svolgimento delle attività personali, così come di quelle professionali. È sufficiente pensare alla frequenza e all'estrema facilità con la quale – in qualsiasi momento e da qualunque luogo – possiamo, ad esempio: controllare l'account di lavoro restando aggiornati in tempo reale; condividere documenti con tecniche che hanno soppiantato il vecchio e lento fax (WhatsApp, Google

Drive, Dropbox,...); prendere parte a una conference call risparmiandoci viaggi e perdite di tempo (Skype, GoToMeeting, Cisco Webex Meetings,...); gestire la rete domestica e gli elettrodomestici di casa (Smart Living, Neurio, MyVirtuoso Home,...); oppure monitorare il nostro stato di salute (iFarmaci, Laboratory Gear Medical, PubMedClip,...).

Supporti irrinunciabili ai quali fanno, però, da contrappeso anche tutta una serie di criticità, che vanno dagli atteggiamenti scorretti e/o disfunzionali, sino ai c.d. *cyber crimes*. Un ampio e variegato ventaglio di fattispecie, fra le quali spiccano condotte come: la *diffusione di fake news*[105]; il *furto d'identità*[106]; il *cyberstalking*[107]; il *cyberbulling*[108]; il *troll*[109]; l'*hate speech*[110]; il *sexting*[111]; oppure la *sextortion*[112] e, ancora, il *revenge porn*[113]. Comportamenti lesivi che, non di rado, si annidano tra le pieghe dei social e che, per certi versi, sono incentivati dalla struttura e dalle caratteristiche proprie dei network.

Il motivo è presto detto: la virtualità, sommata alla semplicità di accesso e di utilizzo, fa sì che i social vengano percepiti alla stregua di ambienti prettamente ludici e privi di conseguenze. Si sviluppa, così, l'illusione di operare in una sorta di *Far West giuridico*[114], dove ci si crede facoltizzati ad utilizzare un eloquio più anticonformista e diretto[115], e ad adottare atteggiamenti più disinvolti e spregiudicati. Un'illusione che nasce da un duplice fraintendimento di fondo e, nello specifico, da una visione distorta del virtuale e della Rete.

Per un verso, si crede che il virtuale si contrapponga al reale e che tutto ciò che accade online (in quanto, per l'appunto, *non-reale*) non possa determinare né ricadute sociali, né, men che meno, conseguenze e/o sanzioni di tipo giuridico. Quando, invece – derivando dal latino *virtus* e avendo la sua radice etimologica in *vis-roboris* (forza, potenza) – il virtuale è il contrario dell'attuale[116] e rappresenta ciò che "non-è-ancora", ma "è-in-potenza". Una dimensione che, contrariamente a quello che si può supporre, comporta dei riverberi assolutamente concreti (e *reali*) sulla vita offline.

Per un altro verso, si pensa che in Rete (e, dunque, anche nei social) regni l'anonimato più assoluto, tanto che – riprendendo il celebre fumetto Steiner[117] – si potrebbe dire: *on the Internet nobody knows you're a dog!* Una falsa credenza, che induce alla perdita (o comunque alla riduzione) del controllo sociale[118]. Si sviluppa, così, un meccanismo che, *mutatis mutandis*, sembra ricordare quello evidenziato da Stanley Milgram nel suo *Obbedienza all'autorità*. Con la differenza che – mentre negli esperimenti condotti dallo psicologo statunitense l'anonimato garantiva e rafforzava l'obbedienza all'autorità – in Rete e sui social l'anonimato diventa un incentivo a violare qualsiasi genere di regola.

Fraintendimenti ed errate letture, in cui – nonostante i diversi provvedimenti normativi europei[119] e nazionali[120] – in molti, tuttora, incorrono spesso, in particolar modo fra i più giovani[121]. Difatti, pur essendo nati e cresciuti assieme ad Internet e ai nuovi media ed avvalendosene di continuo, i nativi digitali non sono sempre adeguatamente alfabetizzati al loro uso corretto e, anzi, sono fra le categorie più esposte ai *cyber crimes*, dei quali, non di rado, oltre che vittime, diventano attori inconsapevoli[122].

Ed è proprio ai giovani che il diritto *dei/nei* social oggi guarda con particolare interesse e prudenza, come è stato recentemente dimostrato dal General Data Protection Regulation (GDPR) che, all'articolo 8, disciplina il consenso al trattamento dei dati prestato dai minori durante l'accesso ai servizi della società dell'informazione[123]. Disposizione con la quale il Regolamento (UE) 2016/679 ha cercato di contemperare il diritto del minore ad usufruire delle straordinarie opportunità offerte dai nuovi media (che se utilizzati in maniera appropriata possono anche supportare lo sviluppo degli adolescenti[124]) con la necessità di tutelarne i dati e di scongiurare il pericolo di violazioni ed abusi[125]. Un tentativo, quello dell'articolo 8, dettato dalla consapevolezza che – al di là delle criticità e dei possibili rischi – i social network (così come il Web in generale), per noi uomini, sono un po' come il mare descritto da Baudelaire ne *Les Fleurs du mal*: forza ignota, talvolta pericolo, ma anche, richiamo irresistibile, attrazione affascinante, spazio fecondo portatore di nuove opportunità e di ricchezze e, perché no, anche occasione di libertà:

> *Homme libre, toujours tu chériras la mer!*
> *La mer est ton miroir; tu contemples ton âme*
> *Dans le déroulement infini de sa lame,*
> *Et ton esprit n'est pas un gouffre moins amer.*
> *Tu te plains à plonger au sein de ton image;*
> *Tu l'embrasses des yeux et des bras, et ton cour*
> *Se distrait quelques fois de sa propre rumeur*
> *Au bruit de cette plainte indomptable et sauvage.*
> *Vous êtes tous les deux ténébreux et discrets:*
> *Homme, nul n'a sondé le fond de tes abîmes;*
> *O mer, nul ne connaît tes richesses intimes,*
> *Tant vous êtes jaloux de garder vos secrets!*
> *Et cependant voilà des siècles innombrables*
> *Que vous vous combattez sans pitié ni remord,*
> *Tellement vous aimez le carnage et la mort,*
> *O lutteurs éternels, o frères implacables!*[126]

Note

[1]Mi avvalgo di questa singolare espressione (ultimamente sempre più usata nel campo dell'informatica), che indica sia le

"tracce" lasciate dagli utenti, sia i link inseriti all'interno dei menu dei siti e/o delle pagine web per favorire la navigazione.

[2]Sugli effetti dei social network, particolarmente significative le osservazioni di G. Lovink che, con l'acume che lo contraddistingue e senza sfociare nel pessimismo, invita ad un approccio critico (G. Lovink, *Ossessioni collettive. Critica dei social media*, (trad. it.), Università Bocconi, 2012; Id., *Nichilismo digitale. L'altra faccia delle piattaforme*, (trad. it.), Università Bocconi, 2019). Ben diversa è la posizione di J. Lanier che, invece, prospetta una critica assai più aspra e perentoria (J. Lanier, *Dieci ragioni per cancellare subito i tuoi account social*, (trad. it.), Il Saggiatore, 2018).

[3]In merito alle ripercussioni che i social hanno sui nostri comportamenti, inducendoci a gesti e approcci inconsueti, interessanti gli studi di P. Wallace, *La psicologia di Internet*, (trad. it.), Raffaello Cortina, 2017.

[4]E proprio a proposito della perdita della capacità di conversare "faccia a faccia" e dei diversi risvolti patologici dei social, come la dissociazione psichica o la riduzione delle capacità emotive e affettive, particolarmente interessante la ricostruzione di S. Turkle, *La conversazione necessaria. La forza del dialogo nell'era digitale*, (trad. it.), Einaudi, 2016.

[5]Cfr. il sito del progetto.

[6]Tendenza, questa, che è stata confermata anche da J.A. Roberts e M.E. David. In particolare, secondo i ricercatori della Baylor University, stiamo assistendo ad una preoccupante inversione di prospettiva. Anziché pensare ai social come ad un elemento di distrazione dalla vita reale, accusiamo la vita reale di distoglierci dalla frequentazione dei social network (J.A. Roberts, M.E. David, *My life has become a major distraction from my cell phone: Partner phubbing and relationship satisfaction among romantic partners*, in "Computers in Human Behavior", vol. 54, January 2016, p. 134-141).

[7]Guardando l'immagine, potremmo dire – con Turkle – che i due sposi sono insieme ma soli. Cosa che, è ovvio, non ci si aspetta, soprattutto da due novelli sposi (S. Turckle, *Insieme ma soli. Perché ci aspettiamo sempre più dalla tecnologia e sempre meno dagli altri*, (trad. it.), Einaudi, 2019).

[8]Nel dettaglio, la fotografia alla quale rinvio corredava il dossier di J. Leuil, *Ce que le porno nous apprend*, in "Elle Man France", aprile 2014.

[9]Tutte le immagini sono pubblicate online sul sito del fotografo. È interessante ricordare che il progetto *Sur-fake* – in cui, per l'appunto, i volti vengono risucchiati dal cellulare – è stato anticipato da un lavoro di senso "opposto": *Sur-face* che, invece di risucchiarli, nascondeva i volti delle persone sotto una specie di cono.

[10]Realizzato dalla regista australiana premio Oscar Eva Orner, e presentato a Melbourne il 21 settembre 2017, Il documentario segue la giornata di cinque australiani, filmandone gli atteggiamenti. Presi dalla smania di controllare il cellulare in qualsiasi momento, anche quando sono alla guida, i protagonisti non si avvedono nemmeno dei rischi ai quali espongono la loro incolumità e quella degli altri. Il filmato integrale è disponibile in streaming.

[11]Sull'uso (e sull'abuso) dello smartphone, merita d'esser menzionata la campagna di informazione dal titolo *Il tuo cellulare è intelligente usalo con intelligenza*, avviata – dal Ministero della Salute, Ministero dell'Ambiente, Ministero della Tutela del Territorio e del Mare, Ministero dell'Istruzione, Ministero dell'Università e della Ricerca – il 19 luglio 2019. Iniziativa, adottata in ottemperanza alla sentenza n. 500/2019 del TAR del Lazio, che mira ad incentivare l'adozione di corrette modalità di utilizzo dei dispositivi telefonici e a sensibilizzare la popolazione (e in special modo i più giovani) sulle ripercussioni che un utilizzo improprio del cellulare può avere sulla salute e sull'ambiente.

[12]M. Spitzer, *Solitudine digitale. Disadattati, isolati, capaci solo di una vita virtuale?*, (trad. it.), Corbaccio, 2016, p. 15.

[13]G. Riva, *I social network*, il Mulino, 2016, in part. p. 27.

[14]Basti pensare che – come ha sottolineato Goleman – l'intelligenza emotiva si sviluppa grazie alla capacità di intravedere e di cogliere le emozioni e i sentimenti degli altri. Una capacità, questa, che – come è evidente – i social network affievoliscono e riducono molto (cfr. D. Goleman, *Intelligenza emotiva*, (trad. it.), Rizzoli, 1995).

[15]Sul punto, K.S. Young, *Internet Addiction: Symptoms, Evaluation, and Treatment*, in L. Vande Creek, T. Jackson (eds.), "Innovations in Clinical Practice: A Source Book", vol. 17, Professional Resource Exchange, 1999, p. 19-31. Inoltre, per un agile approfondimento cfr. S. Bernardi, S. Pallanti, *Internet addiction: a descriptive clinical study focusing on comorbidities and dissociative symptoms*, in "Comprehensive Psychiatry", vol. 50, 2009, n. 6, p. 510-516; G. Rossi, *IAD. La nuova dipendenza patologia da Internet*, in "Fatto&Diritto", aprile 2014; come pure, A. Montano, A. Valzania, *Dipendenza da Internet*, Istituto A.T. Beck, 2018.

[16]Fra le patologie: 1) la *nomofobia* (che sta per "no mobile fobia") e indica la paura di rimanere senza smartphone e senza connessione mobile; 2) la *fomo* (ossia "fear of mission out") e, dunque, la paura di perdersi qualcosa, qualche notizia, qualche post e – in breve – di essere "tagliato fuori" da ciò che accade in Rete e nei social.

[17]Cfr., fra gli altri, C. Ricci, *Hikikomori: adolescenti in volontaria reclusione*, Franco Angeli, 2017; M.R. Parsi, M. Campanella, *Generazione H. Comprendere e riconnettersi con gli adolescenti sperduti nel web tra Blue whale, Hikikomori e sexting*, Piemme, 2017.

[18]In merito alla stretta relazione fra giovani affetti dalla sindrome di *hikikomori* e fumetti manga (A.M. Caresta, *Generazione hikikomori. Isolarsi dal mondo, fra web e manga*, Castelvecchi, 2018).

[19]In generale, a proposito delle comunità virtuali, meritano d'esser qui ricordate le parole di Rheingold: «[...] c'è sempre qualcun altro là. È come essere in un bar, circondato dai soliti vecchi amici e da nuove presenze, molto simpatiche; al posto di mettermi, però, in giacca, spegnere il computer e camminare verso l'angolo, mi basta accendere il mio modem e essi sono là» (H. Rheingold, *Comunità virtuali: parlare, incontrarsi, vivere nel ciberspazio*, (trad. it.), Sperling & Kupfer, 1994, p. 24).

[20]Cfr. S. Turkle, *Crisi d'identità*, in Id., "La vita sullo schermo. Nuove identità e relazioni sociali nell'epoca di Internet", (trad. it.), Feltrinelli, 1997, pp. 307-325.

[21]Così, G. Pravettoni, *Web Psycology*, Guerini e Associati, 2002, in part. p. 46.

[22]In merito all'utilizzo che i social fanno delle informazioni che ci riguardano, Talia osserva: «Tutti o quasi usiamo quei servizi senza chiederci come mai siano gratuiti, come mai questi colossi informatici regalino tutto questo. [...] le monete con cui paghiamo [...] [sono] le informazioni». Informazioni che, ad esempio, una volta tratte dai network, possono poi essere utilizzate per formulare proposte commerciali *ad hoc*. Emblematico l'*anticipatory shipping* proposto da Amazon (D. Talia, *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*, Rubettino, 2018, in part. pp. 47-49 e pp. 25 e 26).

[23]È interessante ricordare che – sebbene sia nato ufficialmente il 6 aprile 1991 presso il CERN di Ginevra – il Web è stato anticipato da una (più rudimentale) versione precedente: ARPANET. Realizzata a partire dal 1969 dalla DARPA (*Defence Advanced Research Projetcs Agency*) ARPANET aveva lo scopo di collegare centri di calcolo e terminali di Università, Laboratori di ricerca ed Enti militari.

[24]T. Berners Lee, *L'architettura del nuovo web*, (trad. it.), Feltrinelli, 2001, in part. p. 113.

[25]Creato nel 1997 da Andrew Weinreich e attivo sino al 2001, anno in cui è stato chiuso per carenza di fondi, *SixDegrees.com* è considerato da molti come l'antenato di Facebook. Nel dettaglio, si trattava di un sito di incontri che – a partire dalla nota teoria dei *sei gradi di separazione* formulata, per la prima volta, nel 1929 dallo scrittore ungherese Frigyes Karinthy – consentiva ai suoi utenti di stringere amicizia solo con coloro i quali erano distanti al massimo tre gradi di separazione e, dunque, solo con *gli amici degli amici degli amici*. Singolare restrizione che era volta a permettere di: a) verificare la veridicità delle notizie pubblicate sui profili; b) ottenere informazioni indirette; c) favorire i contatti fra persone provenienti da analoghi contesti socio-culturali. (Cfr., fra gli altri, M. Adebiyi, O. Ogunlade, *Development of a Social Networking Site with a Networked Library and Conference Chat*, in "Journal of Emerging Trends in Computing and Information Sciences", vol. 2, 2011, n. 8, p. 396-401). Circa la teoria dei sei gradi di separazione e – in particolar modo – dei "mondi piccoli", cfr. A.L. Barabási, *Link. La scienza delle reti*, (trad. it.), Einaudi, 2004.

[26]«Internet è la trama delle nostre vite. Se la tecnologia dell'informazione è l'equivalente odierno dell'elettricità nell'era industriale, Internet potrebbe essere paragonata sia alla rete elettronica sia al motore elettrico, grazie alla sua capacità di distribuire la potenza dell'informazione in tutti i campi dell'attività umana. [...] Internet è la base tecnologica della forma organizzativa nell'età dell'informazione: è il network» (M. Castells, *Galassia Internet*, (trad. it.), Feltrinelli, 2010, p. 13). Sull'affermazione dei nuovi network come forma dominante di organizzazione sociale, cfr. anche B. Wellman, *Physical Place and Cyberplace: The Rise of Personalized Networking*, in "International Journal of Urban and Regional Research", vol. 25, 2001, n. 2, p. 227-252.

[27]A proposito della *comunicazione mediata dal computer* (CMC), cfr. R. Stella, C. Riva, C.M. Scarcelli, M. Drusian, *Sociologia dei new media*, UTET, 2014, in part. pp. 31-33.

[28]In merito ai riverberi dei media sulla comunicazione, cfr. G. Riva, C. Galimberti, G. Mantovani, *La comunicazione virtuale: un'analisi del legame tra psicologia sociale e nuovi ambienti di comunicazione*, in A. Quadrio, L. Venini (a cura di), "La comunicazione nei processi sociali e organizzativi", Franco Angeli, 1997; G. Riva, *Web Usability Revisited: A Situated Approach*, in "PsychNology Journal", vol. 1, 2002, n. 1, p. 18-27; L. Paccagnella, *La comunicazione al computer. Sociologia delle reti telematiche*, il Mulino, 2000; Id., *Sociologia della comunicazione*, il Mulino, 2010; A. Miconi, *Teorie e pratiche del web*, il Mulino, 2014.

[29]Nel Web «[...] la massa dei soggetti riceventi non ha la possibilità di influenzare le caratteristiche e i contenuti dei messaggi trasmessi, che sono invece definiti da un élite di professionisti, spesso sotto il controllo diretto o indiretto del potere politico ed economico» (così, G. Riva, *I social network*, cit., p. 56).

[30]Val la pena ricordare che il termine Web 2.0 si deve alla casa editrice americana O'Reilly Media (fondata da Tim O'Reilly) che, nel 2004, scelse l'espressione "Web 2.0" come titolo per una serie di conferenze dedicate alla "nuova generazione" dei servizi Internet.

[31]Sulla differenza fra mezzi di massa e mezzi per le masse con particolare riferimento alla responsabilità del provider, cfr. G. Saraceni, *I reati informatici. Dalla diffusione di virus all'accesso abusivo*, in A.C. Amato Mangiameli, G. Saraceni, "I reati informatici. Elementi di teoria generale e principali fattispecie criminose", Giappichelli, 2019, in part. p. 105.

[32]Stando alle più recenti indagini pare che, ad oggi, in Rete siano disponibili all'incirca duecentocinquanta piattaforme social differenti. Con specifico riferimento all'Italia, poi, è interessante ricordare che – stando ai risultati dell'indagine *We are social* del gennaio del 2019 – il numero degli utenti attivi sui social si attesta attorno ai 35mln, pari al 59% della popolazione totale. La classifica dei social network più usati dagli italiani, inoltre, vede in testa YouTube, seguito da WhatsApp, Facebook, Instagram e Messenger, mentre Skype si attesta soltanto all'ottava posizione.

[33]In ordine all'analisi degli aspetti che contraddistinguono i social, opportuno – e per rilevanza tecnica sempre attuale – il richiamo ai lavori di: J. Heidemann, M. Klier, F. Probst, *Online social networks: A survey of a global phenomenon*, in "Computer networks", vol. 56, 2012, n. 18, p. 3866-3878; L. Garton, C. Haythornthwaite, B. Wellman, *Studying Online Social Networks*, in "Journal of computer-mediated communication", vol. 3, 1997, n. 1; A. Mislove, M. Marcon, K.P. Gummadi et al., *Measurement and Analysis of Online Social Networks*, in C. Dovrolis, M. Roughan (eds.), "IMC'07 Proceedings of the 2007 ACM SIGCOMM Internet Measurement Conference", 2007, p. 29-42; H. Kwak, C. Lee, H. Park, S. Moon, *What is Twitter, a social network or a news media?*, in J. Freire, S. Chakrabarti (eds.), "Proceedings of the 19th International conference on World wide web", April 26-30, 2010.

[34]È il caso di Facebook. Nota con singolare efficacia ed ironia Scrima: «La frase con cui Facebook ci accoglie ogni volta che ci connettiamo è "A cosa stai pensando?" E noi, lusingati da cotanta attenzione, gli confidiamo tutto, anche i segreti più intimi – che smettono così di esserlo» (S. Scrima, *Socrate su Facebook. Istruzioni filosofiche per non rimanere intrappolati nella rete*, Castelvecchi, 2018, p. 10).

[35]È interessante sottolineare che – da questo punto di vista – i social network si rifanno alla c.d. *Teoria dell'identità sociale* (*Social Identity Theory*) elaborata, a partire dagli anni Settanta, da Tajfel e Turner (cfr. H. Tajfel, J.C. Turner, *An integrative theory of intergroup conflict. The social psychology of intergroup relations?*, in W.G. Austin, S. Worchel (eds.), "The Social Psychology of Intergroup Relations", Brooks/Cole Pub, 1979, p. 33-47).

[36]Cfr. quanto osservato da G. Riva, *I social network*, cit., p. 13.

[37]Sul *cyberspazio*, sulle caratteristiche che lo individuano (de-territorializzazione e de-centralizzazione) e sulle nuove relazioni che si generano al suo interno (tribù virtuali e agorà digitali), d'obbligo il rinvio alle osservazioni di A.C. Amato Mangiameli, *Diritto e Cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Giappichelli, 2007.

[38]Cfr. G. Lovink, *Nichilismo digitale*, cit., p. X.

[39]Fase che implica la trasformazione del World Wide Web in una sorta di database dove i documenti pubblicati vengono associati ad informazioni e dati (metadati) che ne specificano il contesto semantico. Cfr., fra gli altri, V. Eletti, *Complessità, cambiamento, comunicazioni. Dai social network al web 3.0*, Guaraldi, 2012.

[40]Cfr. L. Montagna, *Realtà virtuale e realtà aumentata. Nuovi media per nuovi scenari di business*, Hoepli, 2018; F. Almeida, *Concept and Dimensions of Web 4.0*, in "International Journal of Computers and Technology", vol. 17, 2017, n. 7, p. 7040-7046; N. Choudhury, *World Wide Web and Its Journey from Web 1.0 to Web 4.0*, in "International Journal of Computer Science and Information Technologies", vol. 5, 2014, n. 6, p. 8096-8100.

[41]Cfr. K. Patel, *Incremental Journey for World Wide Web: Introduced with Web 1.0 to Recent Web 5.0*, in "International Journal of Advanced Research in Computer Science and Software Engineering", vol. 3, 2013, n. 10, p. 410-417).

[42]Proposto da KIA, il *R.E.A.D. System* è un prototipo di "guida emotiva" e "adattiva", grazie alla quale il veicolo è in grado di "leggere" le emozioni del pilota e dei passeggeri, adattando così le condizioni di guida e l'habitat interno all'abitacolo.

[43]Cfr. il sito ufficiale dell'evento – svoltosi dal 20 al 25 agosto 2019 – per una più dettagliata descrizione delle novità presentate.

[44]Nonostante tali "anteprime" testimonino gli enormi passi in avanti fatti nel campo della robotica e della domotica – secondo l'autorevole parere di Faggin (fisico al quale si deve l'invenzione del microprocessore e del touchscreen) – l'IA sembra essere ancora molto lontana dall'eguagliare il ragionamento umano (F. Faggin, *Silicio. Dall'invenzione del microprocessore alla nuova scienza della consapevolezza*, Tecniche Nuove, 2019).

[45]«We define social network sites as webbased services that allow individuals to (1) construct a public or semipublic profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system» (D.M. Boyd, N.B. Ellison, *Social network sites. Definition, history, and scholarship*, in "Journal of Computer-Mediated Communications", vol. 13, 2007, n. 1, p. 210-230, in part. 211).

[46]Ed «è per questa ragione che stanno proliferando in tutti i campi dell'economia e della società, superando nella competizione e nelle prestazioni le imprese organizzate verticalmente e le burocrazie centralizzate» (M. Castells, *Galassia Internet*, cit., p. 13).

[47]«La comunicazione consapevole (il linguaggio umano) è ciò che determina la specificità biologica della specie. Dato che la nostra attività è basata sulla comunicazione e Internet trasforma il nostro modo di comunicare, le nostre vite sono segnate profondamente da questa nuova tecnologia di comunicazione [...]» (*ivi*, p. 16).

[48]Un tipico esempio di rappresentazione analogica è costituito dall'orologio automatico, all'interno del quale lo scorrere del tempo viene descritto dal movimento continuo della lancetta dei secondi sul quadrante.

[49]Paradigmatico della rappresentazione digitale è, invece, l'orologio a cristalli liquidi, dove il passare del tempo viene descritto in maniera discontinua (o discreta) dalla successione di scatti che determina l'avanzamento dei numeri.

[50]La codifica delle informazioni – e, dunque, la loro traduzione in forma codice binario (0/1, spento/acceso) e, successivamente, in algoritmi – costituisce un passaggio imprescindibile per consentirne l'elaborazione da parte dei microprocessori, che, per l'appunto, sono in grado di elaborare solo informazioni digitalizzate e rese discrete. Per un ulteriore e più approfondita analisi rinvio a A.C. Amato Mangiameli, *Tra leggi del pensiero e linguaggio giuridico*, in Id., *Informatica giuridica. Appunti e materiali ad uso di lezioni*, Giappichelli, 2010, pp. 89-165, in part. pp. 127-134.

[51]Vantaggio, ma anche pericolo, in quanto talvolta la modularità può anche aprire il varco a violazioni del diritto d'autore. Aspetto particolarmente delicato sul quale si segnala la Risoluzione del Parlamento europeo del 26 marzo 2019 sulla proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale, P8_TA(2019)0231.

[52]Sull'ipertesto e sui suoi effetti, meritano d'esser qui ricordate le parole di Lévy: «l'ipertesto [...] [è] un testo costituito da nodi (gli elementi di informazione, paragrafi, immagini, sequenze musicali ecc.) e da collegamenti tra questi nodi (riferimenti, note, link, 'pulsanti' che indirizzano il passaggio da un nodo all'altro. [...] [È] un testo mobile, caleidoscopico, che mostra tutte le sue facce, gira, si piega e si spiega a volontà di fronte al lettore». Ed è questo motivo che – come spiega il filosofo francese – «l'ipertestualizzazione [...] può essere definita come una tendenza all'indistinzione, alla parziale sovrapposizione delle funzioni di lettura e scrittura». «[...] Un movimento ininterrotto tra interiorità e esteriorità, [...] [fra] l'intimità dell'autore e l'estraneità del lettore rispetto al testo. [...] [un] costante passaggio dal dentro al fuori come in un anello di Moebius» (P. Lèvy, *La virtualizzazione del testo*, in Id., *Il virtuale*, (trad. it.), Raffaello Cortina, 1997, pp. 25-41, in part. pp. 34-35). Sull'ipertesto, cfr. anche: J. Nyce, P. Kahn (eds.), *Da Memex a Hypertext: Vannevar Bush e la macchina per la mente*, (trad. it.), Muzio, 1992; G.P. Landow, *Ipertesto. Il futuro della scrittura*, (trad. it.), Baskerville, 1993, p. 132; J.D. Bolter, *Lo spazio dello scrivere. Computer, ipertesto e la ri-mediazione della stampa*, (trad. it.), Vita e Pensiero, 2002.

[53]Cfr. E. Arielli, P. Bottazzini, *Idee virali. Perché i pensieri si diffondono*, il Mulino, 2018; C. Palazzini, L. Galli, *YouTubers. Chi sono e perché hanno successo*, San Paolo, 2017.

[54]L'approccio ai social network può essere, infatti, determinato da una serie di ragioni assolutamente distinte: personali, ludiche e di svago, professionali, politiche, religiose, di marketing, ecc.

[55]Un altro elemento non trascurabile è dato dal fatto che ai social accedono fasce eterogenee d'età e che, spesso, all'interno del social, tutte quelle differenze che nella vita appaiono evidenti e fungono in un certo qual modo da freno e da filtro alla comunicazione e al contatto, sembrano dissolversi.

[56]Teoria, in base alla quale, più un individuo percepisce che un *medium* è in grado di soddisfare i suoi bisogni e più sarà indotto a farne uso, soprattutto per ovviare a quelle necessità che, in altra maniera, non riesce ad appagare (cfr. E. Katz, J.G. Blumler, M. Gurevitch, *Utilization of Mass Communication by the Individual*, in J.G. Blumler, E. Katz (eds.), "The Uses of Mass Communications: Current Perspectives on Gratifications Research", Sage Publications, 1974, p. 19-31; E. Katz, J.G. Blumler, H. Hass, *On the use of mass media for important things*, in "American Sociological Review", vol. 38, 1973, n. 2, p. 164-181; E. Katz, *Communication research since Lazarsfeld*, in "Public Opinion Quarterly", vol. 51, 1987, n. 4, p. 525-545; E. Katz, *Mass communication research and the study of culture*, in "Studies in Public Communications", vol. 2, 1959, p. 1-6; D. Mcquail, *With the benefit of hindsight. Reflections on uses and gratifications research*, in "Critical Studies in Mass Communication", vol. 1, 1984, n. 2, p. 177-193.

[57]Secondo il noto psicologo americano i bisogni che ognuno di noi avverte non sono isolati e "a sé stanti", ma tendono a seguire in una gerarchia e un ordine di priorità. Per questo motivo, Maslow dispone le principali necessità dell'individuo all'interno di una piramide dove, alla base, ci sono i bisogni fisiologici di tipo primario (ossia tutte le necessità direttamente connesse alla sopravvivenza), mentre, al vertice, quelli che hanno a che vedere con l'autorealizzazione personale. Ciò che è importante sottolineare è che, all'interno della piramide, il passaggio da un bisogno ad un altro avviene "per soddisfazione". In pratica, per accedere – e avvertire – il bisogno successivo (più complesso ed elevato), è necessario aver già appagato quello precedente (di livello inferiore) (A.H. Maslow, *Motivation and Personality*, Edition by Harper & Row, 1954).

[58]Cfr. F. Colombo, *"Il 'dire di sé' sul Web 2.0"*, in Id., "Il potere socievole. Storia e critica dei social media", Mondadori, 2013, p. 138 ss.

[59]Cfr. G. Riva, *Selfie. Narcisismo e identità*, il Mulino, 2016.

[60]Neologismo, sempre più diffuso ed in voga, che riprendo da S. Scrima, *op. cit.*, in part. p. 8. Cfr. anche G. Lovink, *Ossessioni collettive. Critica dei social media*, cit., *passim*.

[61]Like che, oramai, non hanno più solo la funzione di gratificare l'autostima di chi pubblica, ma che hanno acquisito anche un vero e proprio valore economico. Come avviene, ad esempio, su YouTube, dove i profitti dei video caricati sono direttamente proporzionali al numero degli utenti iscritti al canale e ai consensi che – di volta in volta – riscuotono i diversi filmati (vlog, tutorial, ecc.). (A proposito del "fenomeno like", cfr., fra gli altri: G. Lovink, *Zero comments. Teoria critica di internet*, Mondadori, 2008; Id., *L'abisso dei social media. Nuove reti oltre l'economia dei like*, (trad. it.), Università Bocconi, 2016).

[62]A questo proposito, merita d'esser ricordato quanto affermato, alcuni anni fa, da Lewis: «[...] Al cuore del social networking c'è uno scambio di informazioni personali. Gli utenti sono ben contenti di rivelare dettagli intimi della propria vita personale, di postare informazioni accurate, di condividere fotografie» (P. Lewis, *Teenager networking websites face anti-paedophilie investigation*, in "The Guardian", 3 July 2006).

[63]Z. Bauman, D. Lyon, *Sesto potere. La sorveglianza nella modernità liquida*, (trad. it.), Laterza, 2015, pp. 15-17.

[64]R. Silverstone, *What's New about New Media?*, in "New Media & Society", vol. 1, 1999, n. 1, p. 10-12.

[65]Moltissimi gli studiosi che si sono occupati della questione, fra questi: J.D. Bolter, R. Grusin, *Remediation. Competizione e integrazione tra media vecchi e nuovi*, (trad. it.), Guerini e Associati, 2003; L. Gitelman, G.B. Pingree (eds.), *New Media. 1740-1915*, MIT Press, 2003; D. Gauntlett, R. Horsley (eds.), *Web.Studies*, Bloomsbury Academic, 2004; L. Gorman, D. McLean, *Media e società nel mondo contemporaneo*, (trad. it.), il Mulino, 2011; T. Flew, *New Media: an introduction*, Oxford University Press, 2008; M. Lister, J. Dovey, S. Giddings et al. (eds.), *New Media. A critical introduction*, Routledge, 2008; N. Couldry, *Sociologia dei nuovi media. Teoria sociale e pratiche mediali digitali*, (trad. it.), Pearson, 2015.

[66]Sulla distinzione fra vecchi e nuovi media cfr. anche G. Granieri, *La società digitale*, Laterza, 2006.

[67]M. Spitzer, *op. cit.*, p. 18.

[68]Cfr., fra gli altri, R. Silverstone, *Televisione e vita quotidiana*, (trad. it.), il Mulino, 2000; R. Stella, C. Riva, C.M. Scarcelli, M. Drusian, *op. cit.*, in part. pp. 6-7.

[69]P. Lévy, *Il nuovo spazio pubblico*, in Id., "Cyberdemocrazia", (trad. it.), Raffaello Cortina, 2008, p. 37.

[70]Cfr. V. Hugo, *Notre-Dame de Paris*, (trad. it.), Einaudi, 2007.

[71]D'obbligo il rinvio a M. Serres, *Non è un mondo per vecchi*, (trad. it.), Bollati Boringhieri, 2013, *passim*.

[72]Cfr. P. Virilio, *L'orizzonte negativo. Saggio di dromoscopia*, (trad. it.), Costa & Nolan, 2005.

[73]Id., *La bomba informatica*, (trad. it.), Raffaello Cortina, 2000, in part. p. 9.

[74]Per un ulteriore approfondimento, si vedano, fra gli altri, K.Y.A. McKenna, J.A. Bargh, *Causes and consequences of social interaction on the Internet. A conceptual framework*, in "Media Psychology", vol. 1, 1999, n. 3, p. 249-269; K.Y.A. McKenna, *Through the Internet looking glass. Expressing and validating the true self*, in A. Joinson, K.Y.A. McKenna, T. Postmes, U.D. Reips (eds.), "The Oxford handbook of Internet Psychology", Oxford University Press, 2007, p. 205-221; A.L. Gonzales, J.T. Hancock, *Mirror, Mirror on my Facebook Wall: Effects of Exposure to Facebook on Self-Esteem*, in "Cyberpsychology, Behavior, and Social Networking", vol. 14, 2011, n. 1-2, p. 79-83.

[75]L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, (trad. it.), Raffaello Cortina, 2017, in part. p. 69. A proposto del rapporto fra new media e costruzione del sé, cfr. anche G. Riva, *I social network*, cit., p. 119; F. Colombo, *Il potere socievole*, cit., p. 139.

[76]W. James, *Principi di psicologia. Il flusso di coscienza*, cap. IX-X, (trad. it.), Mondadori, 1998.

[77]«Perfino nei più insignificanti dettagli della nostra vita, non siamo un tutto costruito materialmente, identico per tutto il mondo e di cui ciascuno potrebbe avere coscienza come di un quaderno delle spese o di un testamento; la nostra personalità sociale è una creazione del pensiero altrui. [...] Riempiamo l'apparenza fisica dell'essere che ci sta davanti di tutte le nozioni che abbiamo su di lui, e, nell'insieme che ci rappresentiamo, queste nozioni costituiscono la parte più importante. Finiscono per riempire così perfettamente le guance, per seguire con tale esatta aderenza la linea del naso, si industriano così bene di sfumare la sonorità della voce come se questa non fosse che un involucro trasparente, che ogni volta che vediamo quel viso, che sentiamo quella voce, ritroviamo e diamo retta soltanto a quelle nozioni» (M. Proust, *Alla ricerca del tempo perduto. Dalla parte di Swann*, (trad. it.), Einaudi, 1990).

[78]Così, J. Rifkin, *La civiltà dell'empatia. La corsa verso la coscienza globale nel mondo in crisi*, (trad. it.), Mondadori, 2011, p. 537.

[79]Cfr. F. Colombo, *Di cosa parliamo quando parliamo di social media*, in Id., "Il potere socievole", cit., pp. 38-39.

[80]*Ibidem*.

[81]«[...] la principale trasformazione nelle società complesse si è verificata attraverso la sostituzione delle comunità spaziali con i network come forme prime di socialità» (cfr. M. Castells, *Comunità virtuali o società in rete?*, in Id., "Galassia Internet", cit., p. 117).

[82]Cfr. G. Riva, *I social network*, cit., p. 14.

[83]Circa la nozione di inter-realtà, cfr. J. Van Kokswijk, *Hum@n: Telecoms and Internet as Interface to Interreality: a Search for Adaptive Technology and Defining Users*, Bergboek, 2003; G. Riva, *Interreality: A New Paradigm for E-health*, in "Studies in Health Technology and Informatics", vol. 144, 2009, p. 3-7; Id., *Irrealtà. Reti fisiche e digitali e post-verità*, in "il Mulino", 2017, n. 2, pp. 326-334.

[84]A proposito della comunità di luogo (e, in modo particolare, del rapporto e del distinguo fra comunità e società), d'obbligo il rinvio alla nota teoria elaborata da F. Tönnies, *Comunità e società*, (trad. it.), Laterza, 1963, pp. 45-46.

[85]Sul passaggio dalla comunità alla Rete e sulla differenza che si dà fra le due dimensioni, meritano d'esser qui ricordate le osservazioni di Bauman: «[...] appartenere a una comunità è una condizione molto più sicura e affidabile che far parte di una rete, anche se comporta sicuramente più vincoli e più obblighi. La comunità ti osserva da vicino e ti lascia poco spazio di manovra (può metterti al bando e spedirti in esilio, ma non ti consente di uscirne di tua iniziativa), mentre la rete può non preoccuparsi minimamente che tu obbedisca alle sue norme [...], e dunque ti lascerà le briglie molto più lente e, soprattutto, se te ne vai non ti penalizzerà» (Z. Bauman, D. Lyon, *op. cit.*, p. 25).

[86]In particolare – come sottolinea Lévy – i nuovi media «[...] non sono più legati ad una zona geografica, ma ad una comunità virtuale di ascoltatori, spettatori o lettori che possono abitare ovunque nel mondo» (P. Lévy, *Cyberdemocrazia*, cit., p. 48).

[87]M. Castells, *Comunità virtuali o società in rete?*, cit., p. 130.

[88]G. Simmel, *Socievolezza*, (trad. it.), Armando Editore, 1997.

[89]Come Lévy evidenziava già alcuni anni fa: «l'evoluzione contemporanea della libertà di espressione nel cyberspazio, come l'esplosione quantitativa e qualitativa del Web, sembra portarci verso una situazione dove tutte le istituzioni, le imprese, i gruppi, le équipe e gli individui diventeranno mass media di loro stessi e gestiranno la loro comunità virtuale

che corrisponde alla loro zona di influenza sociale» (P. Lévy, *Cyberdemocrazia*, cit., p. 52).

[90] «I nuovi sviluppi tecnologici sembrano accrescere le possibilità che l'individualismo in rete diventi la nuova forma dominante di socialità». Assistiamo, invero, allo sviluppo e all'aumento di un networking sempre più personalizzato per un'ampia gamma di situazioni sociali. «[...] tendenze che equivalgono al trionfo dell'individualismo» (M. Castells, *Comunità virtuali o società in rete?*, cit., pp. 130-131).

[91] Sulla nascita di comunità incentrate sul singolo, cfr. M. Corney, *Sustaining the New Economy. Work, Family and Community in the Information Age*, Cambridge University Press, 2000; R. Putnam, *Bowling Alone. The Collapse and Revival of American Community*, Simon & Schuster, 2000; M. Castells, *La nascita della società in rete*, (trad. it.), Egea, 2002.

[92] A proposito dei riverberi dell'individualismo, cfr. A.C. Amato Mangiameli, *Tra pensiero moderno e diritto. Oltre l'individualismo possessivo*, in L. Congiunti, A. Ndreca, G. Formica (a cura di), "Oltre l'individualismo. Relazioni e relazionalità per ripensare l'identità", Urbaniana University Press, 2017, in part. pp. 101-113. Inoltre, per un'agile ricostruzione v. M.N. Campagnoli, *Ragionando oltre l'individualismo. Appunti e riflessioni a partire da una lettura*, in "Rivista di Filosofia del Diritto", 2019, n. 1, pp. 205-219.

[93] In tal senso, cfr. B. Wellman, *Physical place and cyberspace: the rise of networked individualism*, in "International Journal of Urban and Regional Research", vol. 25, 2001, n. 2, p. 227-252.

[94] «[...] in un mondo commerciale che strumentalizza in maniera crescente le tendenze narcisistiche e voyeuristiche, Internet» e i social network diventano «uno strumento imbattibile per trasformare in merce ogni ambito della vita» (J. Rifkin, *op. cit.*, pp. 537-538).

[95] Particolarmente interessanti, sul punto, le recenti riflessioni di G. Ziccardi, *L'uso delle nuove tecnologie in politica*, in Id., "Tecnologie per il potere", Raffaello Cortina, 2019, in part., pp. 15-50.

[96] Fra i più noti disturbi conseguenti all'uso (e all'abuso) dei social network: la cyberdipendenza (molto simile a quella creata dall'assunzione di alcool o di sostanze psicotrope) e l'incapacità di controllare il tempo trascorso on-line; il multitasking che, a lungo andare, incrementa la propensione alla distrazione e riduce la capacità di immagazzinare informazioni; la sindrome da vibrazione fantasma che porta al controllo ossessivo e continuo dello smartphone e/o del tablet; l'insonnia digitale, ovvero l'alterazione dei ritmi circadiani e lo sviluppo di forme; la depressione digitale, la perdita di interesse per la vita reale e di qualsiasi forma di empatia verso gli altri (cfr. M. Spitzer, *op. cit.*, in part. pp. 153-176 e pp. 279-290).

[97] Si veda quanto osservato all'inizio in merito alla sindrome da *hikikomori*, *infra*, paragrafo 1.

[98] Cfr. G. Anders, *Il mondo dopo l'uomo. Tecnica e violenza*, (trad. it.), Mimesis, 2008, p. 93.

[99] Cfr. B.-C. Han, *Nello sciame. Visioni del digitale*, (trad. it.), Nottetempo, 2015.

[100] Sulla sindrome di Parigi, v.: P. Adam, *Le Syndrome de Paris*, Inventaire, 2005; A. Viala, H. Ota, M.N. Vacheron et al., *Les japonais en voyage pathologique à Paris: un modèle original de prise en charge transculturelle*, in "Nervure de journal Psychiatrie", 2004, n. 5, pp. 31-34.

[101] Non a caso, con una pittoresca – ma efficace – metafora Siva Vaidhyanathan sottolinea che i social (l'autore, per il vero, parla in modo particolare a Fecebook) ci attirano attraverso un meccanismo simile a quello delle patatine fritte, facendoci assaporare piccoli ma frequenti piaceri ai quali ci assuefacciamo presto. Gratificazioni che – fra le altre cose – non implicano, né particolari capacità critiche, né men che meno un'analisi approfondita dell'esperienza che stiamo facendo (S. Vaidhyanathan, *Anti-Social Media*, Oxford University Press, 2018, p. 35).

[102] Cfr. C. Brod, *Technostress. The Human Cost of the Computer Revolution*, Addison-Wesley, 1984; T.S. Ragu-Nathan, M. Tarafdar, B.S. Ragu-Nathan, Q. Tu, *The consequences of technostress for the users in organizations. Conceptual development and empirical validation*, in "Information Systems Research", vol. 19, 2008, n. 4, p. 417-433; Q.E. Booker, C.M. Rebman Jr., F.L. Kitchens, *A model for testing technostress in the online education environment. An exploratoty study*, in "Issues in Information Systems", vol. 15, 2014, n. 2, p. 214-222.

[103] Espressione con la quale rinvio alle ricostruzioni di S. Turkle, *La vita sullo schermo*, cit.), che, più di vent'anni fa – e tra i primi – si interrogava sui riverberi legati all'avvento di Internet.

[104] Cfr. J.M. Twenge, *Iperconnessi. Perché i ragazzi oggi crescono meno ribelli, più tolleranti, meno felici e del tutto impreparati a diventare adulti*, (trad. it.), Einaudi, 2018.

[105] Notizie che vengono diffuse da bots programmati per fingersi umani e per trarre in inganno la platea degli utenti, allo scopo di creare tensioni o di orientare le decisioni politiche. Fenomeno che è stato già oggetto d'attenzione da parte del legislatore, come testimonia il d.d.l. 2688 del 2017 "Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica", che prevede l'introduzione di una contravvenzione (art. 656-*bis*) e di due nuove fattispecie di criminose (artt. 265-*bis* e 265-*ter*); ed il d.d.l. 3001 del 2017 "Norme generali in materia di social network e per il contrasto della diffusione su internet di contenuti illeciti e delle fake news", che mira a «responsabilizzare i fornitori dei servizi di social network sui contenuti veicolati attraverso le proprie piattaforme, tutelare gli utenti da notizie costruite intenzionalmente per trarli in inganno e contrastare la commissione di reati attraverso la rete». Sul tema, fra i tanti, mi permetto di rinviare a M.N. Campagnoli, *Informazione, social network & diritto. Dalle fake news all'hate speech online. Risvolti sociologici, profili giuridici, interventi normativi*, Key, 2020.

[106] Di cui Zao è solo l'ultima minaccia in ordine di tempo. App virale, che affascina gli utenti consentendo di scambiare i loro volti con quelli dei personaggi cinematografici e/o televisivi, e che – avendo accesso alle loro immagini – può facilmente aprire il varco a pericolose violazioni e sottrazioni (cfr. G. Scorza, *Arriva Zao e di nuovo la privacy va in fumo per una risata*, in "L'Espresso", 3 settembre 2019).

[107] Per uno specifico approfondimento G. Ziccardi, *Cyberstalking e molestie portate con strumenti elettronici: aspetti informatico-giuridici*, in "Rassegna italiana di criminologia", 2012, n. 3, pp. 160-173.

[108] A contrasto del quale è intervenuta la l. 29 maggio 2017, n. 71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo". Per un'interessante analisi della fattispecie cfr., fra gli altri, F. Tonioni, *Cyberbullismo*, Mondadori, 2014; M.L. Genta, A. Brighi, A. Guarini, *Bullismo elettronico: fattori di rischio connessi alle nuove tecnologie*, Carocci, 2009.

[109] Particolare comportamento che prevede la creazione di pagine e/o di gruppi volutamente provocatori, polemici e incitanti alla violenza (ad es., "non vogliamo le persone di colore"; "tutti contro i musulmani"; "no a down"; ecc.), che hanno lo scopo di scatenare discussioni e litigi online. Cfr. D. Facchini, *Trolls Inc. Il volto autoritario della rete tra libertà d'insulto, pubblicità e privacy*, Altreconomia, 2015.

[110] E, cioè, la diffusione di espressioni d'odio e discriminatorie. Condotta sulla quale si segnala: Autorità per le Garanzie nelle Comunicazioni (AGCOM), Allegato B alla

delibera n. 157/19/CONS del 15 maggio 2019, con la quale è stato approvato il "Regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di non discriminazione e di contrasto all'hate speech".

[111]Vale a dire, l'invio di testi o immagini sessualmente esplicite tramite Internet o telefono cellulare. V., fra gli altri, F. Currò, *Il sexting*, in "Profiling. I profili dell'abuso", 2017, n. 2; S. Shariff, *Sexiting e cyberbullismo. Quali limiti per i ragazzi sempre connessi?*, (trad. it.), Edra, 2016.

[112]Attività estorsiva a sfondo sessuale (ricatto sessuale), che, in una prima fase, si avvale degli strumenti e dei canali informatici per contattare le vittime e per indurle a pratiche sessuali (invio di foto, video, testi espliciti); mentre, nella seconda fase, implica l'estorsione. La vittima viene, infatti, costretta al pagamento di una somma di denaro in cambio della mancata divulgazione del materiale compromettente precedentemente condiviso. Con specifico riferimento alla condotta agita nei confronti dei minori, cfr. Europol, *Online sexual coercion and extortion as a form of crime affecting children: law enforcement perspective*, May 2017.

[113]Per un'agile ricostruzione, rinvio a M.N. Campagnoli, *"Revenge porn" when the gender violence goes viral*, in "Humanities and Rights", 2021, n. 2, p. 146-178.

[114]Riprendo, qui, l'efficace espressione utilizzata da G. Ziccardi, *Social media. Uso sicuro di web, messaggistica, chat e social network*, Corriere della Sera, 2017, pp. 7-12.

[115]A tal proposito, è interessante ricordare che negli anni si è sviluppata la netiquette: un insieme di regole che disciplinano il comportamento che gli utenti dovrebbero tenere in Rete. Un galateo per il Web che non è disciplinato da leggi *ad hoc*, ma che si fonda su una serie di pratiche e di convenzioni generali e condivise. Regole che, tuttavia, vengono spesso richiamate all'interno dei contratti di fornitura di servizi di accesso da parte dei provider e delle quali il mancato rispetto comporta una generale disapprovazione da parte degli altri utenti e, nei casi più gravi, sono punite tramite *ban*.

[116]P. Lévy, *Il virtuale*, cit., p. 6: «Il virtuale [...] non si contrappone al reale ma all'attuale. Contrariamente al possibile, statico e già costituito, il virtuale è come un complesso problematico, il nodo di tendenze e di forze che accompagna una situazione, un evento, un oggetto o un'entità qualsiasi, e che richiede un processo di trasformazione: l'attualizzazione».

[117]Stringa pubblicata sul *New Yorker* il 5 luglio 1993.

[118]Così Riva: «Nonostante siano nati proprio per evitare il problema dell'anonimato, la loro progressiva trasformazione da reti chiuse in reti aperte consente nuovamente agli utenti di nascondere facilmente la propria identità. E come mostrato da decine di studi su questi temi, non potendo riconoscere l'identità del soggetto si riduce il controllo sociale e, quindi, gli utenti tendono a comportarsi in maniera più disinibita» (G. Riva, *I social network*, cit., p. 139.

[119]Tantissimi i provvedimenti adottati in ambito europeo, fra i più noti ed importanti: la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 (in tema di tutela dei dati personali); la Convenzione di Budapest del Consiglio d'Europa del 23 novembre del 2001 (sulla criminalità informatica); la Risoluzione legislativa del Parlamento europeo sulla proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale, P8_TA(2019)0231, cit.

[120]A livello nazionale, si possono ricordare: la l. 23 dicembre 1993, n. 547 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"); la l. 31 dicembre 1996, n. 675 ("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"); il d.lgs. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali"); il d.lgs. 7 marzo 2005, n. 82 ("Codice della Pubblica amministrazione digitale"); la l. 6 febbraio 2006, n. 38 ("Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"); la l. 18 marzo 2008, n. 48 ("Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica"); la l. 23 aprile 2009, n. 38 ("Conversione in legge, con modificazioni, del decreto-legge 23 febbraio 2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori").

[121]Di qui, l'importanza e l'utilità delle tante campagne di informazione e delle iniziative realizzate nell'ambito del Progetto SIC (Generazioni Connesse). Progetto finanziato dalla Commissione europea, coordinato dal Ministero dell'Istruzione, dell'Università e della Ricerca, e realizzato in collaborazione con l'Agenzia Generale per l'Infanzia e l'adolescenza, con la Polizia Postale e delle Comunicazioni, nonché, con Save the Children, Telefono Azzurro, e con il Movimento in Difesa del Cittadino.

[122]Cfr. L. Di Mele, E. Isatto, *Se la competenza digitale non contrasta il cyber-bullismo*, in "Media Education. Studi, ricerche, buone pratiche", vol. 9, 2018, n. 1, pp. 146-160.

[123]Così, l'art. 8 co. 1: «[...] per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni». E, proprio con riferimento alla possibilità che gli Stati membri hanno di stabilire un'età inferiore a quella prevista dal GDPR, è interessante ricordare che il d.lgs. 10 agosto 2018, n. 101, con l'articolo 2-*quinquies*, ha previsto un limite di 14 anni.

[124]Cfr. H. Jenkins, *Culture partecipative e competenze digitali. Media education per il XXI secolo*, Feltrinelli, 2010; P.G. Lange, M. Ito, *Creative production*, in M. Ito, S. Baumer, M. Bittanti et al., (eds.), "Hanging Out, Messing Around, and Geeking Out: Kids Living and Learning with New Media", MIT Press, 2010, p. 243-293.

[125]Cfr. G. Riva, *Social network*, cit., p. 169; R. Trinchero, *Io non ho paura. Capire e affrontare il bullismo*, Franco Angeli, 2013.

[126]C. Baudelaire, *Les Fleurs du Mal*, Gallimard, 2015.

* * *

Relationships and loneliness on the Net. #Social_relation_&_confessional_society

Abstract: As part of a discussion dedicated to Internet governance, a specific observation must be dedicated to the particular forms of communication and relationship that develop within social media. Hasty interactions and solitary narratives, which must be the subject of attention and regulation.

Keywords: Social network – Communication – Relation – Like – Confessional society

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0078
Articolo sottoposto a peer review

Diritti "in rete" e libertà religiosa. L'effettività dei diritti attraverso l'efficacia della Internet governance

Antonella Losanno

La cultura digitale ha una valenza che risente della globalizzazione in atto e ne determina lo sviluppo. Il presente contributo pone l'accento sulla possibilità di considerare un esercizio della libertà religiosa nella società digitale, ovvero verifica come le libertà e i diritti, che, come corollari, discendono dalla libertà religiosa, possano coniugarsi con un esercizio "on line" del culto. Il digitale è diventato il mezzo che abbatte più di tutti le barriere di spazio e tempo: la stessa essenziale assemblea di fedeli che diventa una assemblea, aperta, ma nello stesso tempo non virtuale, quanto piuttosto caratterizzata dalla nuova forma di partecipazione. Partendo dall'analisi dell'assegnazione dei nomi di dominio di primo livello, sarà poi evidenziata la centralità di attuare una efficace Internet governance, finalizzata a garantire fra gli altri, integrazione globale, difesa dei diritti delle persone, e in generale opportunità culturali, economiche, sociali per ognuno nel rispetto dell'effettiva tutela del diritto di ciascuno alla privacy e alla protezione dei dati personali.

Accesso a Internet – Diritti in "rete" – Libertà religiosa – Privacy – Internet governance

Sommario: *1. Considerazioni introduttive – 2. Diritto "alla rete" e diritti "in rete" – 3. Culto on line e cyberspazio. Verso una libertà religiosa "informatica" – 4. L'assegnazione dei nomi a dominio di primo livello: il TLD* .catholic *– 5. L'effettività dei diritti (e della libertà religiosa) in Internet: l'efficacia della Internet governance anche attraverso un'efficiente "gestione" dei dati personali – 6. Osservazioni conclusive*

1. Considerazioni introduttive

L'interazione tra l'individuo e la rete dà vita a molteplici e complesse relazioni che si possono sintetizzare da un lato nei diritti nascenti dalla rete e dall'altro nell'esercizio dei diritti in rete. Più che "un gioco di parole" i due profili evidenziano una problematica sostanziale diversa: la prima incentrata sulla necessità di trovare una giusta e per certi versi "congrua e consona" tutela dei cd. "nuovi diritti" che nascono dalla coscienza sociale, a seguito dello sviluppo tecnologico[1], ricollocandoli nell'ambito di una tutela ordinamentale[2]; la seconda più tesa a riscontrare se i diritti della persona, laddove esercitati in rete, abbiano effettivamente in questo "nuovo spazio", inteso quale nuovo luogo di esercizio, una concreta tutela per come l'ordinamento l'appresta[3].

In particolare, per i primi sorge immediato interrogarsi sul problema della loro consistenza giuridica ovvero chiedersi se possano ritenersi quali mere liceità facilitate dall'evoluzione del mezzo tecnologico o, piuttosto, veri e propri "agere posse" giuridicamente assistiti: una volta stabilito che di diritti soggettivi si tratti, rimane da chiarire se possa essere riconosciuta una loro dignità costituzionale senza una loro catalogazione fra i diritti previsti dalla Costituzione.

A. Losanno ha conseguito il titolo di dottore di ricerca in Diritto ecclesiastico presso l'Università di Salerno, già docente di Diritto e Religioni presso l'Università Magna Graecia di Catanzaro, dal 2020 è docente a contratto presso l'Istituto di Studi Politici "San Pio V" di Roma.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

Senza avere la pretesa di un'analisi che tenti di addivenire ad una soluzione delle questioni poste, molteplici e in evoluzione, si tenterà di porre l'attenzione sul secondo profilo, incentrando e caratterizzando l'indagine sull'esercizio "in rete" di talune situazioni soggettive espressamente riconosciute in Costituzione, nello specifico, fra le altre, la libertà di religione e di culto con i relativi diritti e libertà ad essa collegati dal cui esercizio discende una complessa problematica relativa all'applicazione delle garanzie costituzionali. I diritti di libertà, infatti, non sono del tutto sovrapponibili tra loro, ma presentano, in quanto specifici istituti di diritto positivo, peculiari discipline costituzionali che presuppongono una diversa declinazione dei valori in gioco che a loro volta vanno raffrontati con lo spazio virtuale nel quale sono esercitati.

Si potrebbe dire, che in base a tale accezione "i diritti tradizionali" stiano subendo una sorta di "modernizzazione" per nuovi modo e luogo di esercizio. Ma procediamo per gradi.

2. Diritto "alla rete" e diritti "in rete"

La rete rappresenta un luogo, anche se virtuale, in cui ognuno si ritrova. L'essere in rete può essere ormai definito un diritto di ciascuno, cosicché in Internet[4] ciascuno, non quale soggetto passivo dell'informazione ma nella sua interattività, può esercitare on line i propri diritti, dalla libertà di espressione all'iniziativa economica privata, e le proprie libertà fondamentali, ma anche potenziare l'accesso agli altri diritti umani fondamentali: valga per tutti il diritto all'istruzione o il diritto di partecipare alla vita culturale o di trarre i benefici del progresso scientifico nell'attuazione, ad esempio, del diritto alla salute. Inoltre, attraverso la rete, le libertà si sono potute sviluppare ed espandere verso nuove mete dell'agire umano non più e non solo racchiuse all'interno dei perimetri normativi statali, ma protese verso una extraterritorialità che trascende i sistemi valoriali delle Costituzioni[5] dei singoli Stati.

La centralità della persona e il suo *agere* nella rete hanno fatto sì che a livello sovranazionale o dei singoli Stati, a ben vedere, è stato riconosciuto un vero e proprio diritto all'accesso alla rete[6].

Emblematico, a riguardo, il riconoscimento da parte del Consiglio sui Diritti Umani delle Nazioni Unite[7] che invita gli Stati a favorire l'accesso a Internet quale diritto fondamentale della persona umana[8] che consente di accelerare il progresso e lo sviluppo in ogni sua forma e che può essere veramente tale se ne è garantita la neutralità[9].

Su questa linea si pongono le statuizioni europee[10]. Il Regolamento UE 2015/2120 al considerando n. 1 dispone che il testo di legge ha l'obiettivo di «definire norme comuni per garantire un trattamento equo e non discriminatorio del traffico nella fornitura di servizi di accesso a Internet e tutelare i relativi diritti degli utenti finali (...), tutelare gli utenti finali e, garantire, al contempo, il funzionamento ininterrotto dell'ecosistema di Internet quale volano per l'innovazione»[11].

La previsione che si ricollega direttamente al diritto di accesso a Internet, così come previsto nella Carta dei diritti di Internet[12], evidenzia l'universalità e l'impegno nel rimuovere tutti quegli ostacoli che possono impedirne l'effettivo esercizio allorquando specificamente statuisce che «gli utenti finali dovrebbero avere il diritto di accedere a informazioni e contenuti e di diffonderli, nonché di utilizzare e fornire applicazioni e servizi senza discriminazioni, tramite il loro servizio di accesso a Internet».

Nell'evidente soluzione di continuità della citata statuizione rispetto al riconoscimento nazionale, la Carta dei diritti di Internet all'art. 2 dispone infatti: «l'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale; ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale». Internet diventa allo stesso tempo diritto della persona e mezzo a cui accedere per lo sviluppo completo della sua personalità. La Carta prevede altresì che «le istituzioni pubbliche assicurano la creazione, l'uso e la diffusione della conoscenza in rete intesa come bene accessibile e fruibile da parte di ogni soggetto»[13]. «Ogni persona, ha diritto ad essere posta in condizione di acquisire e di aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali. Le istituzioni pubbliche promuovono, in particolare attraverso il sistema dell'istruzione e della formazione, l'educazione all'uso consapevole di Internet e intervengono per rimuovere ogni forma di ritardo culturale che precluda o limiti l'utilizzo di Internet da parte delle persone. L'uso consapevole di Internet è fondamentale garanzia per lo sviluppo di uguali possibilità di crescita individuale e collettiva, il riequilibrio democratico delle differenze di potere sulla rete tra attori economici, istituzioni e cittadini, la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui»[14]. E in questi termini l'approccio ad una consapevole, in quanto basata sulla conoscenza, cultura digitale diventa fondamentale anche nell'ottica di esercizio

del culto e di rendere effettivo e concreto il differente approccio alle manifestazioni di fede.

Un riconoscimento, quello effettuato nella Carta dei diritti di Internet, «... di principi e diritti. I principi di riferimento sono libertà uguaglianza e dignità. I quali, poi, si traducono in questo documento, anzitutto nel diritto di accesso alla Rete, ad Internet, come diritto fondamentale della persona, poiché Internet è ormai uno spazio nel quale si manifesta sia l'attività pubblica sia lo svolgimento della vita privata. E questo evidentemente è una condizione di eguaglianza»[15]. Difatti, la Carta trova la sua fondatezza direttamente nella previsione dell'art. 3 della Carta costituzionale e nel principio di eguaglianza, ma anche nella manifestazione del pensiero di cui all'articolo 21 della Costituzione[16] che è attuazione della stessa libertà religiosa e che proprio grazie alla rete ha trovato una nuova forma di espressione che ha mutato, a dire il vero, anche il ruolo della persona stessa.

Tale diritto va qui inteso in riferimento sia alla libertà di esprimere le proprie opinioni sia alla libertà di informazione, cioè di informare e di essere informati. Perciò viene preso in considerazione non soltanto l'uso della parola e dello scritto, ma anche "ogni altro mezzo di diffusione" quale la radio, la televisione, il cinema, le riproduzioni audiovisive e, per estensione, Internet. L'individuo non "subisce" l'informazione, ma "fa" l'informazione[17]. Ne consegue che la libertà di espressione su Internet risulta essere ampliata in forma così illimitata che è necessario un bilanciamento anche con altri diritti fondamentali, quali il diritto alla privacy, alla trasparenza delle fonti di informazione e alla protezione dai reati informatici, diritti fondamentali che si riferiscono alla tutela della vita privata in un ambiente pubblico.

Il diritto di accesso ad Internet, con l'evolversi della società digitale, è presupposto inoltre di numerosi altri diritti[18] e rappresenta la vera sfida della Carta che riconosce il diritto di accesso come diritto fondamentale e che si propone di offrire un insieme di principi e di valori di alto livello fondati sul rispetto della dignità, della libertà, della eguaglianza e della diversità di ogni persona[19]. Tale diritto, pur non trovando esplicito riferimento in Costituzione, ha trovato riconoscimento nello specifico nel Codice dell'Amministrazione Digitale (CAD), testo unico che riunisce le norme riguardanti l'informatizzazione della pubblica amministrazione, ove viene riconosciuto quale presupposto fondamentale per la costruzione di una cittadinanza digitale[20].

A riguardo fondamentale anche il ruolo assunto dal 2014 dalla Commissione europea che monitora i progressi compiuti dagli Stati membri nel settore digitale e pubblica relazioni annuali sull'indice di digitalizzazione dell'economia e della società (DESI)[21]. Anche nell'ultimo rapporto, l'Italia è significativamente in ritardo rispetto ad altri paesi dell'UE in termini di capitale umano. Rispetto alla media UE, registra infatti livelli di competenze digitali di base e avanzate molto bassi[22]. Sono necessarie misure volte a migliorare le competenze digitali di base della popolazione, ad aumentare l'offerta formativa in materia di competenze digitali avanzate, a riqualificare la forza lavoro e a migliorarne le competenze[23]. Nel 2020 l'Italia ha varato la sua prima Strategia Nazionale per le Competenze Digitali, che definisce un approccio globale allo sviluppo delle competenze digitali per colmare i divari con gli altri paesi dell'UE[24]. La strategia comprende quattro assi di intervento e contempla un'ampia gamma di settori e vede quali gruppi di destinatari, fra gli altri, studenti inseriti in percorsi di istruzione e formazione, per integrare le competenze informatiche nelle scuole primarie e secondarie e nei curricula universitari e di istruzione superiore; pubblico in generale, per sviluppare le competenze digitali necessarie a esercitare i diritti di cittadinanza sostenendo l'alfabetizzazione digitale della popolazione.

Al centro delle esperienze di apprendimento, per garantire sicurezza e inclusione dei nuovi cittadini, deve essere posta, pertanto, l'educazione all'uso consapevole di Internet. L'utilizzo di Internet può infatti essere una "garanzia" per lo sviluppo di uguali possibilità di crescita del singolo soggetto e della intera collettività. È innegabile, infatti, che il *diritto alla conoscenza e all'educazione in rete* significa il possesso di competenze digitali e la capacità di utilizzare Internet in modo consapevole per l'esercizio dei diritti e delle libertà fondamentali, condizione necessaria per vivere questo "allargamento" della cittadinanza alla dimensione digitale[25].

3. Culto on line e cyberspazio. Verso una libertà religiosa "informatica"

Il tentativo di delineare i confini giuridici della rete è diventato ancor più importante in quest'ultimo biennio, caratterizzato dalla pandemia Covid-19, dal momento che proprio Internet è diventato lo strumento più idoneo a consentire l'esercizio dei diritti e libertà fondamentali garantiti nella Costituzione. È innegabile che il diritto all'istruzione, quanto quello al lavoro o alla salute o ancora la libertà di riunione o associazione o quanto piuttosto l'esercizio della libertà religiosa, a voler esemplificare, si siano potuti esplicare proprio "in rete" e che la rete, anzi, sia diventata nel periodo di lockdown a cui siamo sta-

ti costretti, l'unico luogo in cui l'esercizio dei diritti innanzi elencati è stato possibile.

Le manifestazioni tipiche di esercizio della libertà religiosa sono, infatti, state escluse nell'ottica della necessità di limitare e di evitare assembramenti a tutela della sicurezza pubblica preordinata alla più ampia tutela del diritto alla salute di ciascuno[26]. In un momento storico caratterizzato "dall'emergenza" si sono inseriti i numerosi provvedimenti governativi[27] succedutisi uno dopo l'altro, statuendo limitazioni e restrizioni al fine di circoscrivere la diffusione del virus[28].

Le restrizioni resesi necessarie al fine di evitare che le celebrazioni liturgiche potessero essere luogo di assembramento hanno fatto sì che si fosse predisposti alla ricerca di soluzioni alternative che, in ossequio a quanto previsto alle misure di contenimento predisposte dal Governo e condivise dalla Chiesa italiana, permettessero l'attuazione della libertà religiosa attraverso forme "consentite" di esercizio del culto.

Nella nuova forma di esercizio a cui si è stati costretti, sia pur restrittiva per il necessario contenimento della pandemia, vi è chi ha rilevato una sorta di «compressione e limitazione di diritti e libertà fondamentali costituzionalmente rilevanti»[29], da cui non è rimasto escluso il diritto di libertà religiosa che ha assunto in questo contesto un nuovo contenuto.

Tanto non significa che il diritto alla libertà religiosa sia da considerare "un nuovo diritto", quanto piuttosto che applicato al mondo di Internet assume nuove sfaccettature che ne rendono interessante una rilettura, con riferimento all'esistenza o meno, anche ad esempio, di una "diversa" – da quella tradizionale – nozione di buon costume che sussuma le tradizioni comuni dei vari ordinamenti collegati in rete.

In questo contesto Internet ha consentito l'esercizio, nel cyberspazio, delle funzioni religiose. Le celebrazioni in streaming sono diventate la regola, nel periodo di lockdown, e coesistono, ad oggi, con le celebrazioni in presenza.

L'utilizzo della rete quale nuovo spazio liturgico ha, di fatto, realizzato una realtà lontana dall'immaginario comune, che ha sollecitato nei confronti di ciascuno come singolo e come membro della comunità ecclesiale non poche perplessità rispetto alla effettività della "celebrazione on line" ma che in ogni caso ha consentito l'esercizio del culto.

Internet è diventato un ulteriore mezzo di comunicazione attraverso cui trasmettere il messaggio cristiano, il mezzo che abbatte più di tutti le barriere di spazio e tempo e così la celebrazione delle funzioni in rete, in streaming, è stato il mezzo per poter seguire da casa le funzioni, tentando e realizzando una sorta di riavvicinamento dei fedeli al sentimento religioso tramite forme "artificiali di partecipazione"[30].

Sono state incrementate in questi due anni le possibilità di interazione mediante tecnologie basate sul Web o su app, trasmettendo, per esempio, la messa in streaming su diverse piattaforme (YouTube, Facebook, Instagram), o offrendo la possibilità di condividere momenti di preghiera in gruppi più ristretti, interagendo in tempo reale con il celebrante.

La pandemia ha permesso di scoprire una Chiesa Cattolica "in rete", sempre più "connessa": le dirette delle messe disponibili on line si sono moltiplicate, per continuare a restare vicini alle singole comunità. Internet è diventato il luogo di comunicazione e di effettivo esercizio del culto al punto che si sono moltiplicati i canali social delle parrocchie. È stata così garantita ai fedeli, pur se sottoposti alla "quarantena" in casa, una qualche forma di fruizione delle cerimonie religiose attraverso i social media, portando il digitale nelle chiese, rendendo possibile l'esercizio della libertà di religione sancita dall'art. 19 Cost.

Anche se da alcuni anni è in atto un processo di avvicinamento e cura dei fedeli attraverso le tecnologie digitali, che ha portato già molti anni fa a coniare l'espressione di *religion surfers* per indicare i fedeli che utilizzano Internet e le tecnologie digitali come supporto alla propria fede[31], per certi versi, si potrebbe affermare che la pandemia è stata l'occasione per rendere concreto quanto previsto nel documento 22 febbraio 2002, *Chiesa e Internet*[32], del Pontificio Consiglio per le Comunicazioni sociali, diffuso in parallelo a *Etica in Internet*, che evidenziava «l'interesse della Chiesa per Internet» e affrontava le implicazioni che Internet avrebbe potuto avere per la religione.

Lo sviluppo della rete ha coinvolto anche il fenomeno religioso. Anzi, la diffusione di Internet tra i mezzi di comunicazione ha ridefinito, fra le altre, la geografia religiosa nel senso che Internet rappresenta un territorio alternativo all'*off line*. Le dimensioni *off line* e *on line* si "fondono" e "confondono", si potrebbe dire, attraverso la cultura digitale a cui il fenomeno religioso ha mostrato particolare interesse, dal momento che la dimensione digitale crea aggregazione e sviluppa un senso di appartenenza collettiva[33]. In tal modo, l'utente-fedele di una determinata confessione può servirsi di una modalità nuova attraverso cui professare attivamente la propria fede, partecipando e interagendo con la propria comunità di appartenenza e con fedeli di altre confessioni religiose e non restando passivamente ad assistere di fronte a uno schermo pc, ora anche smartphone[34]. Puntualmente, a riguardo, si è introdotta la distinzione fra *religion online* delle istituzioni religiose, che si

adattano a comunicare via Internet, e *online religion* quale creazione di nuovi network capaci di promuovere la formazione di comunità virtuali, nelle quali la definizione dei contenuti e dei significati religiosi o spirituali è affidata all'interazione via computer fra gli individui[35]. In questo secondo modello, non c'è la mera sequenza emittente-ricevente della *religion online*, ma si è di fronte ad un rilevante cambiamento socio-culturale, in quanto, un sito, che rientra in questa tipologia, offre uno spazio creativo e interattivo per una vasta (più o meno anonima) platea di utenti, i quali, in tal modo, danno l'idea di farsi una religione a loro misura[36].

Ebbene, il sentire religioso non può più essere solo considerato quale prodotto dell'intimità e della coscienza, ma diventa il frutto di un continuo confronto dialettico tra l'individuo e la sua dimensione pubblica o social, tant'è che, anche se non si volesse ammettere l'influenza totalizzante di Internet sui principi che reggono la libertà religiosa, difficilmente potrebbe negarsi la sua autorevole influenza sulla formazione della coscienza religiosa[37].

In questo contesto, più di un interrogativo si appalesa. Si è detto che la rete ha consentito l'esercizio di diritti fondamentali, nel caso specifico della libertà religiosa, ma tale forma di esercizio può essere considerata l'equivalente della celebrazione in presenza, più che nel senso della fisicità e della contestualizzazione spaziale, nel senso sostanziale della partecipazione attiva del fedele? Ed ancora. Nel momento in cui il fedele è davanti a uno schermo, è tutelato e protetto da qualsivoglia forma di ingerenza estranea?

Non bisogna dimenticare che nel momento in cui il cittadino/fedele è connesso a Internet viene in rilievo *in primis*, inevitabilmente il suo diritto alla riservatezza o alla privacy che dir si voglia, e nel caso specifico tale diritto assume un significato e un peso particolare in quanto si tratta di un diritto, quello di cui all'articolo 19 della Costituzione, che riguarda il cd. foro interno e la libertà di coscienza di ciascuno.

Orbene, anche la libertà *religiosa informatica* ritrova una sua dimensione positiva e negativa. In chiave positiva, esprime il diritto a che non siano pubblicate, da parte di qualunque soggetto, via Web le proprie professioni di fede, le inclinazioni, le pratiche di culto religioso esercitate, affinché esse non divengano fonte di discriminazione e di etichettamento. In chiave negativa, invece, manifesta il diritto a poter esercitare un controllo sui dati concernenti la propria persona contenuti su Internet e, dunque, il diritto di poter controllare in prima persona le informazioni di matrice religiosa contenute sul Web e potere, conseguentemente, azionare degli strumenti certi e rapidi di tutela. L'accertamento, se da un lato ricomprende le notizie immesse dallo stesso soggetto e, dunque, implica il diritto di aggiornamento sulle proprie notizie – magari, ormai superate e non più rispondenti alla realtà storica –, dall'altro lato, a maggior ragione, ricomprende la verifica sulle notizie afferenti la propria vita religiosa inserite da "altri soggetti"[38].

E quando si parla di altri soggetti, sono innanzitutto da ricomprendere coloro che detengono il potere informatico e che più facilmente rispetto ad altri possono alterare il sistema di verità informatica a danno di un individuo. In questo senso, allora, per libertà religiosa informatica non intendiamo solo il diritto di difesa che può azionare il soggetto che si ritiene leso ma, più ampiamente, intendiamo un vero e proprio diritto attivo di partecipazione del soggetto al circuito delle informazioni di matrice religiosa che lo riguardano[39].

Ma allora, il fedele è legittimamente protetto nella gestione dei video e delle immagini, da possibili interferenze, manipolazioni e/o sottrazioni di dati personali?

L'interrogativo è più che mai legittimo in quanto l'esercizio ormai informatizzato della libertà religiosa è tutt'ora utilizzato relativizzando lo spazio liturgico e la stessa essenziale assemblea di fedeli che diventa una assemblea "fluida", aperta, perché composta da fedeli in presenza e da fedeli, "on line", ma nello stesso tempo non virtuale, quanto piuttosto digitale, presente e partecipativa, dal momento che anche i fedeli "on line" non assistono, ma partecipano attivamente alla celebrazione attraverso un coinvolgimento naturale degli utenti tramite l'utilizzo di app, con un'interazione tale che si potrebbe pensare alla creazione di una vera e propria identità religiosa[40].

Internet, quale nuovo luogo di esercizio della libertà religiosa, impone di verificare se e come l'accesso alla rete e l'essere in rete realizzino pienamente la libertà religiosa innanzi delineata. Uno dei parametri più rilevanti, a riguardo, è costituito dall'effettività del diritto alla privacy che investe anche lo specifico campo religioso. Difatti, il diritto alla privacy in ambito religioso è stato normativizzato con la cd. "tutela del dato religioso". Quando parliamo di tutela dei dati religiosi ci riferiamo al diritto che hanno i soggetti a non veder divulgato a soggetti terzi i propri dati in materia religiosa. Viene infatti definito un diritto *erga omnes*, cioè assoluto[41].

Secondo quanto previsto dal d.lgs. 30 giugno 2003, n. 196, testo unico per il trattamento dei dati personali, tra i diritti da tutelare in materia di privacy, rientra anche la libertà religiosa e, in modo particolare, questa libertà rientra fra i dati sensibili. E infatti, la citata normativa prevede che «in materia religiosa i dati sensibili siano quelli che rivelano l'origine raz-

ziale ed etnica, le convinzioni religiose e filosofiche, le opinioni politiche, l'adesione a partiti, sindacati ed organizzazioni di carattere religioso e atti idonei a rivelare stati di salute e l'orientamento sessuale».

Le confessioni religiose sono del tutto esenti dal regime di protezione rinforzata dei dati sensibili relativamente al trattamento dei dati degli aderenti e dei soggetti che entrano in contatto con esse solo per finalità religiose; pertanto, le confessioni religiose possono effettuare il trattamento dati dei loro aderenti senza nessun consenso scritto degli interessati.

E allora viene da chiedersi se nel momento in cui il singolo si "connette in rete" ed entra nella "chiesa digitale" sia tutelato al pari di quando assiste a una celebrazione religiosa in presenza. In quest'ultimo caso, infatti, ciascuno recandosi in chiesa è come se implicitamente acconsentisse reciprocamente rispetto ai partecipanti a far conoscere il proprio orientamento religioso, ma in una chiesa diventata sempre più digitale, in cui sembra quasi che non vi sia contrapposizione fra ambiente reale e cyberspazio, in cui ormai la liturgia e i sacramenti hanno trovato una loro giustificata collocazione, è fondamentale allora verificare se Internet sia in grado di apprestare le dovute e necessarie garanzie al singolo rispetto a una platea di utenti indefinita.

4. L'assegnazione dei nomi a dominio di primo livello: il TLD *.catholic*

Appare evidente che la diffusione della rete comporti problematiche assai complesse: la tutela delle libertà fondamentali di cui la libertà religiosa rappresenta una delle manifestazioni, ma anche la protezione della privacy, quanto piuttosto il controllo sul contenuto delle informazioni. Centrale diventa, allora, in primo luogo, il sistema dei nomi a dominio in quanto la sua gestione può effettivamente considerarsi un modo per controllare il funzionamento di Internet[42]. La Internet Corporation for Assigned Names and Numbers (ICANN)[43], istituita per il coordinamento delle attività di gestione del Domain Name System (DNS), al fine di garantire l'univocità del sistema dei nomi a dominio, la stabilità, la sicurezza e la resilienza di Internet, nasce da un tentativo autocontraddittorio di "privatizzare" il sistema dei nomi di dominio (DNS). Tuttavia, la presenza degli Stati, sempre più interessati alla regolazione della rete, mette in luce come la forma di governo settoriale abbia acquisito una natura mista, pubblico-privata. Non si è di fronte ad un'organizzazione internazionale creata da Stati nazionali, né ad un'organizzazione di seconda generazione, ma ad un soggetto di natura privata che svolge, però, la sua attività su scala mondiale e coinvolge un numero amplissimo di utenti: l'ente è privato, ma ad esso è affidata una funzione pubblica; è nazionale, ma le sue funzioni hanno una rilevanza globale[44]. Non si può certo pensare che lo Stato o altri attori di carattere pubblico rimangano assenti rispetto al dibattito sull'impiego delle tecnologie, abdicando in favore delle forze di mercato, degli istituti di gestione degli standard tecnici e delle lobbies multinazionali, nella misura in cui dette scelte tecniche sono in grado di incidere fortemente sui diritti, sulle libertà e sulla protezione dei soggetti utilizzatori[45].

La sfida affrontata dall'ICANN riguarda allora non solo il grado di potere che i governi possono esercitare nei suoi processi (dell'ICANN), ma ancora più importanti sono le procedure e meccanismi istituzionali all'interno dei quali quel potere deve essere esercitato[46].

In riferimento alle assegnazioni dei nomi di dominio di primo livello, non poche sono state le problematiche derivanti dall'assegnazione di domini a carattere religioso, in particolare del TLD *.catholic*. Il Pontificio Consiglio delle Comunicazioni Sociali (PCCS)[47] ne aveva chiesto all'ICANN l'assegnazione affinché fosse l'unico soggetto legittimato a registrare a sua volta all'interno del TLD .catholic un affiliato alla Chiesa cattolica. L'estensione era riservata alle istituzioni della Chiesa cattolica, quali diocesi, parrocchie, ordini religiosi, scuole, università o ospedali così come risultanti, anche se non esclusivamente, dall'elenco dell'Annuario Pontificio[48]. Ebbene, fra le obiezioni mosse all'ICANN rispetto all'assegnazione di un dominio .catholic, rilevante fu quella della Saudi Communication and Information Tecnology Commission rispetto alle varie applicazioni .catholic. Si obiettava nello specifico che «molti altri cristiani usano il termine "cattolico" per riferirsi più ampiamente a tutta la Chiesa cristiana a prescindere dall'affiliazione confessionale e... anche altre comunità cristiane rivendicano il termine "cattolico" fra le quali la Chiesa ortodossa e la Chiesa ortodossa orientale»[49].

L'obiezione non è stata di poco rilievo in quanto, effettivamente, l'ICANN l'ha dovuta considerare per l'assegnazione del nome di dominio richiesto. Infatti, con riferimento alle assegnazioni dei nomi a dominio a carattere religioso (ad esempio, .catholic, .anglican, .orthodox, .hindu, .islam, .muslim, .buddhist, ecc...), questi gTLD[50] avrebbero potuto provocare rivendicazioni fra le tradizioni teologiche e religiose tali da, eventualmente, sfociare in aspre dispute che avrebbero costretto l'ICANN, implicitamente o esplicitamente, ad abbandonare la sua politica di neutralità pur riconoscendo ad un particolare gruppo o ad una specifica organizzazione la legittimità di rappresentare una determinata tradizione religiosa.

Di qui, anche al fine di rispettare «le sensibilità riguardo ai termini con significato nazionale, culturale, geografico e religioso», la necessità di una particolare e acuta attenzione ai domini concernenti le tematiche religiose e sul processo di assegnazione dei gTLD con significato religioso, prima di procedere con l'assegnazione stessa per evitare che l'ICANN «possa direttamente o indirettamente abbandonare la propria neutralità dovendo valutare se e quali gruppi o organizzazioni siano rappresentativi di una tradizione religiosa»[51].

L'ICANN con riferimento alla richiesta avanzata dalla Chiesa cattolica, a seguito delle obiezioni mosse, ha dovuto prendere atto[52] che la Chiesa Cattolica Romana «non controlla e non rappresenta tutti gli usi e le identificazioni con il termine "catholic"», ponendo la rilevante questione connessa alla libertà religiosa in relazione all'uso del dominio ma, in ogni caso, non ha potuto prescindere dal dato oggettivo che il «richiedente (PCCS) rappresenta la maggioranza dei cattolici ed è in grado di gestire il TLD come richiesto»[53] e che, pertanto, gli poteva essere assegnato. Tanto non ha significato da parte dell'ICANN una sorta di avallo al gruppo religioso, quanto piuttosto un prendere atto che il richiedente, quale soggetto "ex se" considerato aveva i necessari requisiti e possedeva quindi il potenziale di rappresentare a lungo termine precisi target, settori o temi, elementi necessari affinché gli fosse rilasciata la chiesta assegnazione di dominio di primo livello.

Ne è conseguito che il 21 ottobre 2015 è stato assegnato al registro vaticano il dominio di primo livello .catholic, compreso il nome in alfabeto arabo, cinese e cirillico[54]. L'uso del dominio che rappresenta la garanzia che un determinato sito è autenticamente cattolico, è riservato non ai singoli individui, ma alle istituzioni della Chiesa cosicché intende creare una presenza coesa e organizzata on line della Chiesa, in modo da essere l'immagine speculare on line della Chiesa stessa. Sempre con questa finalità è stato istituito un apposito ufficio su impulso della Segreteria di Stato e della Segreteria per la Comunicazione, denominato «DotCatholic» che ha lo scopo di utilizzare il dominio Internet generico di primo livello ".catholic" per condividere gli insegnamenti, il messaggio ed i valori della Chiesa Cattolica secondo assegnazioni ufficiali con la più ampia comunità globale nel ciberspazio[55], in cui la natura di "formazione sociale" delle "comunità di utenti" è necessario trovi un giusto bilanciamento fra l'utilizzo in funzione protettiva dei diritti individuali, nel senso che il riconoscere la natura di formazioni sociali di queste aggregazioni dovrebbe costituire l'impalcatura concettuale per rafforzare la tutela dei "diritti inviolabili" di costoro, appunto, anche "all'interno" delle formazioni sociali e la possibilità di rafforzare e legittimare il potere di controllo e di governo della rete dei grandi intermediari: poteri che subiscono, per così dire, una sorta di trasfigurazione, e vengono rappresentati non già nella loro nuda realtà di espressione di potere economico, ma come frutto, in qualche modo, di un ruolo, di una responsabilità attribuita e riconosciuta dalla stessa "comunità di riferimento", espressione di "autonomia" della "formazione sociale"[56].

5. L'effettività dei diritti (e della libertà religiosa) in Internet: l'efficacia della Internet governance anche attraverso un'efficiente "gestione" dei dati personali

Si può, allora a ragion veduta, affermare che l'effettività dei diritti in Internet, e nello specifico del diritto di libertà religiosa, per come innanzi delineato nel contenuto, è strettamente connessa a una concreta efficacia della Internet governance (IG), quale complesso di iniziative di una pluralità di soggetti, governi, settore privato, società civile, per sviluppare e attuare principi, norme, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet[57]; una "gestione" di Internet finalizzata, così, a garantire integrazione globale, libertà di mercato ed equa concorrenza, difesa dei diritti delle persone, e in generale opportunità culturali, economiche, sociali per tutte le persone: dalla gestione delle risorse della rete, alle questioni della sicurezza, alle diseguaglianze nella diffusione e nell'accesso a tali risorse, fino alla tutela dei diritti umani in quanto rientrano a pieno titolo in una riflessione centrata sulla sfida democratica nel mondo digitale[58].

Per tale finalità le iniziative e le tappe che si sono succedute hanno avuto vario oggetto[59]: di standardizzazione tecnica (IETF)[60], di gestione delle policy sulle risorse (ICANN), a cui innanzi si è più ampiamente fatto riferimento, e di discussione generale sul futuro della rete (IGF)[61].

In particolare, il forum di discussione sul futuro della rete (IGF), istituito nel 2006, rende possibile la condivisione delle decisioni prese nelle varie macroaree di intervento fra cui quella concernente l'educazione on line, la diversità culturale, i diritti umani (on line e off line), la privacy e la protezione dei dati personali[62]. Pertanto, dato l'oggetto pluridisciplinare della Internet governance, si cercherà di verificare come la stessa vada ad impattare sulle questioni più strettamente connesse all'oggetto del presente contributo, ovvero in relazione alla possibilità di esercitare

nel nuovo "spazio dimensionale" di Internet un'ampia categoria di diritti individuali e collettivi, fra cui appunto la libertà religiosa e di culto.

A riguardo è innegabile il ruolo centrale che abbia avuto l'approvazione della richiamata Costituzione dei diritti di Internet nel 2015 a cui direttamente si ispira il Regolamento 2015/2021 UE e che conferma due punti fondamentali: il concetto di Internet aperta viene assorbito nei diritti degli utenti finali; la neutralità della rete viene associata al trattamento equo e non discriminatorio e limitata al diritto delle comunicazioni elettroniche, sottraendone un contenuto trasversale. L'Internet aperta è collegata alla libertà di «collegarsi alla rete Internet pubblica senza che i governi o i fornitori pongano limitazioni per quanto riguarda i contenuti, i siti, le piattaforme, il tipo di attrezzature che possono essere utilizzate». Una rete aperta applica standard liberi e pubblicamente disponibili, che «chiunque può utilizzare per creare siti web, applicazioni e servizi, e perché gestisce tutto il traffico più o meno nello stesso modo», senza «chiedere autorizzazioni ai fornitori o di pagare loro supplementi per raggiungere altri utenti on line»[63].

Ed ancora, la Raccomandazione del 7 marzo 2018 del Consiglio d'Europa ha sancito che l'«access to the internet is a precondition for the exercise of Convention rights and freedoms online», stabilendo una relazione tra le responsabilità degli ISP e l'esercizio di diritti fondamentali tutelati dalla CEDU[64].

Sulla stessa linea si collocano altresì i risultati raggiunti nella IGF Italia 2018 e 2020 in materia di inclusione digitale e diritto di accesso e di privacy, diritti e cittadinanza digitale[65]. Ed infatti, quanto all'inclusione digitale e diritto di accesso, è stata evidenziata la necessità di migliorare la cultura digitale dei cittadini al fine di consentire il pieno esercizio dei diritti di cittadinanza digitale. È emersa la necessità di creare le competenze digitali per le generazioni future sin dai primi anni di età, comprendendo l'istruzione degli insegnanti su queste tematiche, evidenziando come l'educazione al digitale e l'utilizzo responsabile e consapevole di Internet, siano uno strumento fondamentale per garantire la protezione delle libertà individuali grazie a una piena partecipazione alla vita sociale.

In relazione invece alla privacy, ai diritti e alla cittadinanza digitale, è stata sollevata la problematica dell'appartenenza dei dati. A chi dovrebbero appartenere i dati generati dagli utenti? Chi è legittimato ad utilizzarli? Tenendo conto che, nell'era dell'informazione, avere la proprietà del dato equivale ad esercitare una fortissima influenza in ogni contesto, disciplinarla rappresenta una sfida futura. Si è portato all'attenzione anche il tema del diritto all'oblio, invitando ad adottare cautela nell'implementarlo, poiché talvolta si potrebbe permettere la cancellazione di informazioni e memorie riguardanti il passato e la storia, accessibili al giorno d'oggi quasi esclusivamente tramite la rete.

I dati sensibili assumono rilievo, infatti, anche in relazione alle categorie di dati personali di cui all'art. 9 del Regolamento Generale sulla Protezione dei Dati, in quanto dati personali idonei a rivelare le convinzioni religiose o filosofiche, rappresentando una tematica ampia[66] che ha destato sempre molto interesse soprattutto in relazione alle anagrafi religiose, alla tutela dei dati "ex sensibili" e all'autorizzazione generale dell'Autorità Garante per la protezione dei dati personali relativa al trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose[67].

Ma, in ogni caso, ben si è evidenziato che differente è la regolamentazione in Internet dei social network e delle app in quanto rappresenta un *quid novi*, innanzitutto perché non sempre chi raccoglierà i dati è un ente religioso, secondariamente perché, oltre ai dati immessi consapevolmente dall'utente, vi sono molti altri dati "esterni" che vengono comunque raccolti e che contribuiscono a creare un'informazione sempre più completa sull'individuo e sulle sue credenze. Difatti, da parte di alcuni social network, vi è la previsione di presentare tra le domande del profilo quella relativa alla propria appartenenza confessionale, ma spesso gli utenti non si rendono conto di quale possa essere l'ambito di diffusione di questa informazione e quanto possa essere facile da estrarre, utilizzando sistemi di profilazione dei soggetti sulla base di specifici indicatori. E proprio la profilazione desta perplessità al legislatore europeo che la definisce come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[68].

Per questo motivo, il legislatore ha previsto un generale divieto nel trattamento delle categorie particolari di dati personali, a meno che non ricorra in sostanza il consenso esplicito al trattamento dei dati personali per una o più finalità specifiche, che infatti è la modalità mediante la quale tutti i social e le app ottengono la facoltà di trattare i dati dell'interessato.

Mai come nel caso delle applicazioni, però, è possibile che avvengano dei trattamenti non dichiarati o

ultronei rispetto a quelli enunciati nell'informativa, senza che l'utente possa essere in grado di accorgersene. Anche per i social network, l'ambito di diffusione del dato molte volte diventa ben più ampio di quanto l'utente avrebbe desiderato, circostanza verificatasi più volte in relazione ad informative poco chiare o alla scarsa dimestichezza dell'utente con i controlli privacy messi a disposizione della piattaforma. Purtroppo, la velocità della trasmissione dei dati in rete rende difficile il contenimento delle informazioni nel momento in cui escono dalla disponibilità dell'interessato, per cui è bene che le prescrizioni legislative trovino una trasposizione certa nelle modalità progettuali delle tecnologie, le quali dovranno essere strutturate per preservare adeguatamente la riservatezza degli utenti, soprattutto quando pensate per trattare categorie particolari di dati personali come le convinzioni religiose[69].

Il Regolamento Generale sulla Protezione dei Dati contiene, già in sé, delle prescrizioni volte a incorporare la tutela dell'interessato nella tecnologia prima ancora che nella gestione del rapporto tra interessato e titolare, in particolare mediante i concetti di *data protection by design*[70] e di *data protection by default*[71]. Il nucleo fondamentale delle disposizioni è contenuto nel primo e secondo comma dell'articolo 25 del Regolamento, nella parte dedicata agli obblighi generali del titolare del trattamento[72].

Già da questi principi generali è possibile ricavare dei suggerimenti importanti in termini di politiche di sviluppo e implementative, che dovranno essere seguiti dal titolare di un trattamento di dati personali.

Le valutazioni in merito, ad esempio, all'ampiezza dei dati trattati, alla natura dei dati che si andranno a chiedere all'utente, all'obbligatorietà o meno di conferire quei dati per usufruire del servizio e al periodo di conservazione, saranno fondamentali per fissare il livello di protezione desiderabile, date le caratteristiche proprie di quel trattamento. A tanto dovrà seguire l'implementazione dei princìpi essenziali del trattamento dei dati personali, enucleati nell'art. 5 del Regolamento 679/2016, soprattutto in merito alla minimizzazione dei dati e alla limitazione della conservazione. Nel caso di un'app che voglia, ad esempio, consentire l'accesso a determinati testi religiosi o a contenuti multimediali verificati presenti in Rete, non vi sarà alcun bisogno di registrare dati quali quelli provenienti dal ricevitore GPS del dispositivo, oppure richiedere forme di registrazione e di autenticazione all'utente, oppure, infine, accedere ad altri componenti del dispositivo quali la fotocamera o il microfono. Di eguale importanza è il principio della limitazione della conservazione, volto a prevenire che i dati permangano quando si sia esaurito lo scopo del trattamento o, comunque, non vi sia più titolo per detenerli legittimamente. La stratificazione di dati non più oggetto di trattamento, infatti, fa naturalmente ridurre l'attenzione nei confronti di questi dati. Quando dovessero pervenire richieste di cancellazione dell'account, quindi, soprattutto nel caso del trattamento di categorie particolari di dati personali, il sistema deve essere configurato in maniera tale da provvedere immediatamente alla cancellazione sicura dei suddetti dati, rinviando a una successiva registrazione l'eventuale ripensamento dell'utente.

Infine, il legislatore richiama l'attenzione verso una misura più tecnica rispetto a quelle fin qui esaminate: la pseudonimizzazione[73], ovvero un procedimento di trasformazione del dato teso a separare i dati identificativi dagli altri tipi di dati, in particolare i dati "ex-sensibili". In questo modo, anche nel caso in cui un soggetto non autorizzato dovesse aver accesso a parte o a tutto il database di informazioni detenuto da un titolare, non sarebbe in grado di ricostruire l'identità del soggetto e, quindi, la violazione del dato non esisterebbe.

Proprio sul tema della protezione dei dati fin dalla progettazione e per impostazione predefinita, lo *European Data Protection Board* (EDPB) ha pubblicato delle *Guidelines*[74] esplicative dell'art. 25 del Regolamento 679/2016; in esse viene evidenziata l'importanza della trasparenza nelle informazioni che devono essere trasmesse all'interessato *ex* art. 13 del Regolamento, requisito così importante nella progettazione ed offerta di strumenti che potrebbero avere delle ricadute per i diritti e le libertà delle persone fisiche.

E sulla specifica libertà religiosa merita di essere evidenziato, in ultimo, l'approccio multidimensionale e la nozione di sicurezza «integrata» da un'adeguata tutela dei diritti fondamentali e delle libertà religiose, fornito dalle Linee Guida 2019 in materia di «Libertà di religione o convinzione e sicurezza» dell'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE) con orientamenti pratici e raccomandazioni per garantire un approccio basato sui diritti umani, sensibile al genere, alla libertà di religione o di credo e sicurezza per i politici e i professionisti della sicurezza, organizzazioni della società civile, comunità religiose o di credo e media, regolamentazioni che dovranno necessariamente integrarsi nella loro coesistenza al fine di rendere effettivi i diritti nel loro esercizio in rete.

6. Osservazioni conclusive

Le tematiche affrontate hanno evidenziato che le problematiche collegate all'utilizzo di Internet sono molteplici e interconnesse. Del resto, Internet rappresen-

ta "il più largo spazio pubblico che l'umanità abbia conosciuto", nel quale i diritti di ciascuno possono trovare ingresso e cittadinanza in nuovi contenuti: comunità virtuali, esercizio on line dei diritti fondamentali e del culto in particolare sono solo alcune manifestazioni concrete derivanti dal nuovo contesto identificato dalla rete.

Di qui la necessità di una regolamentazione della rete ampia che travalichi i confini territoriali degli Stati e allo stesso tempo la sola giustiziabilità dei diritti. Infatti, l'effettiva tutela dei diritti non è più necessariamente affidata ai tradizionali procedimenti giudiziari, ma può essere resa possibile da iniziative che, partendo dalla società civile e avendo come riferimento documenti internazionali, riescono a rendere concrete le garanzie.

Garantire l'accesso a Internet significa garantire e tutelare effettivamente i diritti fondamentali, non solo un generico riconoscimento della libertà in rete, ma la concreta possibilità di esercitare «virtù civiche», dunque di dar corpo ad una cittadinanza attiva: con tale finalità Internet è una risorsa per la democrazia[75].

Salvaguardare la neutralità della rete anche nella sua accezione di rete «aperta»[76], considerare l'accesso a Internet quale diritto fondamentale della persona e diritto attraverso il quale si esercitano gli altri diritti già positivizzati dagli ordinamenti sovranazionali e nazionali significa apprestare una tutela che da una parte trascenda le regolamentazioni statuali e dall'altra non ne imponga una sovrastatuale[77] dal momento che vi è «l'esigenza di condividere e applicare una sorta di carta di principi universale» non «una costituzione globale che regoli la governance di Internet, ma almeno una condivisione di un insieme minimo di principi sui quali garantire il rispetto di tutti»[78].

L'efficacia di una Internet governance non può che considerare, quindi, la dimensione variegata di diritti[79] coinvolti per forme di tutela integrata *multilevel*, dal momento che i problemi giuridici posti dalla tecnologia informatica, nella sfera tanto del diritto costituzionale quanto in quella del diritto privato, non riescono a trovare più solo nella dimensione statale la sede idonea alla soluzione di essi.

Note

[1]F. Modugno, *I "nuovi diritti" nella Giurisprudenza Costituzionale*, Giappichelli, 1995.

[2]In tale accezione di certo emblematico è il riferimento al diritto di accesso a Internet, il diritto alla neutralità della rete e il diritto all'oblio.

[3]«Le nuove tecnologie hanno in primo luogo creato nuove forme e nuove opportunità per diritti fondamentali già riconosciuti dalle Costituzioni contemporanee; consentono anche nuove minacce e ai diritti fondamentali già riconosciuti; hanno fatto emergere nuovi diritti fondamentali, che in alcuni casi servono a proteggere la persona dalle minacce derivanti dalle nuove tecnologie, mentre in altri sono finalizzate a rendere effettivamente fruibili le nuove opportunità che le nuove tecnologie hanno generato rispetto ai diritti fondamentali già esistenti», così, M. Olivetti, *Diritti fondamentali e nuove tecnologie: una mappa del dibattito italiano*, in "Revista Estudos Institucionais", vol. 6, 2020, n. 2, pp. 395-430.

[4]È il cd. *Right to Internet access* o *right to broadband* (letteralmente diritto alla banda larga).

[5]Sul punto, G. Della Cananea, *Al di là dei confini statuali. Principi generali del diritto pubblico globale*, il Mulino, 2009, p. 95 ss.

[6]A riguardo, M. Pietrangelo, *Accesso a Internet: un diritto ancora diseguale? Aggiornamenti e ripensamenti*, in M.R. Allegri, G. d'Ippolito (a cura di), "Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee", Aracne, 2017; Id., *Introduzione. Il diritto di accesso ad Internet a mezzo secolo dalla nascita di Internet. Stato dell'arte e prospettive*, in M. Pietrangelo (a cura di), "Il diritto di accesso ad Internet", ESI, 2010, p. 11 ss.; A. Busacca, *Il "Diritto di accesso" alla rete Internet*, in "Ordine internazionale e diritti umani", 2017, pp. 345-359; A. Pirozzi, *Il libero accesso alla rete: un diritto in espansione*, in "Diritto dell'informazione e dell'informatica", 2018, n. 2, p. 213 ss.; M. Nisticò, P. Passaglia (a cura di), *Internet e Costituzione*, Giappichelli, 2014; G. De Minico, *Internet. Regola e anarchia*, Jovene, 2012; P. Costanzo, *Miti e realtà dell'accesso a Internet (una prospettiva costituzionalistica)*, in "Consulta online", 2012; F. Badocco, *Riflessioni sul diritto di accesso a Internet nell'ambito del diritto dell'Unione europea*, in "Informatica e diritto", 2009, n. 1, pp. 153-163; F. Borgia, *Riflessioni sull'accesso a internet come diritto umano*, in "La Comunità internazionale", 2010, n. 3, pp. 395-414. B. Carotti, *L'accesso alla rete e la tutela dei diritti fondamentali (Nota a Conseil Constitutionnel, Décision 10 giugno 2009, n. 580)*, in "Giornale di diritto amministrativo", vol. 16, 2010, n. 6, pp. 643-649; S. Rodotà, *Una costituzione per internet?*, in "Politica del diritto", 2010, n. 3, pp. 337-351; E. De Marco (a cura di), *Accesso alla rete e uguaglianza digitale*, Giuffrè, 2008.

[7]Con la Risoluzione A/HCR/20/L.13, del 29 giugno 2012.

[8]Impostazione che si ritrova in dichiarazioni del Parlamento europeo e del Consiglio d'Europa, in iniziative di Stati come la Finlandia, nel piano del Presidente Obama sul servizio universale.

[9]A riguardo, S. Rodotà, *Il diritto di avere diritti*, Laterza, 2013, p. 131, che ritiene Internet quale spazio comune dove dev'essere respinta ogni forma di diseguaglianza digitale, controllo esterno, censura.

[10]Si fa riferimento in particolare alle direttive sulle comunicazioni elettroniche: la Direttiva accesso (2002/19/CE) e la Direttiva servizio universale (2002/22/CE), oggetto di un'ampia revisione successiva, dapprima nel 2009 con le direttive 2009/136/CE e 2009/140/CE, in seguito con l'approvazione del Regolamento (UE) 2015/2120 sulle misure riguardanti l'accesso a un'Internet aperta. Nell'ordinamento italiano, l'accesso a Internet in condizioni non discriminatorie e dietro corrispettivo monetario è riconosciuto dall'art. 54 del Decreto legislativo n. 259/2003, il c.d. Codice delle comunicazioni elettroniche, che recepisce la direttiva 2002/19/CE del Parlamento e del Consiglio del 7 marzo 2002.

[11]Considerando n. 6 del Regolamento UE 2015/2120.

[12]La Carta dei diritti di Internet è approvata il 3 novembre del 2015 dalla Camera dei deputati all'unanimità, a segui-

to della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015.

[13]È il cd. "Diritto alla conoscenza e all'educazione in rete", riconosciuto all'art. 3 della Carta dei diritti di Internet.

[14]L. Maci, *Carta dei diritti in Internet, cos'è e cosa cambia*, in "Economyup.it", novembre 2015.

[15]Così, S. Rodotà, *La Carta dei Diritti in Internet*, in "Privacyitalia.eu", 24 giugno 2017.

[16]«Tutti hanno il diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione».

[17]S. Greco, *Libertà di espressione su internet: fra anarchia e censura*, in "DirittoConsenso", 11 novembre 2020.

[18]R. Pisa, *L'accesso ad internet, un nuovo diritto umano fondamentale?*, in "Treccani giuridica", 7 gennaio 2010.

[19]F. Cerquozzi, *"Diritto di accesso ad Internet" e Costituzione*, in "Iusinitinere.it", 31 ottobre 2020.

[20]Il Codice dell'Amministrazione Digitale (CAD) riunisce e organizza le norme riguardanti l'informatizzazione della pubblica amministrazione nei rapporti con i cittadini e le imprese. Istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016, n. 179 e poi con il decreto legislativo 13 dicembre 2017, n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale.

[21]Ogni anno le relazioni comprendono profili nazionali, che aiutano gli Stati membri a individuare settori di intervento prioritari, e capitoli tematici che forniscono un'analisi a livello dell'UE nei principali ambiti della politica digitale.

[22]Come risulta dal *Digital Economy and Society Index – DESI 2021*, in Italia la percentuale di utenti on line italiani che utilizzano servizi di amministrazione on line (e-government) è aumentata dal 30% nel 2019 al 36% nel 2020, ma è ancora nettamente al di sotto della media UE. Anche l'uso dei fascicoli sanitari elettronici da parte dei cittadini e degli operatori sanitari rimane disomogeneo su base regionale.

[23]Misura prevista dal piano per la ripresa e la resilienza dell'Italia (PNRR).

[24]Cfr. Ministero per l'Innovazione tecnologica e la digitalizzazione, *Strategia Nazionale per le Competenze Digitali*, luglio 2020.

[25]S. Troia, *Nuovi cittadini dell'era dell'accesso*, in "Pearson", 2020.

[26]V. Pacillo, *"A chiare lettere-Confronti". La libertà di culto al tempo del coronavirus: una risposta alle critiche*, in "Stato, Chiese e pluralismo confessionale", 2020, n. 8, pp. 85-94; A. Ruggeri, *Il coronavirus, la sofferta tenuta dell'assetto istituzionale e la crisi palese, ormai endemica, del sistema delle fonti*, in "Consulta online", 2020, n. 1, pp. 210-223.

[27]Il d.l. 23 febbraio 2020, n. 6, convertito, con modificazioni, dalla l. 5 marzo 2020, n. 13; il d.P.C.M. 23 febbraio 2020 nonché il successivo decreto del 1° marzo 2020. Ed ancora, il d.P.C.M. 8 marzo 2020, il d.P.C.M. 9 marzo 2020, il d.l. 25 marzo 2020, n. 19, il d.P.C.M. 1° aprile 2020 e il d.P.C.M. 10 aprile 2020, il d.P.C.M. 7 agosto 2020, il d.P.C.M. 3 novembre 2020.

[28]M. Luciani, *Il sistema delle fonti del diritto alla prova dell'emergenza*, in "Rivista AIC", 2020, n. 2, pp. 109-141.

[29]P. Consorti, *La libertà religiosa travolta dall'emergenza*, in "Forum di Quaderni Costituzionali", 2020, n. 2.; S. Prisco, in S. Prisco, F. Abbondante, "I diritti al tempo del coronavirus. Un dialogo", in "Federalismi.it", 24 marzo 2020 (che parla addirittura di Costituzione sospesa); V. Pacillo, *La sospensione del diritto di libertà religiosa nel tempo della pandemia*, in OLIR, 16 marzo 2020; M. Carrer, *Salus Rei Publicae e salus animarum, ovvero sovranità della Chiesa e laicità dello Stato: gli artt. 7 e 19 Cost. ai tempi del coronavirus*, in "BioLaw Journal", 2020, n. 2.

[30]N. Colaianni, *La libertà di culto al tempo del coronavirus*, in "Stato, Chiese e pluralismo confessionale", 2020, n. 7, pp. 25-40.

[31]P. Perri, *La tutela dei dati personali nei social networks e nelle app religiose*, in "Jus-Online", 2020, n. 3 che richiama il report del 2001 di E. Larsen, *Cyber Faith: How Americans Pursue Religion Online*, pubblicato dal Pew Research Center. Interessante è anche il successivo report del 2014 *Religion and Electronic Media*, sempre a cura del Pew Research Center.

[32]L'analisi della dimensione etica delle questioni digitali era rimessa ad un altro documento del Pontificio Consiglio delle Comunicazioni Sociali, pubblicato nello stesso giorno e intitolato appunto "Etica in Internet". Da sottolineare il capitolo delle raccomandazioni: «ai responsabili ecclesiali» perché si curi un'adeguata «formazione mass-mediale», provvedendo anche a individuare le forme per una «certificazione volontaria a livello locale e nazionale con la supervisione di rappresentanti del magistero» dei siti «cattolici» (n. 11); «agli operatori pastorali» per uno studio di Internet al fine di utilizzarlo quale strumento del proprio ministero; «agli educatori e ai catechisti... ai genitori... ai bambini e ai giovani», perché valorizzino le potenzialità pedagogiche di Internet e insieme vigilino sulle possibili fughe diseducative; «a tutte le persone di buona volontà», infine, perché si rendano consapevoli delle minacciose conseguenze del digital divide e coltivino la virtù della solidarietà globale e concreta».

[33]D. Lochhead, *Shifting Realities. Information Technology and the Church*, WCC, 1997.

[34]Vi è stato chi ha parlato della cd. "chiesa elettronica", a riguardo cfr. ampiamente P. Luca Trombetta (a cura di), *Cristiani senza frontiere: le chiese pentecostali nel mondo*, in "Religioni e Società", 2012, n. 73.

[35]C. Helland, *Online-religion/religion online and Virtual Communities*, in J.K. Hadden, D.E. Cowan (eds.) "Religion on the Internet: Research prospects and promises", 2000, p. 205-223.

[36]E. Pace, *Le religioni in rete: come comunicano e come studiarle*, in "Sociologia italiana", 2013, n. 1, p.16.

[37]L. Pedullà, *Accesso a internet, libertà religiosa e buon costume*, in "Stato, Chiese e pluralismo confessionale", 2012, n. 35, p. 6.

[38]In tema di declinazione costituzionale della libertà informatica, si veda T.E. Frosini, *Il diritto costituzionale di accesso ad internet*, in "Rivista AIC", 2011, n. 1.

[39]L. Pedullà, *op. cit.*, p. 7.

[40]W. Bellar, *Private practice: Using digital diaries and interviews to understand evangelical Christians' choice and use of religious mobile application*, in "New Media & Society", vol. 19, 2017, n. 1, p. 111-125.

[41]C. Valentino, *La libertà religiosa ai tempi del covid 19*, in "diritto.it", 5 maggio 2020.

[42]B. Carotti, *L'ICANN e la Governance di Internet*, in "Rivista trimestrale di diritto pubblico", 2007, n. 3, pp. 681-721.

[43]La *Internet Corporation for Assigned Names and Numbers* è un'organizzazione internazionale no profit che svolge il coordinamento delle attività di gestione del DNS (*Domain Name System*) garantendo l'univocità del sistema dei nomi a dominio, la stabilità, la sicurezza e la resilienza di Internet. Opera attraverso un modello multistakeholder che vede coinvolti i governi, la società civile, le aziende e la società tecnico-accademica secondo principi di apertura, trasparenza e inclusività. Utilizza un modello decentrato, distribuito, "bottom up", con processi aperti, inclusivi e trasparenti che si ispira al modello Internet. A seguito della transizione delle funzioni IANA (*Internet Assigned Numbers Authority*), avvenuta il 1° ottobre del 2016, ICANN svolge le funzioni di coordinamento

del DNS per conto della comunità internazionale e non più per conto del solo governo americano.

[44]K.-H. Lauder, *Globalization and Global Governance: A Contradiction?*, in Id (ed.), "Public Governance in the Age of Globalization", Routledge, 2004, p. 71 ss.

[45]In tal senso le riflessioni di J. Berleur, Y. Poullet, *Quelles régulation pour l'Internet?*, in J. Berleur, C. Lazaro, R. Queck (eds.), "Gouvernance de la société de l'information. Loi, autoréglementation, éthique", Bruylant, Cahiers du CRID n. 22, 2002, p. 133 ss.

[46]J. Weinberg, *Governments, Privatization, and "Privatization": ICANN and the GAC*, in "Michigan Telecommunications & Technology Law Review" , vol. 18, 2011, n. 1, p. 189 ss.

[47]Dicastero della Curia romana, soppresso nel marzo 2016. Le sue funzioni sono state attribuite al Dicastero per la comunicazione, istituito da papa Francesco il 27 giugno 2015.

[48]L'Annuario Pontificio, organo informativo pubblicato ogni anno dalla Segreteria di Stato Vaticano, contiene informazioni e gli indirizzi completi della Santa Sede, di tutte le sedi apostoliche e le istituzioni cattoliche nel mondo: gli uffici della Curia Romana, i corpi diplomatici presso la Santa Sede, gli ordini religiosi in tutto il mondo, le Accademie Pontificie e le Università, oltre che un sommario statistico.

[49]C. Williams, *Saudis attempt to block Vatican plan for .catholic web addresses*, 14 August 2012.

[50]*Generic top-level domain* (dominio di primo livello generico) è un'estensione del nome di dominio Internet con tre o più caratteri e rappresenta una delle categorie del dominio di primo livello (TLD).

[51]In tale prospettiva si pone la lettera del 20 febbraio 2009, del rappresentante della Santa Sede, Mons. Carlo Maria Polvani, indirizzata al Presidente dell'ICANN, Paul Twomey.

[52]Dall'*Independent Objector* (OI), che, quale responsabile di determinare se un'applicazione di nuovo gTLD sia presa nel migliore interesse della comunità di Internet, è abilitato a presentare obiezioni formali contro l'applicazione di un nuovo gTLD.

[53]In questi termini cfr. *Catholic General Comment, Independent Objector New gTLDs.org*.

[54]Si veda il testo dell'accordo.

[55]Così come annunciato il 4 aprile 2016 da Radiovaticana.

[56]M. Cuniberti, *Potere e libertà nella rete*, in "MediaLaws", 2018, n. 3, p. 43.

[57]Così come definita dal *Report of the Working Group on Internet Governance* del giugno 2005. Per un'ampia panoramica della regolamentazione della I.G., cfr., C. Rossello, *La governance di Internet tra diritto statuale, autodisciplina, soft law e lex mercatoria*, in "Diritto del commercio internazionale", 2006, n. 1, pp. 45-95; P. Costanzo, *I profili costituzionali di Internet*, in G. Tosi (a cura di), "I problemi giuridici di Internet", Giuffrè, 2003, p. 53 ss.

[58]E. Pavan, C. Padovani, *Reti di informazione, governance di Internet e innovazione nella politica mondiale*, in "Quaderni di Sociologia", 2009, n. 49, pp. 61-88

[59]Un'analisi dei soggetti coinvolti e delle finalità della I.G. è evidenziata in modo puntuale in J. Mathiason, M. Mueller, H. Klein et al., *Internet Governance: The State of Play*, 9 settembre 2004.

[60]*Internet Engineering Task Force* ha come obiettivo di far funzionare meglio Internet producendo documenti tecnici pertinenti e di alta qualità che influenzano il modo in cui le persone progettano, utilizzano e gestiscono Internet.

[61]L'*Internet Governance Forum* è un processo globale, condotto sotto l'egida delle Nazioni Unite, che favorisce il confronto e il dibattito tra tutte le parti interessate (stakeholders) permettendo di discutere, scambiare informazioni e condividere iniziative inerenti alla Governance di Internet. L'IGF si basa sui principi di trasparenza, apertura, inclusività e l'identificazione dei temi in agenda attraverso un "approccio dal basso". *Internet Governance Forum* facilita il confronto tra tutte le parti interessate all'ecosistema Internet seguendo un principio di partecipazione egualitaria. *Internet Governance Forum* è stato istituito dal Segretario dell'ONU nel 2006 come risultato del Summit Mondiale sulla Società dell'Informazione (WSIS 2003–2005) con il mandato di discutere le questioni di interesse pubblico relative alla governance della Rete. Esso è diventato negli anni il punto di riferimento per la discussione globale sui temi della governance di Internet e sul modello di discussione e confronto multistakeholder.

[62]Infrastrutture: infrastrutture di telecomunicazione, Internet service providers, Protocolli di controllo di trasmissione e protocolli internet, DNS (Domain Name Systems), Root zone e Root Servers, neutralità della Rete, standard tecnici e del web, servizi di Cloud, ecc.; sicurezza: cybersecurity, cybercrime, infrastrutture critiche, cyber terrorismo, cyberconflitti e guerra informatica, crittografia, spam, firma digitale, sicurezza dei minori on line, ecc.; legalità: strumenti legali, giurisdizioni, risoluzioni alternative di dispute, diritto di proprietà intellettuale, copyright, marchi registrati, patenti e brevetti, leggi del lavoro, intermediari ecc.; commercio: E-commerce, Internet Data Economy, Internet Access Economy, trend emergenti: Internet of things, Intelligenza Artificiale, sharing economy, E-banking, Emoney e valute virtuali, protezione dei consumatori, tasse ecc.; sviluppo: tecnologie digitali e sviluppo delle società, digital divide, sviluppo di competenze e capacità; socioculturale: policy dei contenuti, educazione on line, diversità culturale, multilinguismo, beni pubblici ecc.; diritti umani: diritti umani on line e off line, privacy e protezione dei dati personali, diritti dei minori on line, diritti delle persone con disabilità, diritti di genere on line.

[63]S. Poma, *L'interpretazione del regolamento 2015/2120 tra principio di neutralità della rete, principio di non discriminazione e «Internet aperta»*, in "MediaLaws", 26 ottobre 2021.

[64]Council of Europe, Committee of Ministers, *Recommendation to member States on the roles and responsibilities of internet intermediaries*, CM/Rec(2018)2, 1: «The internet plays a particularly important role with respect to the right to freedom of expression. It also enables the exercise of other rights protected by the Convention and its protocols, such as the right to freedom of assembly and association and the right to education, and it enables access to knowledge and culture, as well as participation in public and political debate and in democratic governance».

[65]*Report IGF Italia 2018*.

[66]Cfr. V. Marano, *Protezione dei dati personali, libertà religiosa e autonomia delle Chiese*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019, p. 579 ss.; M. Ganarin, *Salvaguardia dei dati sensibili di natura religiosa e autonomia confessionale. Spunti per un'interpretazione* secundum Constitutionem *del regolamento europeo n. 2016/679*, in "Stato, Chiese e pluralismo confessionale", 2018, n. 11, p. 1 ss.; G. Mazzoni, *Le autorizzazioni generali al trattamento dei dati sensibili da parte delle confessioni religiose. Osservazioni alla luce delle recenti riforme in materia di privacy*, in "Stato, Chiese e pluralismo confessionale", 2020, n. 7, pp. 66-90; D. Milani, *Le autorizzazioni generali al trattamento dei dati sensibili*, in "Quaderni di diritto e politica ecclesiastica", 2000, n. 2, pp. 399-400.

[67]Autorizzazione n. 3/2016 del 15 dicembre 2016.

[68]P. Perri, *op. cit.*

[69]*Ibidem*.

[70]L'art. 25 primo comma, in merito alla *data protection by design* statuisce che «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di ap-

plicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonomizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».

[71]L'art. 25, secondo comma, prescrive l'adozione di misure volte a garantire la *data protection by default*: «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

[72]Sul tema si veda G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, 2017; M. Cassaro, E. Faccioli, *Il "GDPR" [General Data Protection Regulation - Regolamento generale per la protezione dei dati personali] e la normativa di armonizzazione nazionale alla luce dei principi: "accountability" e "privacy by design"*, in "Il Diritto industriale", 2018, n. 6, pp. 561-566; E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in "Contratto e impresa", 2018, n. 1, pp. 106-125; S. Calzolaio, *"Privacy by design". Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in "Federalismi.it", 2017, n. 24, 21 p.; G. Finocchiaro, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e D. Lgs. 10 agosto 2018, n. 101*, Zanichelli, 2019.

[73]*Ex* art. 4 n. 5) del Regolamento 679/2016.

[74]Da ultimo nella versione del 18 gennaio 2022, le *Guidelines* si sono incentrate soprattutto sull'art. 15.

[75]S. Rodotà, *Una Costituzione per Internet?* in "Politica del diritto", 2010, n. 3, pp. 348-351.

[76]Il Regolamento 2015/2021, al considerando n. 6, conferma a riguardo, che il concetto di Internet aperta viene assorbito nei diritti degli utenti finali; che la neutralità della rete viene associata al trattamento equo e non discriminatorio e limitata al diritto delle comunicazioni elettroniche, sottraendone un contenuto trasversale. Il principio è stato ribadito anche nella pronuncia della Corte di Giustizia, del 15 settembre 2020, resa nelle cause riunite C-807/18 e C-39/19, *Telenor Magyarország Zrt. / Nemzeti Média- és Hírközlési Hatóság Elnöke.*

[77]T.E. Frosini, *Il diritto costituzionale di accesso ad Internet*, in M. Pietrangelo (a cura di), "Il diritto di accesso ad Internet", Collana ITTIG-CNR, Serie "Studi e documenti", ESI, 2011, n. 9, pp. 23-43.

[78]C. Cassa, F. Pirro, *L'Italia sta trascurando l'internet governance, ecco i temi importanti (per tutti noi)*, in "Agenda Digitale", 11 giugno 2018.

[79]C. Caruso, *L'individuo nella rete: i diritti della persona al tempo di internet*, in "Forumcostituzionale.it", 28 aprile 2013.

* * *

"Networked" rights and religious freedom. The Effectiveness of Rights through the effectiveness of Internet governance

Abstract: Digital culture has a valence that is affected by the ongoing globalization and determines its development. This paper places emphasis on the possibility of considering an exercise of religious freedom in the digital society, that is, it verifies how the freedoms and rights, which, as corollaries, derive from religious freedom, can be combined with an "online" exercise of worship. The digital has become the medium that breaks down the barriers of space and time more than any other: the same essential assembly of the faithful that becomes an assembly, open, but at the same time not virtual, but rather characterized by the new form of participation. Starting from the analysis of the assignment of top-level domain names, the centrality of implementing effective Internet governance will then be highlighted, aimed at ensuring among others, global integration, defense of people's rights, and in general cultural, economic, and social opportunities for everyone while respecting the effective protection of everyone's right to privacy and protection of personal data.

Keywords: Internet access – Online rights – Freedom of religion – Privacy – Internet governance

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0077
Articolo sottoposto a peer review

Lo smart working in Italia tra rivoluzione culturale, normativa emergenziale e un futuro ancora da scrivere

Paola Polliani • Andrea Coldesina

L'articolo presenta la nascita e lo sviluppo del lavoro agile in Italia, dal 2017 ad oggi. Entrambi i momenti sono visti attraverso lo sguardo dell'avvocato giuslavorista, le cui lenti sono state chiamate in questi anni ad interpretare e tradurre in applicazione concreta una disciplina più volte adattata alle esigenze del momento ed alle trasformazioni della società. Dopo un'introduzione dedicata alla transizione digitale, di cui il lavoro in modalità agile rappresenta, per l'appunto, un'espressione, l'analisi degli autori ripercorre le origini della disciplina dettata in materia nel nostro ordinamento giuridico. Dal primo periodo, caratterizzato da un utilizzo prudente della modalità lavorativa agile, sino all'ampia diffusione della stessa a seguito della pandemia da Covid-19, per arrivare ai possibili effetti sull'organizzazione aziendale, fino alle norme che traghetteranno lo smart working alla disciplina post emergenziale.

Lavoro agile – Transizione digitale – Ordinamento – Organizzazione – Prestazione

Sommario: *1. La transizione digitale e il rilancio dello smart working in Italia – 2. Dall'essenzialità della disciplina originaria al susseguirsi delle norme d'urgenza. La diffusione della modalità di lavoro cd. "agile" durante la pandemia – 3. Il lavoro agile nel rapporto con le altre norme dell'ordinamento: il diritto alla disconnessione – 4. Le modifiche normative all'orizzonte*

1. La transizione digitale e il rilancio dello smart working in Italia

La transizione digitale, ovvero l'insieme delle trasformazioni sociali, culturali e tecnologiche associate all'utilizzo della tecnologia digitale, è un fenomeno in evoluzione costante in tutti i settori della società, dal diritto all'economia, dalla medicina all'attività manifatturiera. E proprio in nome della transizione digitale le imprese stanno via via modificando i loro processi interni in modo sempre più virtuoso, discostandosi dai vecchi paradigmi organizzativi e muovendosi verso approcci che si concentrino sulle nuove tecnologie per ottimizzare processi, dati e soluzioni. Gli ostacoli da superare, in questa direzione, non sono pochi, soprattutto se si pensa che l'Italia, secondo l'Indice di digitalizzazione dell'economia e della società – il cd. "DESI" – elaborato per il 2021, occupa la ventesima posizione rispetto agli attuali 27 Stati membri dell'Unione europea, con un punteggio pari a 45,5 (la media europea è 50,7)[1].

Nel nostro Paese una prima sfida è rappresentata senza dubbio dalla necessità di superare il divario Nord/Sud sotto il profilo dell'accesso alla connettività e, in particolar modo, attraverso fibra ottica e 5G. Una condizione che al momento non consente di

Paola Polliani è avvocato e socia dello Studio Franzosi Dal Negro Setti, responsabile del dipartimento di Diritto del lavoro e delle relazioni industriali. Andrea Coldesina è avvocato; ha maturato un'esperienza pluriennale nel settore del Diritto del lavoro e delle relazioni sindacali, nonché della previdenza sociale.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

immaginare uno sviluppo omogeneo del Paese e che richiede immediati interventi strutturali[2]. Al tempo stesso, occorrerebbe necessariamente migliorare le competenze in ambito digitale della popolazione, attraverso un percorso che, in tempi rapidi, consenta di realizzare il traguardo di una vera e propria "alfabetizzazione" digitale[3]. Un obiettivo di difficile realizzazione, ma assolutamente prioritario nell'ottica di una concreta trasformazione digitale del Paese, è rappresentato dall'ammodernamento e digitalizzazione della pubblica amministrazione, da compiersi attraverso il passaggio al cloud, il coordinamento per la diffusione dell'identità digitale, ma, soprattutto, mediante la definizione di una politica nazionale per la gestione e l'analisi dei dati. Nella stessa direzione debbono muoversi rapidamente l'innovazione digitale in ambito sanitario e quella nell'ambito dell'istruzione e della ricerca scientifica. Nel primo caso, gli obiettivi da perseguire sono la realizzazione di una concreta assistenza remota ai pazienti e l'adozione su tutto il territorio nazionale di modelli di gestione della sanità che consentano alla popolazione di avere un rapporto più stretto e immediato con medici e strutture. Nel secondo, gli investimenti dovrebbero essere veicolati al fine di consentire la diffusione di scuole che diano vere competenze tecnologiche agli studenti, implementando le competenze informatiche, tanto di base quanto avanzate, lasciando alle spalle disparità sociali, geografiche ed economiche.

Le risorse economiche necessarie a realizzare concretamente la transizione digitale prevista per i prossimi anni saranno, per lo più, attinte dal Pnrr (Piano nazionale di ripresa e resilienza). Il capitolo del Piano dedicato a "Digitalizzazione, innovazione, competitività, cultura e turismo" prevede complessivamente 40,49 miliardi di euro, pari al 21% dell'intero programma. Si tratta di fondi consistenti che, verosimilmente, daranno una scossa positiva al processo di ammodernamento del Paese da un punto di vista sia strutturale sia organizzativo[4]. Si può, quindi, in qualche modo affermare che le risorse economiche indispensabili per la realizzazione del programma di transizione digitale saranno reperibili anche in virtù della necessità di rilanciare l'economia nazionale dopo lo stallo causato dalla pandemia da Covid-19. L'emergenza sanitaria degli ultimi anni ha inevitabilmente accelerato quei processi di valutazione già avviati nel corso del decennio precedente, ed ha fatto sorgere nuove problematiche e temi di discussione: durante i lockdown, il ricorso forzato alla tecnologia e, in modo particolare, allo smart working ha costretto a un sostanziale ripensamento di tale modalità di svolgimento dell'attività lavorativa; in particolare, si è tornati a parlare di lavoro agile sia per le implicazioni riguardanti i diritti dei lavoratori, sia per la necessità di ripensare la stessa organizzazione degli apparati produttivi e della pubblica amministrazione[5]. Si può dire, insomma, che il lavoro agile abbia conosciuto proprio durante il periodo pandemico una "seconda giovinezza", dimostrandosi, pur rivelando qualche limite procedurale e richiedendo alcuni accorgimenti, uno strumento flessibile e adattabile ad una situazione decisamente diversa da quella per cui era stato originariamente pensato. Di fatto, da strumento utilizzato solo da una cerchia ristretta di lavoratori, il lavoro agile è diventato, in poco tempo, una modalità di lavoro largamente diffusa, a tratti persino generalizzata.

La flessibilità come punto di forza, dunque, ma non solo. Il lavoro agile presenta caratteristiche notevolmente impattanti sulla vita quotidiana dei lavoratori e sull'organizzazione della stessa attività lavorativa. Secondo un'indagine dell'*Economist* del 10 aprile 2021[6], il lavoro a distanza generalizzato sta già producendo effetti di ibridazione permanente non solo dei luoghi di lavoro ma anche del modo in cui il lavoro stesso viene percepito dai suoi attori. Da un lato, si registra un incremento del coinvolgimento dei lavoratori e dell'identificazione di questi ultimi con l'impresa e con i suoi obiettivi. Dall'altro, ciò che sorprende è la nuova considerazione che ciascun lavoratore agile sembra sviluppare in merito al lavoro di superiori e colleghi, attraverso una valorizzazione della dimensione relazionale dell'attività lavorativa[7]. Il lavoro agile richiede, infatti, un'organizzazione di lavoro che si sviluppi per progetti, articolati in fasi, percorsi e cicli. In questa nuova tipologia di organizzazione si inserisce la figura di un manager cui si richiedono competenze trasversali di base, ma anche competenze informatiche, statistiche, linguistiche. Soprattutto, alle figure manageriali è e sarà sempre più richiesta una capacità di coordinamento delle risorse che non si realizzi solo attraverso il mero controllo, ma che si traduca in una valorizzazione delle loro qualità specifiche. E ciò allo scopo di favorire e rendere possibile la delega di attività sempre più significative da parte del manager ai suoi riporti, in un clima di mutuo rispetto e scambio relazionale che possa incidere positivamente anche in termini di produttività.

Da ultimo, il lavoro agile rappresenta uno dei principali strumenti di realizzazione della sostenibilità in ambito lavorativo. In proposito, si sente sempre più spesso parlare di "ESG", come acronimo di: "Environmental", "Social" e "Governance". La sigla in questione indica, in massima sintesi, un sistema di rating idoneo a consentire una valutazione del livello di sostenibilità delle aziende in relazione alle pre-

dette tematiche. Lo smart working, infatti, non solo incide sulla produttività e sull'organizzazione del lavoro, ma può avere anche un effetto positivo anche sull'ambiente: più persone che lavorano da casa determinano, in effetti, meno spostamenti in automobile, con una conseguente diminuzione degli sprechi di carburante e, soprattutto, delle emissioni di agenti inquinanti. Ma il lavoro da casa e una minore presenza in ufficio consentono anche una riduzione del consumo energetico derivante dall'uso dei dispositivi elettronici necessari allo svolgimento dell'attività lavorativa, così come di quello necessario al riscaldamento ed al raffreddamento degli uffici. Si può, tuttavia, affermare che, in fondo, il più significativo contributo dello smart working alla sostenibilità derivi da un miglioramento complessivo dell'efficienza lavorativa, del cd. *worklife balance* e, infine, del livello di motivazione dei singoli lavoratori.

2. Dall'essenzialità della disciplina originaria al susseguirsi delle norme d'urgenza. La diffusione della modalità di lavoro cd. "agile" durante la pandemia

Il lavoro agile ha conosciuto una prima ed organica traduzione normativa nel nostro ordinamento giuridico con la l. 22 maggio 2017, n. 81, dedicata all'introduzione di forme di tutela del lavoro autonomo non imprenditoriale ed alla realizzazione di misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato. L'art. 18 della predetta legge, in particolare, ha precisato i contenuti del lavoro agile, definendolo come una «modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa». Una modalità di svolgimento della prestazione lavorativa che, secondo quanto previsto dalla norma, può essere eseguita, «in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva».

Alla luce di una definizione quale quella appena menzionata, appare chiaro come l'inserimento nell'ambito di una legge dedicata al lavoro autonomo di una disciplina organica dello smart working non sia stato certamente casuale: il legislatore ha, cioè, immaginato una prestazione lavorativa modellata su quella già caratterizzante il lavoro autonomo e fondata, quindi, non più sulla messa a disposizione delle energie lavorative in favore dell'azienda, bensì sulla base di un risultato da raggiungere anche per fasi, cicli ed obiettivi; ciò con il duplice intento di ottenere un incremento della competitività, da un lato, e una più semplice conciliazione dei tempi di vita e di lavoro, dall'altro. Una disciplina, quella introdotta dal legislatore nel 2017, volutamente flessibile ed essenziale, pensata e dettata nell'ottica di conseguire un sostanziale contemperamento tra gli interessi datoriali e la tutela dei lavoratori mediante un accordo tra le parti a suggellarne l'intesa, da considerarsi accessorio rispetto al rapporto di lavoro subordinato in essere tra le medesime[8].

Peraltro, è facilmente verificabile come attraverso una dettagliata disciplina delle modalità di svolgimento della prestazione lavorativa da remoto sia possibile disinnescare in radice una parte consistente delle controversie che possono sorgere tra le parti, anche con riferimento ai rapporti tra la fattispecie in oggetto ed i singoli istituti e strumenti di tutela già ampiamente utilizzati dalle aziende[9,10].

Attraverso l'accordo di smart working, ad esempio, le aziende hanno l'opportunità di individuare le condotte, connesse all'esecuzione della prestazione lavorativa all'esterno dei locali aziendali, potenzialmente idonee a dar luogo all'applicazione di sanzioni disciplinari, definendo in tal modo i contorni di esercizio del potere disciplinare e di controllo nel rispetto dell'art. 4 l. 20 maggio 1970, n. 300 (Statuto dei lavoratori) [da ora in avanti S.L.], così come modificato dall'art. 23, d.lgs. 14 settembre 2015, n. 151. E proprio sul rapporto tra la predetta norma ed il ricorso al lavoro agile si è incentrato il dibattito sulla distinzione, prevista dall'art. 4 S.L., tra gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, liberamente utilizzabili dalle aziende[11], dagli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori[12], utilizzabili esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, e per le quali l'art. 4 S.L. comma 1 prevede, inoltre, la sottoscrizione di un accordo collettivo aziendale oppure il rilascio di un'autorizzazione amministrativa da parte dell'Ispettorato del Lavoro.

La diffusione dello smart working, nei primi anni di applicazione della legge che lo ha introdotto nel nostro ordinamento, è stata probabilmente frenata da una cultura manageriale ancora impreparata e legata a doppio filo ad esigenze di accentramento organizzativo e di controllo dei lavoratori e delle loro attività. Il timore che il ricorso al lavoro agi-

le possa determinare uno sfilacciamento dell'organizzazione aziendale e della sua efficienza nel nome di una conciliazione tra esigenze di vita e di lavoro che, evidentemente, ancora fatica ad affermarsi davvero, ha, in sostanza, rappresentato un freno allo sviluppo ed alla diffusione di questa modalità di svolgimento della prestazione lavorativa[13].

In fondo, una dimostrazione di quanto appena evidenziato pare potersi ravvisare nel fatto che la maggior parte delle aziende italiane, anziché adottare modelli di lavoro agile vero e proprio, abbia scelto di avvalersi dello strumento del telelavoro, uno strumento piuttosto datato – a dire il vero – che rispetto allo smart working presenta, però, il vantaggio di una puntuale individuazione della sede lavorativa, prestabilita e concordata tra le parti e normalmente coincidente con l'abitazione del lavoratore stesso. Una modalità di svolgimento della prestazione che, in qualche modo, sembra, pertanto, suscitare meno diffidenza e garantire una maggiore possibilità di verifica e controllo della performance.

La situazione emergenziale, dovuta alla pandemia da Covid-19 ha, in ogni caso, riacceso quasi improvvisamente i riflettori sul lavoro agile, individuato dal Governo quale principale strumento per far fronte alle difficoltà improvvise di organizzazione del lavoro. La normativa specificamente introdotta a riguardo ed in particolar modo il d.l. 19 maggio 2020, n. 34, convertito in l. 17 luglio 2020, n. 77, con l'intento di snellire l'iter procedurale previsto dalla legge, ha fatto venir meno, fino alla cessazione dello stato di emergenza epidemiologica, la necessità di sottoscrivere accordi scritti di smart working tra le parti, sostituendoli con una comunicazione in via telematica al Ministero del Lavoro del numero, dei nominativi e della durata del periodo di svolgimento della prestazione in modalità agile con riferimento a tutti i dipendenti coinvolti[14]. La norma ha, inoltre, confermato l'obbligo per le aziende di effettuare le comunicazioni relative ai rischi lavorativi sia all'INAIL che ai lavoratori, facendo salve, per quanto non previsto, le disposizioni di cui alla l. 81/2017.

Nel corso dei mesi successivi all'introduzione del regime semplificato previsto dal d.l. 34/2020, si sono susseguiti numerosi interventi del Governo in materia di lavoro agile e con lo specifico intento di offrire un sostegno ai genitori ed alle categorie considerate maggiormente svantaggiate.

Inizialmente, con il d.l. 13 marzo 2021, n. 30, convertito con modificazioni dalla l. 6 maggio 2021, n. 61, il Governo aveva garantito, in via alternativa tra i genitori e compatibilmente con le mansioni svolte, il diritto allo smart working in caso di quarantena del figlio minore di anni sedici per tutta la durata della medesima, di sospensione della didattica in presenza o di infezione da SARS Covid-19. In caso di impossibilità di adibizione del genitore al lavoro in modalità agile era stato riconosciuto al medesimo, sempre in via alternativa rispetto all'altro genitore, il diritto ad astenersi dal lavoro per i medesimi periodi poc'anzi ricordati, senza corresponsione di retribuzione o indennità e senza contribuzione figurativa in caso di figlio convivente minore di anni sedici, ma maggiore di quattordici, con divieto di licenziamento e diritto alla conservazione del posto di lavoro. In caso di figlio convivente minore di anni quattordici, invece, il genitore lavoratore avrebbe avuto diritto a percepire un'indennità, su base giornaliera oppure oraria, pari al 50% della retribuzione.

Sempre il d.l. 30/2021 aveva previsto che entrambi i genitori di figli, di qualunque età, con disabilità grave, accertata ai sensi della l. 5 febbraio 1992, n. 104, o con disturbi specifici dell'apprendimento riconosciuti ai sensi della l. 8 ottobre 2010, n. 170, o con bisogni educativi speciali, secondo quanto previsto dalla Direttiva del Ministro dell'Istruzione, dell'Università e della Ricerca del 27 dicembre 2012, avessero diritto a svolgere l'attività lavorativa in modalità agile. Laddove il lavoro in modalità agile non fosse stato praticabile, il lavoratore genitore di figli conviventi, di qualsiasi età, con disabilità in situazione di gravità accertata ai sensi dell'art. 3, co. 3, l. n. 104/1992, avrebbe potuto, alternativamente all'altro genitore, astenersi dal lavoro per il periodo corrispondente alla sospensione dell'attività didattica in presenza a scuola o alla chiusura del centro diurno a carattere assistenziale che ospita il figlio disabile.

Da ultimo, con la l. 19 maggio 2022, n. 52, di conversione con modificazioni del d.l. 24 marzo 2022, n. 24, è stato prorogato sino al 31 luglio 2022 il diritto, per i genitori lavoratori dipendenti del settore privato che abbiano almeno un figlio minore di 14 anni, a condizione che nel nucleo familiare non vi sia altro genitore beneficiario di strumenti di sostegno al reddito in caso di sospensione o cessazione dell'attività lavorativa o che non vi sia genitore non lavoratore, a svolgere la prestazione di lavoro in modalità agile anche in assenza degli accordi individuali e a condizione che tale modalità sia compatibile con le caratteristiche della prestazione. Il medesimo diritto allo svolgimento delle prestazioni di lavoro in smart working è stato, inoltre, riconosciuto, sulla base delle valutazioni dei medici competenti e sempre fino al 31 luglio 2022, anche ai lavoratori maggiormente esposti a rischio di contagio, in ragione dell'età o della condizione di rischio derivante da immunodepressione, da esiti di patologie oncologiche o dallo svolgimento di terapie salvavita o, comunque, da comorbilità che

possono caratterizzare una situazione di maggiore rischiosità accertata dal medico competente, sempre a condizione che tale modalità sia compatibile con le caratteristiche della prestazione lavorativa.

Il Governo è, infine, intervenuto anche con alcune norme specificamente dedicate ai soggetti caratterizzati da gravi disabilità certificate ai sensi della l. 104/1992[15], ed ai lavoratori cd. "fragili" a causa di fattori come età, immunodepressione, patologie oncologiche, svolgimento di terapie salvavita o, comunque, affetti da comorbilità che possono caratterizzare una situazione di maggiore rischiosità accertata dal medico competente[16]. Alle predette categorie, con il d.l. 22 marzo 2021, n. 41, è stato riconosciuto il diritto allo svolgimento della prestazione lavorativa in modalità agile, a condizione che tale modalità sia compatibile con le caratteristiche della loro prestazione lavorativa, anche attraverso l'adibizione a diversa mansione ricompresa nella medesima categoria o area di inquadramento. Tutto ciò, in una prima fase, soltanto sino al 30 giugno 2021, termine in seguito più volte prorogato, da ultimo con la l. 19 maggio 2022, n. 52, di conversione con modificazioni del d.l. 24 marzo 2022, n. 24, sino al 30 giugno 2022. Sempre fino al 30 giugno 2022 resta inoltre ferma, per i lavoratori fragili la cui prestazione non possa essere svolta a distanza, la possibilità di equiparare l'assenza a ricovero ospedaliero. In proposito, si evidenzia come in data 4 febbraio 2022 sia stato emanato il decreto interministeriale con cui, ai sensi del co. 2, art. 17, d.l. 221/2021, sono state individuate le c.d. «patologie croniche con scarso compenso clinico e con particolare connotazione di gravità, in presenza delle quali [...] la prestazione lavorativa è normalmente svolta in modalità agile».

Come risulta evidente dal continuo susseguirsi ed accavallarsi di norme quali quelle sin qui descritte, la fase emergenziale si è sempre contraddistinta per una, forse inevitabile, ipertrofia legislativa. Un tentativo di "tirare le fila" di una regolamentazione divenuta nel corso dei mesi sfilacciata e, a tratti, poco comprensibile, è stato realizzato con il Protocollo siglato il 7 dicembre 2021 da Governo e Parti Sociali allo scopo di fornire a imprese e lavoratori del settore privato le linee guida con cui disciplinare, nell'ambito della contrattazione collettiva, il lavoro agile.

Secondo il Protocollo, l'adesione allo smart working avviene su base volontaria ed è subordinata alla sottoscrizione di un accordo individuale, fermo restando il diritto di recesso. Inoltre, l'eventuale rifiuto del lavoratore di aderire o svolgere la propria prestazione lavorativa in modalità agile non integra gli estremi del licenziamento per giusta causa o giustificato motivo, né rileva sul piano disciplinare. Inoltre, il Protocollo prevede, in dettaglio, i contenuti che l'accordo scritto deve presentare. Tra questi ricordiamo, ad esempio, le previsioni relative all'alternanza tra i periodi di lavoro all'interno e all'esterno dei locali aziendali, ai luoghi eventualmente esclusi per lo svolgimento della prestazione lavorativa al di fuori dei locali aziendali, agli aspetti relativi all'esecuzione della prestazione lavorativa svolta al di fuori dei locali aziendali, anche con riguardo alle forme di esercizio del potere direttivo del datore di lavoro e alle condotte che possono dar luogo all'applicazione di sanzioni disciplinari nel rispetto della disciplina prevista nei contratti collettivi, ai tempi di riposo del lavoratore ed alle misure tecniche e/o organizzative necessarie ad assicurare la disconnessione, alle forme ed alle modalità di controllo della prestazione lavorativa all'esterno dei locali aziendali, nel rispetto di quanto previsto sia dall'art. 4 S.L., sia dalla normativa in materia di protezione dei dati personali, le forme e le modalità di esercizio dei diritti sindacali.

Poche settimane dopo la firma del Protocollo, peraltro, con il d.l. 221/2021, convertito con modifiche dalla l. 11/2022, il Governo ha previsto la proroga dello stato di emergenza nazionale sino al 31 marzo 2022, estendendo, quindi, sino a tale data anche la possibilità per le aziende di avvalersi del regime di smart working semplificato; possibilità da ultimo estesa, in virtù di quanto previsto dalla l. 19 maggio 2022, n. 52, di conversione con modificazioni del d.l. 24 marzo 2022, n. 24, sino al 31 agosto 2022.

Dal 1° settembre 2022, le aziende e i singoli lavoratori torneranno, invece, obbligatoriamente a sottoscrivere tra loro accordi individuali allo scopo di definire le modalità di effettuazione della prestazione resa al di fuori dei locali aziendali in modalità "agile". Sono attualmente in fase di studio alcune misure strutturali di semplificazione delle comunicazioni obbligatorie al Ministero del Lavoro che, secondo quanto anticipato, avranno ad oggetto soltanto la comunicazione dei nominativi dei lavoratori e la data di inizio e cessazione delle prestazioni di lavoro in modalità agile, senza più alcuna necessità di allegare copia dell'accordo individuale sottoscritto con il singolo lavoratore.

3. Il lavoro agile nel rapporto con le altre norme dell'ordinamento: il diritto alla disconnessione

Nel proseguire nella nostra breve disamina, infine, riteniamo opportuno accennare anche ad alcune tra le principali problematiche emerse nel corso degli ultimi mesi a fronte dell'utilizzo massivo alla modalità agile di svolgimento della prestazione lavorativa. Un pri-

mo problema che aziende e lavoratori si sono trovate ad affrontare ha, ad esempio, riguardato l'assoggettamento o meno a tassazione dei rimborsi forfettari delle spese sostenute dai dipendenti in smart working. Ebbene, sul punto, l'Agenzia delle Entrate, con la risposta n. 328/2021 ad interpello, ha precisato che tali rimborsi non possano essere esclusi «in assenza di una precisa disposizione di legge al riguardo, dalla determinazione del reddito di lavoro dipendente».

Per evitare che i rimborsi spese concorrano alla determinazione del reddito di lavoro dipendente occorrerebbe, invece, secondo l'Agenzia, adottare, in luogo della citata forfettizzazione dei costi, un criterio analitico che permetta di individuare con esattezza il risparmio della società con riferimento ai singoli costi sostenuti dal dipendente (es: energia elettrica, Internet etc.). Solo i rimborsi dei predetti costi, certamente sostenuti nell'interesse esclusivo del datore di lavoro, dovrebbero essere, quindi, esclusi dal reddito da lavoro dipendente.

Un discorso a parte merita, infine, il cd. "diritto alla disconnessione", introdotto dal legislatore solo in sede di conversione del d.l. 30/2021. Per la verità, la previsione di una clausola che disciplinasse, all'interno dell'accordo di smart working, la disconnessione del lavoratore era già prevista dall'art. 19, l. 81/2017. Si trattava, per l'appunto, soltanto di un generico rinvio, sul punto, alla negoziazione tra le parti, mentre la norma non dettava una disciplina generale in materia di disconnessione. In epoca più recente, anche il Parlamento europeo era intervenuto sul punto, invitando la Commissione a formulare una proposta di Direttiva dell'Unione riguardante le tutele minime in favore dei lavoratori in smart working, tra cui l'esercizio efficace del diritto alla disconnessione[17].

Non vi è dubbio che le difficoltà causate dalla pandemia ed il ricorso al lavoro agile come soluzione lavorativa emergenziale abbiano, da ultimo, determinato un'accelerazione della spinta alla ricerca di una disciplina più specifica della materia, anche con riferimento alla disconnessione dei lavoratori[18].

Nel nostro ordinamento, con l'articolo 1-*ter*, l. 61/2021[19] è stato, dunque, per la prima volta riconosciuto un vero e proprio diritto del lavoratore che presti la propria opera in modalità agile alla disconnessione, con i limiti rappresentati dalle clausole di cui all'accordo scritto di smart working tra le parti e, in particolare, da quelle riguardanti le fasce di reperibilità concordate in base alle esigenze organizzative aziendali, alle mansioni del lavoratore ed alle esigenze di quest'ultimo. Durante le fasce di reperibilità il lavoratore ha l'obbligo di essere connesso alla piattaforma in cloud o al server aziendale attraverso gli strumenti tecnologici in dotazione e di svolgere la sua prestazione lavorativa. Al di fuori delle predette fasce, al contrario, l'esercizio del suo diritto alla disconnessione legittima il divieto per il datore di lavoro e per i colleghi di contattarlo. Un profilo indubbiamente interessante, sotto il profilo della gestione dei rapporti con i lavoratori, è rappresentato dalla possibilità di prevedere nell'ambito dell'accordo scritto di smart working, attraverso uno specifico richiamo al codice disciplinare aziendale, le sanzioni disciplinari nei confronti del lavoratore che, senza alcuna giustificazione, risulti non reperibile nelle fasce orarie pattuite.

Infine, come sopra ricordato, il recente Protocollo nazionale sul lavoro in modalità agile del 7 dicembre 2021, ha previsto che permanga l'obbligo di individuare la fascia di disconnessione, nella quale il lavoratore non deve erogare alcuna prestazione[20]. Inoltre, viene previsto che il datore dovrà adottare specifiche misure tecniche e organizzative per garantire la fascia di disconnessione. Già all'interno di molti sistemi aziendali vengono bloccate le attività dopo determinate fasce orarie non consentendo comunicazioni in entrata e in uscita nel rispetto del periodo di riposo giornaliero o settimanale del lavoratore. Resta ferma la possibilità per il lavoratore di sospendere la prestazione lavorativa usufruendo dei permessi. Inoltre, con il protrarsi nel tempo della situazione emergenziale e, con essa, dell'applicabilità dello smart working in modalità semplificata, registriamo anche i primi interventi, a riguardo, da parte delle Autorità ispettive e di garanzia. In proposito, si ritiene doveroso sottolineare l'importanza, anche sotto il profilo della collaborazione strategica tra gli organismi istituzionali coinvolti, del Protocollo sottoscritto il 22 aprile 2021 dall'Ispettorato nazionale del lavoro e dal Garante per la protezione dei dati personali, al fine di dettare norme di contrasto all'illecito utilizzo di forme e modalità occulte di controllo della prestazione lavorativa[21]. Un controllo reso possibile dalla necessaria installazione su dispositivi utilizzati dai lavoratori di software e applicativi idonei a violare la privacy degli stessi. Sulla base del documento, che ha una validità di due anni, l'Ispettorato e l'Autorità garante si sono impegnate a realizzare incontri semestrali allo scopo di scambiarsi informazioni ed esperienze sul tema, a porre in essere campagne di informazione comuni, così da prevenire il più possibile il diffondersi di modalità di trattamento dati non conformi all'attuale disciplina in materia di privacy e controlli a distanza della prestazione lavorativa e, infine, a realizzare attività formative in materia di lavoro agile e controlli da remoto.

4. Le modifiche normative all'orizzonte

In conclusione, nessun dubbio, alla prova dei fatti, può emergere in relazione all'efficacia del lavoro agile, implementato e rafforzato in tempi di pandemia in virtù dei numerosi e successivi interventi del Governo. Ciò su cui è lecito interrogarsi oggi, semmai, è se lo smart working, una volta esaurito lo stato di emergenza, possa finalmente trovare un proprio definitivo radicamento non solo normativo, ma anche concreto ed effettivo, diventando una modalità di lavoro efficace per un numero sempre crescente di realtà aziendali. Il lavoro agile rappresenta, in effetti, un passo significativo verso la già menzionata "transizione digitale", ovvero la trasformazione organizzativa, sociale e culturale propedeutica, per le aziende, alla realizzazione del business digitale. Un vero e proprio cambiamento, dal punto di vista della cultura aziendale, che permette ai lavoratori di acquisire nuove competenze per rispondere alle esigenze del cambiamento digitale. Naturalmente, perché una rivoluzione di tale portata possa completarsi occorrerà fare ancora qualche passo nella direzione del superamento di quelle resistenze e di quello scetticismo che fisiologicamente accompagna ogni fase di evoluzione, anche attraverso la predisposizione di un apparato normativo idoneo a rappresentare il sostrato regolamentare del cambiamento culturale.

In tale direzione dovrebbero muoversi le modifiche alla disciplina attualmente vigente in materia di lavoro agile. Il 16 marzo 2022 la Commissione Lavoro della Camera dei Deputati ha, infatti, approvato la proposta di legge su "Disposizioni in materia di lavoro agile e di lavoro a distanza" contenente una serie di modifiche delle norme di cui al Capo II, l. 81/2017, dedicata, come ricordato nei precedenti paragrafi, al lavoro agile.

In primo luogo, è evidente la volontà del legislatore di coinvolgere maggiormente le parti sociali nella disciplina del lavoro agile: se l'accordo individuale non è, infatti, destinato a scomparire, la modifica interverrebbe, anzitutto, sull'art. 18 della legge appena citata, con un articolo 1 comma 1 del testo approvato in Commissione che prevede che il CCNL stipulato dalle organizzazioni sindacali comparativamente più rappresentative sul piano nazionale «nonché i contratti collettivi stipulati ai sensi dell'articolo 51 del decreto legislativo 15 giugno 2015, n. 81» disciplinino: a) la responsabilità del datore di lavoro e del lavoratore per quanto attiene alla sicurezza e al buon funzionamento degli strumenti tecnologici; b) il diritto alla priorità riguardante le richieste di esecuzione del rapporto di lavoro in modalità agile delle seguenti categorie di lavoratori: i) lavoratrici e lavoratori nei tre anni successivi alla conclusione del periodo di congedo di maternità e di paternità; ii) lavoratori con figli in condizioni di disabilità; iii) lavoratori portatori di handicap di cui all'articolo 33, comma 3, della legge n. 104; iv) lavoratori che svolgono funzione di *caregiver* familiare; c) l'equiparazione del lavoratore che svolge la propria attività in modalità agile con il personale operante in presenza; d) il diritto a usufruire delle ferie e dei permessi, con le modalità previste dalla legge e dai contratti collettivi; e) il diritto alla disconnessione.

Proprio il diritto alla disconnessione, da intendersi come «il diritto di estraniarsi dallo spazio digitale e di interrompere la connessione dalle strumentazioni tecnologiche e dalle piattaforme informatiche in proprio possesso, senza che questo possa comportare effetti negativi di natura disciplinare o decurtazioni retributive» secondo quanto previsto dal Testo approvato in Commissione, verrebbe aggiunto all'art. 24, l. 81/2017.

Il Testo Unificato approvato dalla Commissione Lavoro della Camera propone, oltre alle modifiche citate, una serie di incentivi dedicate alle imprese che facilitano l'implementazione delle modalità di smart working: in particolare, nel testo in questione è prevista l'introduzione di un credito d'imposta per l'acquisto, entro due anni dall'entrata in vigore della disciplina, di nuovi strumenti informatici destinati ad agevolare le attività da remoto, oltre all'applicazione di una riduzione dell'1 per cento sui premi assicurativi INAIL a carico del datore di lavoro. Infine, il testo prevede l'adozione di numerose misure di formazione ed aggiornamento delle competenze dei lavoratori, attraverso l'organizzazione di corsi di formazione e aggiornamento di livello operativo e corsi di aggiornamento sull'innovazione tecnologica.

Note

[1]Il *Digital Economy and Society Index* (DESI) è un indice composito che fornisce informazioni sullo stato di digitalizzazione dei paesi membri sulla base di dati aggregati, e svolge due compiti principali: monitorare le prestazioni digitali complessive e seguire i progressi dei singoli paesi dell'UE nella competitività digitale.

[2]Secondo l'indice DESI 2021, in termini di connettività l'Italia raggiunge un punteggio di 42,4 e nonostante il tasso relativamente elevato di preparazione al 5G (60%), solo l'8% delle zone abitate è coperto dal 5G, un dato inferiore alla media UE pari al 14%.

[3]Il 42% delle persone di età compresa tra i 16 e i 74 anni possiede perlomeno competenze digitali di base. Mentre la media europea è del 56% e solo il 22% dispone di competenze digitali superiori a quelle di base rispetto al 31% della media europea (dati indice DESI 2021).

[4]Le risorse stanziate nel Piano sono pari a 191,5 miliardi di euro, ripartite in sei missioni: Digitalizzazione, innovazione, competitività e cultura - 40,32 miliardi; Rivoluzione verde e

transizione ecologica - 59,47 miliardi; Infrastrutture per una mobilità sostenibile - 25,40 miliardi; Istruzione e ricerca - 30,88 miliardi; Inclusione e coesione - 19,81 miliardi; Salute - 15,63 miliardi. Per finanziare ulteriori interventi il Governo italiano ha approvato un Fondo complementare con risorse pari a 30,6 miliardi di euro (dati forniti dal Ministero dello sviluppo economico). Complessivamente gli investimenti previsti dal PNRR e dal Fondo complementare sono pari a 222,1 miliardi di euro.

[5]Lo smart working ha coinvolto più di 7 milioni di lavoratori nel corso del 2021, secondo l'indagine INAPP (Istituto Nazionale per l'Analisi delle Politiche pubbliche) diffusa il 26 gennaio 2022. Un grande traguardo se si pensa che si tratta di un approccio al lavoro ancora sperimentale e visionario nell'era pre-pandemia e che ormai, invece, si sta avvicinando ad un'applicazione più stabile e diffusa. Già nel 2021, inoltre, una ricerca dell'*Osservatorio Smart Working* metteva in evidenza come il fenomeno fosse comune a tutte le tipologie di organizzazione, dalle grandi imprese (per l'81%), alle PMI (per il 53%) sino alle PA (per il 67%), con l'ingombrante questione dei sistemi adeguati di policy a incombere per queste ultime due realtà (quali, ad esempio, la mancanza di adeguati regolamenti sul lavoro per obiettivi o sulla collaborazione digitale).

[6]Cfr. *The future of work*, in "The Economist", 10 April 2021.

[7]Cfr. B. Caruso, L. Zappalà, *Un diritto del lavoro "tridimensionale": valori e tecniche di fronte ai mutamenti dei luoghi di lavoro*, in R. Del Punta (a cura di), "Valori e tecniche nel diritto del lavoro", Firenze University Press, 2022, pp. 29-80.

[8]L'art. 19 della l. 81/2017 disciplina in modo piuttosto dettagliato i contenuti dell'accordo tra le parti, vincolando, quindi, queste ultime all'osservanza di alcune formalità essenziali: «L'accordo relativo alla modalità di lavoro agile è stipulato per iscritto ai fini della regolarità amministrativa e della prova, e disciplina l'esecuzione della prestazione lavorativa svolta all'esterno dei locali aziendali, anche con riguardo alle forme di esercizio del potere direttivo del datore di lavoro ed agli strumenti utilizzati dal lavoratore. L'accordo individua altresì i tempi di riposo del lavoratore nonché le misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro. L'accordo di cui al comma 1 può essere a termine o a tempo indeterminato; in tale ultimo caso, il recesso può avvenire con un preavviso non inferiore a trenta giorni. Nel caso di lavoratori disabili ai sensi dell'art. 1, l. 12 marzo 1999, n. 68, il termine di preavviso del recesso da parte del datore di lavoro non può essere inferiore a novanta giorni, al fine di consentire un'adeguata riorganizzazione dei percorsi di lavoro rispetto alle esigenze di vita e di cura del lavoratore. In presenza di un giustificato motivo, ciascuno dei contraenti può recedere prima della scadenza del termine nel caso di accordo a tempo determinato, o senza preavviso nel caso di accordo a tempo indeterminato».

[9]In materia di revocabilità da parte del datore di lavoro dei buoni pasto concessi ai lavoratori in smart working, la Corte di Cassazione è recentemente intervenuta, affermando «la natura dei buoni pasto alla stregua, non già di elemento della retribuzione "normale", ma di agevolazione di carattere assistenziale collegata al rapporto di lavoro da un nesso meramente occasionale (Cass. 21 luglio 2008, n. 20087; Cass. 8 agosto 2012, n. 14290; Cass. 14 luglio 2016, n. 14388), pertanto non rientranti nel trattamento retributivo in senso stretto (Cass. 19 maggio 2016, n. 10354; Cass. 18 settembre 2019, n. 23303); sicché, il regime della loro erogazione può essere variato anche per unilaterale deliberazione datoriale, in quanto previsione di un atto interno, non prodotto da un accordo sindacale» (Cass. Ordinanza 28 luglio 2020, n. 16135).

[10]Di recente la Suprema Corte ha individuato – la fattispecie riguardava una lavoratrice mobbizzata dai colleghi – il ricorso allo smart working come un possibile strumento di tutela della salute psicofisica del lavoratore, evidenziando come «la mancata predisposizione di tutti i dispositivi atti a tutelare la salute dei lavoratori sul luogo di lavoro viola l'art. 32 Cost. che garantisce il diritto alla salute come primario ed originario dell'individuo, ed altresì l'art. 2087 c.c. che, imponendo la tutela dell'integrità psico-fisica del lavoratore da parte del datore di lavoro prevede un obbligo, da parte di quest'ultimo, che non si esaurisce "nell'adozione e nel mantenimento perfettamente funzionale di misure di tipo igienico-sanitarie o antinfortunistico", ma attiene anche – e soprattutto – alla predisposizione "di misure atte a preservare i lavoratori dalla lesioni di quella integrità nell'ambiente o in costanza di lavoro anche in relazione ad eventi, pur se allo stesso non collegati direttamente ed alla probabilità di concretizzazione del conseguente rischio"» (Cass. 4 dicembre 2020, n. 27913).

[11]In proposito, il Ministero del Lavoro, con nota del 10 maggio 2016 ha affermato che pc, tablet e cellulari rappresentano strumenti che «non possono essere considerati "strumenti di controllo a distanza" (...) una volta si sarebbero chiamati gli "attrezzi di lavoro"». L'Ispettorato Nazionale del Lavoro, con circolare n. 2/2016 li ha, inoltre, definiti come strumenti che costituiscono un «mezzo indispensabile» al lavoratore per adempiere la prestazione dedotta in contratto.

[12]Secondo il Garante della Privacy, che sul tema si è espresso con la Newsletter n. 419/2016, non sono strumenti di lavoro i sistemi ed i software non necessari per lo svolgimento dell'attività. Sempre il Garante della Privacy, sul punto, ha considerato illegittima l'installazione e l'utilizzazione di apparecchiature tecnologiche e di sistemi in grado di controllare in modo continuativo lo svolgimento a distanza dell'attività lavorativa. (es: piattaforme in grado di registrare ingressi, uscite e complessiva attività svolta, sistemi di *tracking* online, programmi che operano in background e come tali non percepibili dai lavoratori, consentendo una verifica costante e indiscriminata degli accessi degli utenti alla rete e all'e-mail) (cfr. Provv. Garante della Privacy nn. 303/2016 e 547/2016).

[13]Cfr. Cass. 6 dicembre 2016 n. 51897, che ha affermato l'illegittimità di controlli continuativi ed anelastici sull'attività dei lavoratori.

[14]In proposito, ad essere dirimente è sempre la tipologia delle mansioni svolte dal lavoratore. Sul punto, con il decreto n. 1054/2020, il Tribunale di Mantova ha rigettato l'istanza di una dipendente di una multinazionale dei parcheggi che aveva richiesto di svolgere la prestazione in smart working *ex* art. 90, d.l. 19 maggio 2020, n. 34, evidenziando come le mansioni svolte dal lavoratore richiedessero una sua presenza in azienda, in quanto la lavoratrice incontrava sistematicamente i referenti tecnici dei committenti ed era responsabile della sicurezza dei lavoratori.

[15]Di interesse il provvedimento con cui il Tribunale di Grosseto ha accolto un ricorso *ex* art. 700 c.p.c. di un lavoratore addetto al servizio assistenza legale che, pur essendo portatore di una patologia invalidante (invalidità civile) che ne aveva ridotto la capacità lavorativa al 60%, si era visto rifiutare dall'azienda la richiesta di lavoro agile, nonostante tutti i colleghi del suo reparto ne stessero già fruendo. L'azienda invece si era limitata a prospettargli il ricorso alle ferie «anticipate» o, alternativamente, la sospensione in assenza di retribuzione. Il provvedimento in esame, con un'interpretazione effettivamente ardita, ha affermato la sussistenza, non prevista da alcuna norma di legge, di un obbligo da parte dell'azienda di motivare il suo eventuale diniego allo svolgimento della prestazione in modalità agile richiesto dal lavoratore.

[16]Si veda, sul punto, l'ordinanza n. 5961/21 con cui il Tribunale di Roma ha accolto il ricorso *ex* art. 700 c.p.c. di una

lavoratrice, addetta alle relazioni esterne, che si era vista rifiutare la richiesta di lavoro agile inoltrata per assistere la madre, disabile *ex* art. 3, co. 3, l. 5 febbraio 1992, n. 104, e con la stessa convivente. Nel caso di specie, il Giudice ha accertato il diritto della lavoratrice a svolgere la propria prestazione in modalità "agile", in quanto compatibile con le mansioni cui era adibita, al fine di evitare il rischio di un concreto pregiudizio alla stessa ed alla madre disabile, sino alla cessazione dello stato di emergenza epidemiologica.

[17]Il Parlamento europeo, già con la risoluzione del 21 gennaio 2021, aveva invitato la Commissione «a presentare, sulla base di un esame dettagliato, di una valutazione adeguata e di una consultazione degli Stati membri e delle parti sociali, una proposta di direttiva dell'Unione su norme e condizioni minime per garantire che i lavoratori possano esercitare efficacemente il loro diritto alla disconnessione e per disciplinare l'uso degli strumenti digitali esistenti e nuovi a scopi lavorativi ...». Le raccomandazioni contenute nella Risoluzione sono orientate alla predisposizione di un sistema di tutele che contempli il riconoscimento del diritto alla disconnessione quale diritto fondamentale a tutela della salute del lavoratore, al tempo stesso stigmatizzando la «nascita di una cultura del "sempre connesso", "sempre online" o "costantemente di guardia" che può andare a scapito dei diritti fondamentali dei lavoratori e di condizioni di lavoro eque, tra cui una retribuzione equa, la limitazione dell'orario di lavoro e l'equilibrio tra attività lavorativa e vita privata, la salute fisica e mentale, la sicurezza sul lavoro e il benessere, nonché della parità tra uomini e donne, dato l'impatto sproporzionato di tali strumenti sui lavoratori con responsabilità di assistenza, che generalmente sono donne».

[18]Anche il Presidente del Garante per la protezione dei dati, nel corso della sua audizione del 13 maggio 2020 sulle «ricadute occupazionali dell'epidemia da Covid-19» aveva affermato la necessità di garantire «in modo più netto di quanto già previsto anche quel diritto alla disconnessione, senza cui si rischia di vanificare la necessaria distinzione tra spazi di vita privata e attività lavorativa, annullando così alcune tra le più antiche conquiste raggiunte per il lavoro tradizionale». In modo particolare, il Presidente aveva sottolineato la necessità di vietare alle aziende di adottare dispositivi idonei a consentire un controllo da remoto della prestazione lavorativa, in particolare impedendo, quindi, «al datore di lavoro di esercitare un monitoraggio sistematico e pervasivo dell'attività compiuta dal dipendente tramite, appunto, questo dispositivo».

[19]L'articolo 1-*ter* l. 6 maggio 2021, n. 61 ha riconosciuto ai lavoratori che prestano la loro attività in smart working il «diritto alla disconnessione dalle strumentazioni tecnologiche e dalle piattaforme informatiche, nel rispetto degli eventuali accordi sottoscritti dalle parti e fatti salvi eventuali periodi di reperibilità concordati. L'esercizio del diritto alla disconnessione, necessario per tutelare i tempi di riposo e la salute del lavoratore, non può avere ripercussioni sul rapporto di lavoro o sui trattamenti retributivi».

[20]L'art. 3 del Protocollo siglato il 7 dicembre 2021 da Governo e Parti Sociali, dedicato all'*Organizzazione del lavoro agile e regolazione della disconnessione* stabilisce che «1. Ferme restando le previsioni di legge e di contratto collettivo, la giornata lavorativa svolta in modalità agile si caratterizza per l'assenza di un preciso orario di lavoro e per l'autonomia nello svolgimento della prestazione nell'ambito degli obiettivi prefissati, nonché nel rispetto dell'organizzazione delle attività assegnate dal responsabile a garanzia dell'operatività dell'azienda e dell'interconnessione tra le varie funzioni aziendali. 2. La prestazione di lavoro in modalità agile può essere articolata in fasce orarie, individuando, in ogni caso, in attuazione di quanto previsto dalle disposizioni normative vigenti, la fascia di disconnessione nella quale il lavoratore non eroga la prestazione lavorativa. Vanno adottate specifiche misure tecniche e/o organizzative per garantire la fascia di disconnessione. 3. Il lavoratore può richiedere, ove ne ricorrano i relativi presupposti, la fruizione dei permessi orari previsti dai contratti collettivi o dalle norme di legge quali, a titolo esemplificativo, i permessi per particolari motivi personali o familiari, di cui all'art. 33 della legge 5 febbraio 1992, n. 104. 4. Salvo esplicita previsione dei contratti collettivi nazionali, territoriali e/o aziendali, durante le giornate in cui la prestazione lavorativa viene svolta in modalità agile non possono essere di norma previste e autorizzate prestazioni di lavoro straordinario. 5. Nei casi di assenze c.d. legittime (es. malattia, infortuni, permessi retribuiti, ferie, ecc.), il lavoratore può disattivare i propri dispositivi di connessione e, in caso di ricezione di comunicazioni aziendali, non è comunque obbligato a prenderle in carico prima della prevista ripresa dell'attività lavorativa. 6. Compatibilmente con l'organizzazione aziendale, le esigenze produttive e l'attività svolta dal lavoratore, al lavoro agile possono accedere, previo accordo individuale ex art. 19, l. n. 81/2017, i lavoratori inseriti nelle aree organizzative in cui lo stesso viene utilizzato».

[21]Ai sensi dell'art. 1 del Protocollo d'intesa sottoscritto il 22 aprile 2021 dall'Ispettorato nazionale del lavoro e dal Garante per la protezione dei dati personali, in particolare, si evidenzia quanto segue: «Il presente Protocollo ha per oggetto l'attivazione di una collaborazione strategica tra le Parti, nell'ambito delle rispettive competenze. Al riguardo le Parti si impegnano a realizzare processi di stabile connessione tra le due Istituzioni, al fine di assumere orientamenti condivisi su questioni specifiche, sia in una prospettiva interna di approfondimento e confronto, sia in una prospettiva esterna, implementando lo sviluppo sinergico e la coerenza delle decisioni dei due organismi». Inoltre, l'art. 2 del Protocollo in esame stabilisce che «Le Parti si impegnano a fornire reciproca collaborazione e attività consultiva sulle tematiche di rispettiva competenza, con particolare riferimento all'utilizzo di strumenti tecnologici connessi allo svolgimento del rapporto di lavoro, anche fuori dei casi in cui è previsto un parere formale, concorrendo così all'individuazione delle soluzioni più idonee e coerenti con il quadro ordinamentale».

* * *

Smart working in Italy between cultural revolution, emergency legislation and a future yet to be written

Abstract: The article shows the birth and development of smart working in Italy, from 2017 to date. Both moments are seen through the eyes of the labour lawyer, whose lens have had in recent years to interpret and translate into an actual application a discipline adapted several times to the needs, even emergency needs, of the moment and to the changes in society. After an introduction devoted to the digital transition, of which smart working is an expression, the authors' analysis retraces the origins of the relevant regulations in the Italian legal system. From the first period, characterised by a cautious use of the smart

working method, to its wide diffusion following the Covid-19 pandemic, to the possible effects on company organisation, up to the regulations that will bring smart working to the post-emergency discipline.

Keywords: Smart working – Digital transition – Legal system – Organization – Performance

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0079
Articolo sottoposto a peer review

La trasmissione dell'eredità culturale ed intellettuale delle Nazioni Unite online nel contesto internazionale della definizione di un ecosistema della governance di Internet e in particolare della scienza aperta

Deborah Grbac

Il Sistema delle biblioteche depositarie delle Nazioni Unite è da alcuni anni attivo nella condivisione di documenti, materiali e buone pratiche, anche grazie ai progetti di digitalizzazione portati avanti dalle due biblioteche presenti presso il quartier generale delle Nazioni Unite a New York e l'Ufficio delle Nazioni Unite di Ginevra. Queste hanno di fatto anticipato ed accompagnato il processo di affermazione della scienza aperta e delle pratiche di scienza aperta a livello mondiale.

Biblioteche depositarie – Nazioni Unite – Scienza aperta – UNESCO – EOSC

Sommario: *1. Ecosistema Internet e sviluppo della scienza aperta a livello internazionale – 2. Come si è arrivati a definire la scienza aperta a livello europeo e mondiale – 3. Un possibile quadro teorico di riferimento: la teoria della "governance sperimentale" – 4. La raccomandazione dell'UNESCO come esempio di "sperimentalismo transnazionale" – 5. L'adozione della governance dell'EOSC come esempio di governance sperimentale – 6. L'ecosistema EOSC, un "sistema dei sistemi", la nuova governance dell'EOSC – 7. Il caso pratico: il Sistema delle biblioteche depositarie delle Nazioni Unite – 8. La trasmissione del patrimonio culturale all'interno del Sistema delle biblioteche depositarie delle Nazioni Unite – 9. La trasmissione del patrimonio della Società delle Nazioni (1919-1946) – 10. Una "conversazione aperta" in corso per una governance della scienza aperta*

1. Ecosistema Internet e sviluppo della scienza aperta a livello internazionale

In questo articolo analizzeremo come la trasmissione del patrimonio culturale ed intellettuale sia legata allo sviluppo della scienza aperta e alla diffusione delle buone pratiche di scienza aperta. Tratteremo di un caso pratico di condivisione culturale e di partecipazione attiva ad una "comunità online" in un momento in cui la rete (Internet) è stata il solo mezzo di comunicazione, sia a causa della distanza fisica fra gli interlocutori, sia a causa dell'isolamento generato dai lockdown presenti in varie parti del mondo durante la crisi pandemica Covid-19. Il caso pratico illustrato è quello dell'evoluzione *de facto* del Sistema delle biblioteche depositarie delle Nazioni Unite,

D. Grbac è bibliotecaria presso la Biblioteca d'Ateneo dell'Università Cattolica del Sacro Cuore di Milano e riferimento per la Biblioteca per il Programma delle Nazioni Unite delle biblioteche depositarie.

L'autrice ringrazia: le colleghe Danuta Urbanska e Angela Contessi e il collega Ivano Spadotto, la già responsabile del coordinamento esterno del *Depository Library Programme*, Ramona Khors e Armando Da Silva, bibliotecario *senior* e assistente del *Depository Library Programme* e la bibliotecaria Cristina Giordano presso la Biblioteca dell'UNOG (Ufficio delle Nazioni Unite di Ginevra). Le opinioni espresse sono quelle dell'autrice e non impegnano le Nazioni Unite.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

che, nel contesto sopra menzionato, diviene paradigmatico di una realtà in cui Internet è diventato il terreno di lavoro e di partecipazione e la cultura, almeno quella che può essere scambiata tramite la rete, il "bene comune" per il reciproco arricchimento e la trasmissione dell'eredità culturale ai posteri.

Nel 2020, Internet, inteso come un mezzo "vocazionalmente partecipativo"[1], è diventato il canale principe di comunicazione e di partecipazione, utilizzato ad esempio in ambiti internazionali, per gestire la fase di consultazione precedente la presa di decisioni all'interno di organizzazioni internazionali, rappresentative di una molteplicità di stakeholder[2], o portatori di interessi, sempre più presenti ed attivi nei forum di discussione, proprio grazie ad Internet.

Internet dunque "veicolo di partecipazione culturale o politica", per l'affermazione della scienza aperta e delle pratiche di scienza aperta, attraverso la condivisione culturale e la trasmissione dell'eredità culturale, e la partecipazione politica attiva nel quadro internazionale, sia mondiale che europeo, alla ricerca di modi e regole di gestione di Internet.

A testimonianza di ciò, tratteremo sia della Internet governance dal punto di vista dello sviluppo della scienza aperta a livello internazionale (la "transnazionalità"[3] di Internet), sia del movimento di partecipazione attiva alla costituzione della scienza aperta attraverso le attività di singoli, istituzioni e privati, impegnati nelle attività di condivisione culturale.

La richiesta di maggiore scienza aperta non proviene più solo dalle istituzioni, enti o agenzie delle Nazioni Unite. Ma è espressione di una vera e propria «partecipazione politica globale, legata ad un'azione politica di tipo transnazionale in ordine a problematiche di interesse mondiale»[4]. Essa avviene dunque anche per mezzo della partecipazione "tecnica" attiva degli esperti o dei cosiddetti "pari", consultati in merito alla creazione di un quadro di azione indirizzato agli stessi Stati membri.

Sullo sfondo la dibattuta ricerca a livello internazionale di una regolamentazione comune per la governance di Internet[5], a partire dalla sua definizione, come da articolo 34 della *Tunis Agenda for Information Society*, ovvero «the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet»[6].

In merito alle diverse applicazioni dell'Internet governance da parte dei diversi attori implicati si è scelto di trattare, a livello teorico, dei processi di adozione di una definizione della scienza aperta a livello mondiale ed europeo e, a livello pratico, di biblioteche, in particolare del Sistema delle biblioteche depositarie delle Nazioni Unite. Un esempio di trasmissione dell'eredità culturale ed intellettuale con particolare riguardo agli aspetti open nell'accesso, non solo a ciò che è di dominio pubblico e quindi "aperto" per natura, ma anche a ciò che è protetto dalla proprietà intellettuale, trasmesso e mediato, nel rispetto dei diritti della proprietà intellettuale, attraverso l'attività di servizio svolta dalle biblioteche.

2. Come si è arrivati a definire la scienza aperta a livello europeo e mondiale

In Europa la scienza aperta è promossa attraverso la *European Research Area* (Spazio Europeo della Ricerca). Lo Spazio è stato costituto nel 2000 ai fini della promozione della ricerca ed innovazione e per incoraggiare la libera circolazione dei ricercatori e della conoscenza. Nel 2018, lo Spazio Europeo della Ricerca è stato rilanciato aggiungendo l'obiettivo di promuovere le pratiche della scienza aperta. Al primo posto fra le venti azioni concrete per la realizzazione delle priorità dell'Agenda politica dello Spazio europeo (Conclusioni del Consiglio sullo Spazio Europeo della Ricerca del 2021), si trova l'azione volta a rendere possibile la cienza aperta anche attraverso l'EOSC, o la *European Open Science Cloud*[7].

L'EOSC dovrebbe costituire «a virtual commons where science producers and science consumers come together for more insights, new ideas and more innovation ... by federating data and services»[8]. Rappresentando il "contributo europeo" alla costituzione del *commons*, o bene pubblico scientifico globale, da intendersi come quel bene che consenta la pubblicazione, la cura e il riuso dei dati[9]. Con l'intento finale di creare «un ambiente virtuale con servizi fruibili gratuitamente, aperti e senza soluzione di continuità per l'archiviazione, la gestione, l'analisi e il riutilizzo dei dati della ricerca, a livello trasversale tra paesi e discipline scientifiche. Il suo sviluppo sarà nelle mani della comunità scientifica, composta dagli utenti più avanzati e dai principali protagonisti nel campo scientifico»[10], ovvero lo spazio della libera circolazione dei dati aperti oltre i confini nazionali e le aree disciplinari. Una sorta di quinta libertà di circolazione, dopo quella delle merci, delle persone, dei servizi e dei capitali.

A livello mondiale, nel novembre 2021, durante la 41ª sessione della Conferenza Generale dell'UNESCO, gli Stati membri hanno adottato la raccomandazione UNESCO sulla scienza aperta. La raccomandazione fornisce una definizione condivisa di valori e principi per la scienza aperta e una serie di misure concrete su come realizzare la scienza

aperta e avvicinare i cittadini alla scienza, facilitando la produzione e la diffusione della conoscenza scientifica nel mondo[11].

L'adozione della raccomandazione rappresenta, nelle parole di Ana Peršić, che ha supervisionato il coordinamento dello sviluppo della raccomandazione UNESCO, il primo strumento normativo e la prima definizione culturalmente concordata, a livello internazionale, di valori, principi e standard della scienza aperta. Una definizione che dovrebbe portare ad una governance condivisa, in quanto era giunto il momento per l'adozione di una politica internazionale e di un insieme comune di azioni, in un contesto mondiale, o rappresentativo delle differenze disciplinari e regionali e da intendersi come contributo all'eliminazione degli esistenti divari digitali, tecnologici e di accesso alla conoscenza[12].

Per entrambi i processi, ovvero la creazione dell'EOSC e la redazione della raccomandazione dell'UNESCO, come vedremo nel dettaglio più avanti, essenziale è stata la partecipazione attiva dei portatori di interesse. Nel caso dell'EOSC, a garanzia di un approccio che attingesse alla "fonte" della community dei portatori di interesse. Per il periodo 2019-2020, il Segretariato dell'EOSC, il primo organo di governance dell'EOSC, ha potuto contare sul supporto di sei gruppi di lavoro. Si è trattato di gruppi di lavoro che hanno fornito l'apporto delle migliori competenze provenienti dalla "comunità di esperti", per mezzo della redazione di relazioni tematiche sintetiche sulle questioni di interesse che necessitavano di una presa di decisione da parte degli organi deliberanti[13].

Nel caso dell'UNESCO, l'esercizio di ricerca di un quadro internazionale di una governance della scienza aperta, culturalmente condiviso e globalmente rappresentativo ha visto il ricorso a diversi meccanismi di consultazione ai quali hanno partecipato diversi portatori di interesse, sia a livello regionale che a livello di rappresentanti delle comunità scientifiche, delle associazioni per la promozione della scienza aperta, di tecnici, e anche biblioteche consultate come esperti nella materia.

Di fatto, in entrambi i casi i processi seguiti nella pratica mostrano molte somiglianze con la teoria della governance sperimentale.

3. Un possibile quadro teorico di riferimento: la teoria della "governance sperimentale"

La governance sperimentale è una teoria studiata tra il 2008 e il 2015 che ha voluto spiegare come la governance possa funzionare in condizioni di incertezza, grazie al ricorso a nuovi modi nell'adozione delle decisioni politiche, in particolare per mezzo del coinvolgimento di nuovi attori. La teoria formulata da Jonathan Zeiltin mirava a dimostrare che, al fine di affrontare questioni di interesse comune ad una pluralità di attori, si dovesse seguire una procedura. La procedura consisteva in diverse fasi. Una prima fase di raccolta di opinioni a diversi livelli, non solo coinvolgendo gli attori istituzionali, come i politici, ma anche coloro che sono più vicini alla questione. Una fase di aggregazione del consenso sulla decisione, tramite accordo, ed infine l'adozione della decisione[14].

La governance sperimentale si presenta come una sorta di governance "dal basso", che raccoglie una pluralità di interessi, perché allargata ad un insieme più ampio di attori, non solo politici, ma anche provenienti dalle professioni (settore privato), o rappresentanti di interessi locali e della società civile. Gli attori non politici vengono chiamati dall'autore anche "pari", ovvero coloro che sono più vicini alla questione e, in base a questo loro posizionamento, maggiormente capaci di trovare una soluzione[15].

Secondo l'autore, la governance sperimentale può anche essere definita come "poliarchia direttamente deliberativa"[16], si tratterebbe di un metodo deliberativo che coinvolge una pluralità di portatori di interesse, applicabile ad una vasta gamma di politiche, a condizione che sia possibile, dopo una prima definizione degli obiettivi, prevedere una loro revisione sulla base del confronto con approcci alternativi[17]. Utilizzando i termini degli autori, si tratta di una pratica di "esplorazione congiunta" per trovare soluzioni e proporre azioni sostenute dalla "pressione dei pari", in grado di garantire allo stesso tempo la soluzione del problema e una sorta di meccanismo indiretto di "accountability", o di responsabilità[18]. Poiché la deliberazione è fondata sull'esperienza appresa dagli altri pari, è l'apprendimento, una volta "interiorizzato", che rende la responsabilità ("accountability") diretta e dinamica.

Gli attori imparano dalle esperienze degli altri partecipanti e applicano localmente ciò che hanno imparato; di fatto superando l'antica divisione tra attori pubblici e privati, essi operano in condizioni di incertezza e creano dei possibili "collegamenti" fra problemi urgenti e risposte efficaci, in una "nuova forma" di responsabilità democratica[19].

Le ricerche sulla teoria della governance sperimentale si sono estese nel tempo al contesto transnazionale, se impegnato nella ricerca di una qualche forma di regolamentazione. In merito, gli autori hanno trovato interessanti percorsi nella direzione dello sperimentalismo transnazionale, nella creazione *ex novo*, all'interno del sistema delle Nazioni Unite, di mec-

canismi multilaterali di apprendimento sperimentale nella negoziazione di accordi internazionali. Anche se gli autori erano ancora cauti, a causa dei rari esempi pratici riscontrati nella realtà, dovuti ai tipici problemi di adozione di "azioni collettive", come la difficoltà di trovare un accordo iniziale su di un quadro comune di obiettivi, spesso ostacolato dal dissenso di alcuni attori, con la conseguente mancanza, il più delle volte, della previsione di procedure di monitoraggio e di apprendimento dall'esperienza altrui[20].

Le cose sembrano invece essere cambiate dieci anni dopo se si analizza il processo di adozione della raccomandazione UNESCO sulla scienza aperta, un primo quadro comune e concordato sull'argomento. Anche grazie alle nuove tecnologie che hanno permesso una partecipazione più facile e attiva al processo di adozione.

4. La raccomandazione dell'UNESCO come esempio di "sperimentalismo transnazionale"

Analizzeremo di seguito come i quattro elementi che costituiscono la governance sperimentale siano presenti nel processo di elaborazione della raccomandazione dell'UNESCO, ovvero: la definizione di un quadro più ampio di obiettivi, la discrezionalità concessa ai livelli inferiori nell'attuazione degli obiettivi, la pratica di relazioni e valutazioni regolari ed infine la revisione periodica degli obiettivi fissati nel quadro[21].

Il processo di elaborazione della raccomandazione è iniziato nel 2019, quando la 40ª Conferenza Generale dell'UNESCO ha dato all'Organizzazione il compito di sviluppare uno standard internazionale strumentale per la scienza aperta sotto forma di raccomandazione. Sono seguite tre fasi: la consultazione globale, la revisione tra "pari", con la contestuale stesura del testo della raccomandazione durante gli incontri intergovernativi e un'ulteriore consultazione sul testo della raccomandazione prima della sua adozione finale da parte della Conferenza Generale dell'UNESCO.

Durante la fase di consultazione, svoltasi tra dicembre 2019 e maggio 2020, è stata istituito il "Partenariato per la Scienza aperta" (sotto forma di un sondaggio condiviso a livello globale) ed è stato creato il "Comitato consultivo della scienza aperta". Secondo Shamila Nair-Bedouelle, il Partenariato è stato strumentale nella mobilitazione di una "comunità di pratiche" mondiale per la scienza aperta e ha fornito suggerimenti tecnici e di contenuto nella redazione della raccomandazione, in quanto i partecipanti rappresentavano vari movimenti e pratiche in diverse discipline ed aspetti delle attività accademiche[22].

Il "Partenariato per la Scienza aperta" era costituito da una pluralità di portatori di interesse: rappresentanti degli Stati membri, dell'intera comunità scientifica, delle principali istituzioni ed enti scientifici internazionali e nazionali, delle agenzie pertinenti delle Nazioni Unite, dei cittadini e dei detentori di conoscenze tradizionali (cultura indigena)[23]. Il Partenariato ha operato sotto la guida del "Comitato consultivo della scienza aperta", composto sia da rappresentanti selezionati degli Stati membri, che da rappresentanti selezionati di istituzioni scientifiche chiave che si occupano di scienza aperta. Il compito del Comitato è stato quello di dirigere le consultazioni fornendo consigli avveduti e strategici[24].

Due tipologie di consultazioni sono seguite, tenutesi sia in presenza che online. Le consultazioni regionali, svoltesi in tre cicli: a dicembre 2019, tra luglio e settembre 2020 e a dicembre 2020. Le consultazioni tematiche e delle parti interessate, svoltesi anch'esse in tre cicli: in una prima fase tra febbraio e maggio 2020, la seconda a gennaio 2021, una terza tenutasi online il 23 aprile 2021. Quest'ultima è stata una riunione di esperti che ha riunito promotori della scienza aperta ed esperti di diritti della proprietà intellettuale.

La fase di redazione della raccomandazione si è svolta durante la consultazione elettronica online sui contenuti della raccomandazione stessa. Dal 6 al 7 e dal 10 al 12 maggio 2021, la revisione dei "pari" si è tenuta sotto forma di riunioni speciali intergovernative che hanno negoziato e concordato la bozza finale del testo poi adottato dalla 41ª Conferenza Generale nel novembre 2022. A questa consultazione hanno partecipato rappresentanti di 100 paesi e 65 osservatori (una "esplorazione congiunta", nei termini della governance sperimentale). Secondo Peršić, la riunione intergovernativa si è svolta online con «conversazioni molto interessanti» (approccio "direttamente deliberativo"). Il risultato è stato l'accordo sulla necessità di fare qualcosa e per ogni Paese di farsi avanti (discrezione nell'attuazione) colmando il divario nella conoscenza[25].

Infine, da maggio a dicembre 2021, tutta la pluralità dei portatori d'interesse (Stati membri, promotori della scienza aperta e altri attori ed enti impegnati attivamente nella scienza aperta) ha potuto inviare commenti sulla prima bozza della raccomandazione.

L'aspetto "sociale" è un elemento importante del modo di funzionamento della governance sperimentale; nel processo sopra esposto diversi portatori di interesse sono stati coinvolti sia nella consultazione globale, che ha avuto luogo con un sondaggio, sia

nelle diverse consultazioni con molteplici portatori di interesse tematici (rappresentanti legali e tecnici), come anche durante il processo di redazione della raccomandazione e nell'ulteriore discussione sui suoi contenuti. I portatori di interesse erano rappresentativi di diverse aree del mondo e di diverse comunità epistemiche, nessuna esclusa, anche la cultura indigena era presente nel Partenariato globale per la Scienza aperta, poiché questo avrebbe dovuto "catturare veramente" che cosa le diverse comunità epistemiche necessitano ed intendono per scienza aperta[26].

La fase di stesura della raccomandazione ha portato a proporre un insieme di azioni favorevoli ad una corretta ed equa operatività della scienza aperta a livello individuale, istituzionale, nazionale, regionale ed internazionale[27]. Tra le aree di azione troviamo anche lo sviluppo di un ambiente politico per la scienza aperta e la promozione della cooperazione internazionale e fra portatori di interesse per la riduzione dei divari tecnologici e nella trasmissione della conoscenza[28], in altre parole un quadro politico di governance transnazionale.

In termini di governance sperimentale, il "Partenariato per la Scienza aperta" ha rappresentato anche la fase di "pressione da parte dei pari", in quanto la comunità di riferimento presente all'interno del Partenariato era composta da "pari", ovvero associazioni di università e di biblioteche, associazioni di enti di ricerca e di editori di pubblicazioni universitarie, organizzazioni di promozione dell'accesso aperto e dei dati aperti. Ma anche da individui "vicini" alla questione come: giovani scienziati e ricercatori, comunità indigene, rappresentanti della *Citizen science*. Si è trattato di organizzazioni, enti ed individui già attivi nelle attività di scienza aperta e in grado di dare l'esempio e fornire la competenza necessaria su come promuovere la scienza aperta.

L'attuazione della raccomandazione potrebbe, sotto questo aspetto e in base alla teoria della governance sperimentale, presentarsi come una "rete di apprendimento" e un'occasione di "apprendimento tra reti". Fra i pilastri chiave della raccomandazione, come riporta Nair-Bedouelle, ci dovrebbe essere anche l'impegno da parte degli attori della società civile, dei cittadini e della scienza partecipativa e la collaborazioni fra scienziati ed attori della società civile che possa andare oltre la comunità di ricerca scientifica, al fine di rendere il processo scientifico più inclusivo ed accessibile ad una fetta maggiore della società, così come ci dovrebbe essere un maggiore dialogo aperto fra sistemi di conoscenza e il riconoscimento della complementarietà fra diversi sistemi di conoscenza[29], o in termini di governance sperimentale: un apprendimento tra reti.

Gli Stati membri che hanno adottato la raccomandazione hanno anche concordato una tabella di marcia comune e si sono impegnati a riferire ogni quattro anni sui loro progressi. Anche questo è un passo fondamentale previsto dall'approccio della governance sperimentale. Infine, si sono impegnati a privilegiare sette aree di attuazione della raccomandazione[30].

Ciò che per ora non è previsto nella raccomandazione, e che invece è una fase necessaria nella teoria della governance sperimentale, è la fissazione di una regolare revisione del quadro. L'unica menzione è presente nel paragrafo V della raccomandazione, intitolato "Monitoraggio", dove si dice che gli Stati membri dovrebbero (*should*) monitorare le politiche e i meccanismi relativi alla scienza aperta[31].

Infatti, a conclusione della sua presentazione, Peršić ha posto la questione del monitoraggio tra le sfide in vista della concreta attuazione della raccomandazione, affermando che il monitoraggio della scienza aperta dovrebbe misurare non solo i progressi nella scienza aperta, ma anche come questa influisca sulla produzione scientifica e sulla società[32].

5. L'adozione della governance dell'EOSC come esempio di governance sperimentale

L'organizzazione della governance all'interno degli organi dell'Unione europea è stato oggetto di studio da parte della teoria della governance sperimentale. In particolare, la teoria si è soffermata sulle modalità di organizzazione dell'attività della Commissione europea, con particolare riguardo alla "Comitologia", e ha studiato gli effetti dell'introduzione del "Metodo aperto di coordinamento" nell'attività del Consiglio dell'Unione europea in seguito all'adozione del Trattato di Lisbona[33].

Non stupisce dunque il fatto che la prima definizione dell'EOSC, risalente al 2016, sia il frutto dell'opera di una Commissione di esperti, riunitasi insieme ai portatori di interesse e ai finanziatori della ricerca, nel corso del 2015. Il gruppo di esperti era composto da rappresentanti di dieci paesi europei, Giappone e Australia. Nel documento prodotto si leggeva che l'obiettivo dell'EOSC era quello di accelerare e sostenere la transazione in corso verso una più efficace scienza aperta, l'innovazione aperta e un mercato unico digitale[34].

Durante il vertice EOSC del giugno 2017, i portatori di interesse del settore della ricerca hanno approvato la prima versione della "Dichiarazione EOSC" oggetto di adozione nell'ottobre 2017, tale dichiarazione, varata ufficialmente a Vienna nel

novembre 2018, definisce i principi guida per l'attuazione dell'EOSC[35].

A questa prima fase deliberativa avvenuta dopo consultazione, sono seguite ulteriori consultazioni da parte della Commissione, al fine di definire la futura struttura di governance dell'EOSC, a partire dalle pratiche di governance in corso presso le esistenti reti scientifiche di grande scala (ovvero i "pari" secondo la teoria della governance sperimentale).

Le consultazioni evidenziarono la necessità di forti linee guida, di un chiaro quadro di governance, multilivello, come anche del coinvolgimento di una molteplicità di portatori di interesse, con chiari ruoli di tipo istituzionale, esecutivo e di consultazione, in grado di rappresentare sia la comunità scientifica, che conferirle autonomia di azione[36].

Come accade anche per altri programmi europei in ambiti simili[37], anche l'EOSC si sta realizzando grazie all'azione di alcuni consorzi co-finanziati dal Programma quadro per la ricerca e l'innovazione tecnologica. Sono dunque i consorzi co-finanziati da Horizon 2020 prima e da Horizon Europe ora che stanno creando l'infrastruttura a sostegno dell'EOSC, dettandone anche le regole di governance[38].

Tali consorzi sono reti di partenariati fra infrastrutture di ricerca (o "reti di apprendimento" secondo la teoria della governance sperimentale) che garantiscono il coinvolgimento di tecnici e allo stesso tempo la consultazione di esperti.

I primi organi di governance dell'EOSC erano costituiti da: Consiglio di amministrazione, formato da rappresentanti degli Stati membri e Paesi associati, presieduto da rappresentanti della Commissione. Il Consiglio direttivo, 11 membri scelti in seguito ad un appello a candidature, il *Forum* dei portatori di interesse, ovvero la riunione di rappresentanti dei progetti in materia di sviluppo delle infrastrutture di ricerca sia europei che nazionali, i fornitori di servizi, il settore pubblico, le piccole e medie imprese, l'industria. I rappresentanti dei portatori di interesse dell'EOSC sono stati a loro volta riuniti in sei gruppi di lavoro tematici creati per coordinare i progressi nell'attuazione delle priorità scelte[39].

6. L'ecosistema EOSC, un "sistema dei sistemi", la nuova governance dell'EOSC

Come abbiamo già accennato, l'EOSC è inclusa nella prima azione prioritaria del piano di realizzazione dello Spazio Europeo della Ricerca, per il periodo 2022-2024. Lo sviluppo dell'EOSC in questo periodo contribuirà alla costituzione di un mercato della conoscenza funzionante, dove la conoscenza circolerà liberamente in quanto oggetto di condivisione e di riuso dei prodotti della ricerca. Perché questo scambio di conoscenza sia possibile è stata costituita per l'appunto l'EOSC, ovvero un ambiente "federale", accessibile, fidato ed aperto nella distribuzione, multidisciplinare nei contenuti, dove i ricercatori, coloro che si occupano di innovazione, le imprese ed i cittadini possano, a seconda delle esigenze specifiche: pubblicare, e/o trovare e soprattutto riutilizzare dati e strumenti per fare ricerca, innovazione ed istruzione, come anche i servizi connessi (il "mercato" dell'EOSC). Si tratta di servizi di analisi, di visualizzazione dei dati, di archiviazione e di conservazione di lungo periodo dei dati, e di servizi di monitoraggio dell'avanzamento nelle pratiche della scienza aperta.

I risultati attesi sono: l'affermazione del principio della scienza aperta e l'identificazione delle migliori pratiche di scienza aperta, la fornitura dei servizi e delle componenti centrali dell'EOSC (il "nucleo centrale sostenibile" per iniziare), il dialogo fra le esistenti infrastrutture europee di gestione dei dati della ricerca, favorendo in particolare l'interoperabilità dei dati. Lo stabilirsi di un meccanismo di monitoraggio per raccogliere dati e modelli di investimenti, politiche, prodotti della ricerca digitali, competenze nella scienza aperta e capacità infrastrutturali relativi all'EOSC. Ovvero, riprendendo una definizione che fu data dal primo gruppo di esperti consultato in merito, l'EOSC come "Internet dei dati e dei servizi"[40].

La realizzazione pratica dell'EOSC sta avvenendo in base alla SRIA – *Strategic Research and Innovation Agenda*, sviluppata in collaborazione con l'intera comunità EOSC, consultata al fine di guidare il processo verso gli obiettivi comuni definiti a più livelli: europeo, nazionale ed istituzionale. La SRIA è il frutto del lavoro del primo organo di governance dell'EOSC: il Segretariato.

L'attività del Segretariato si è svolta fra il 2019 e il 2021. Nella sua attività di governance *ad interim* il Segretariato ha sostenuto il Consiglio direttivo dell'EOSC e i gruppi di lavoro per preparare la strada per l'attuazione pratica dell'EOSC. La SRIA ne raccoglie i risultati, ad essa si aggiungono venti relazioni tematiche contenenti raccomandazioni[41].

L'Associazione EOSC è l'organo che sostituisce il Segretariato nella nuova governance EOSC. Si tratta di un ente legale demandato a governare l'EOSC. Costituita il 29 luglio 2020, essa riunisce rappresentanti dei Paesi membri ed associati che partecipano all'EOSC ed ha come compito di aiutare a coordinare e direzionare gli investimenti attraverso le task force e altri strumenti di governance[42].

La struttura "federata" dell'EOSC risulterà dalla riunione delle esistenti infrastrutture di ricer-

ca "aumentate" dai nuovi servizi dedicati alla condivisione di pubblicazioni, dati, software, a beneficio delle comunità di ricerca. Le singole infrastrutture rimangono le sole responsabili della loro amministrazione.

Il nuovo modello di governance, concordato dai Paesi membri dell'Unione europea, a completamento dell'attuazione dell'EOSC e da realizzarsi nel periodo 2021-2027, è un modello tripartito a cui partecipano: la Commissione europea in rappresentanza dell'Unione europea, l'Associazione EOSC in rappresentanza della community di ricercatori europei, il Comitato direttivo dell'ESOC costituito dai rappresentanti dei Paesi membri e Paesi associati all'Unione europea che hanno accesso al programma di finanziamento alla ricerca e lo sviluppo tecnologico.

Eventuali organizzazioni in rappresentanza della comunità dei ricercatori e delle infrastrutture di ricerca interessate a partecipare possono unirsi all'Associazione EOSC[43]. In alternativa possono partecipare ai momenti di consultazione aperti agli interessati e a coloro che appartengono alla community dei ricercatori europei. Diversi di questi eventi sono stati organizzati dai vari consorzi che sono riusciti ad ottenere un finanziamento dalla Commissione europea[44].

Tale modello di governance, che per la fase di consultazione ha attinto dal basso dalle competenze degli esperti e che nella fase di attuazione propone la partecipazione attraverso l'Associazione EOSC, è simile nella sua dinamica a quello proposto agli Stati membri nella raccomandazione dell'UNESCO sulla scienza aperta. Altrettanto simile è anche il fatto che i Paesi membri dell'Unione europea, la Commissione europea e l'Associazione EOSC si siano impegnati ad aggiungere un meccanismo di monitoraggio continuo per raccogliere dati e contributi paradigmatici relativi all'EOSC, ma non abbiano ancora previsto una possibile modifica del quadro, questo almeno fino alla fine del periodo 2022-2024.

7. Il caso pratico: il Sistema delle biblioteche depositarie delle Nazioni Unite

Fra i tecnici consultati durante il processo di adozione della raccomandazione dell'UNESCO sulla scienza aperta troviamo la Biblioteca Dag Hammarskjöld del Sistema delle biblioteche depositarie delle Nazioni Unite. Essa ha partecipato, con la sua azione a quell'ecosistema globale composto da associazioni di università e biblioteche e da tutti gli attori rilevanti nella scienza aperta, che hanno costituito il "Partenariato per la Scienza aperta"[45].

La biblioteca è stata riconosciuta come uno dei "pari" chiamati ad esprimersi in merito alla scienza aperta, anche grazie all'azione svolta negli ultimi anni al fine del passaggio all'interno del Sistema delle biblioteche depositarie delle Nazioni Unite dal deposito di pubblicazioni e documenti "prevalentemente" sotto forma cartacea, a quello elettronico, e dal deposito di pubblicazioni sottoscritte a quello ad accesso aperto.

Il Sistema delle biblioteche depositarie delle Nazioni Unite fa parte del Sistema delle Nazioni Unite, insieme agli organi, fondi e programmi, le agenzie specializzate e tutte le organizzazioni correlate. Costituito nel 1947, è stato sottoposto a una prima riforma nel 1974, seguita da una seconda nel 2015. Attualmente è costituito da 350 biblioteche sparse in tutto il mondo in 133 Paesi e un territorio. Le biblioteche locali partecipanti al Sistema ricevevano nel passato (fino al 2012) documenti e pubblicazioni prodotti dalle Nazioni Unite in formato cartaceo. Le Biblioteche di New York (chiamata Dag Hammarskjöld Library[46]) e quella di Ginevra presso l'UNOG (Ufficio delle Nazioni Unite a Ginevra[47]), entrambe parte del Sistema, sono state attive non solo nella conservazione di pubblicazioni e documenti, ma anche nella loro diffusione presso le altre biblioteche depositarie[48].

Il materiale prodotto dalle Nazioni Unite è in capo sia al diritto d'autore delle Nazioni Unite (si tratta di opere di dominio pubblico, nel caso di documenti ufficiali, o ad accesso aperto, nel caso di alcune pubblicazioni), sia al diritto d'autore dei singoli autori (si tratta, in questo caso, delle pubblicazioni per la vendita, o pubblicazioni non accessibili tramite accesso aperto).

La transizione all'accesso aperto del deposito ha cambiato il modo in cui le biblioteche depositarie delle Nazioni Unite stanno lavorando per servire le comunità locali nell'accesso ai documenti e alle pubblicazioni delle Nazioni Unite. I bibliotecari delle biblioteche di deposito, che hanno passato anni a tenere in ordine e catalogare le loro collezioni su carta, sono ora chiamati a migliorare le loro competenze dando agli utenti nuovi modi per accedere a documenti e pubblicazioni.

Il lavoro quotidiano di uno staff competente e dedicato di bibliotecari svolge di fatto una funzione di "promozione" per conto delle Nazioni Unite a livello locale, ed ha costituito nel tempo una "base di conoscenza" fatta di archivi, cataloghi di biblioteca, collezioni speciali di biblioteca. Un patrimonio culturale raccolto e acquisito in ben settantacinque anni di attività ed esperienza nella gestione dei materiali delle Nazioni Unite, che ora "comunica" con la versione

online offerta dalla *United Nations Digital Library*[49] e con i prossimamente disponibili (nel corso del 2022) Archivi online della Società delle Nazioni[50].

Durante la crisi della pandemia di Covid nel 2020, il sistema si è evoluto di fatto in una "comunità aperta", che ha fatto perno sulle attività e i servizi della Biblioteca Dag Hammarskjöld offerti online al Sistema e non solo. In particolare, la fruizione dei servizi online è stata organizzata attorno allo strumento della *United Nations Digital Library*[51].

All'interno della comunità delle biblioteche di deposito è stato possibile condividere informazioni (aggiornamenti sui progetti di digitalizzazione, materiali promozionali, guide alla ricerca, dati bibliografici), riutilizzabili dietro la semplice citazione della fonte, documenti ufficiali e periodici accessibili gratuitamente online, iniziative di *Open education*, come la formazione gratuita su come utilizzare gli strumenti digitali delle Nazioni Unite, le banche dati elettroniche e il catalogo della biblioteca, *webinar* e conferenze su argomenti come disinformazione, *infodemics*, biblioteche verdi, archivi di dati certificati, funzionamento dei motori di ricerca su Internet.

Allo stesso tempo, man mano che i progetti di digitalizzazione sono in via di conclusione, da una "base di conoscenza" il Sistema stesso si sta trasformando in una "rete di conoscenza", o una "rete di apprendimento" nei termini della teoria della governance sperimentale. All'interno della quale un patrimonio culturale digitale, organizzato per rendere i contenuti accessibili, sta trasformando il lavoro dei bibliotecari in promotori del loro comune patrimonio culturale e intellettuale, rendendoli attori attivi nella promozione di pratiche di scienza aperta in tutto il mondo.

8. La trasmissione del patrimonio culturale all'interno del Sistema delle biblioteche depositarie delle Nazioni Unite

I progetti di digitalizzazione sia presso la biblioteca di New York che quella di Ginevra sono stati portati avanti fin dagli anni Novanta, ma oggi ne possiamo apprezzare i risultati in termini di un enorme numero di documenti digitalizzati e messi a disposizione gratuitamente via Internet. Si tratta di documenti ufficiali e pubblicazioni ad accesso aperto. Il materiale consiste principalmente in documenti di lavoro prodotti per il funzionamento dell'organizzazione, ma anche di relazioni periodiche prodotte da vari organi, commissioni ed agenzie del Sistema delle Nazioni Unite. Risale al 1992 il primo progetto di digitalizzazione che ha creato il database *United Nations Official Documents System* (ODS)[52]. All'inizio si trattava di un prototipo che offriva accesso online solo ai documenti "nati digitali", ovvero pubblicati dopo il 1993. Nel 1998, la Biblioteca Dag Hammarskjöld, incaricata dall'Assemblea Generale a procedere con alcuni progetti di digitalizzazione, ha completato il database ODS attraverso la scansione di documenti ufficiali pubblicati prima del 1993. Seguì, nel 2007, la creazione di un nuovo database la *United Nations Treaty Series Collection*. Si trattava di una prima raccolta di testi di documenti costituiti da accordi internazionali firmati tra Stati membri delle Nazioni Unite e depositati presso il Segretariato delle Nazioni Unite[53].

Nel 2014, un enorme programma di digitalizzazione è stato possibile grazie allo sforzo congiunto del Dipartimento di Informazione Pubblica e del Dipartimento per l'Assemblea Generale. Il progetto si è svolto sotto la guida della Biblioteca di New York e di quella di Ginevra. Il programma consisteva in due sezioni diverse, la digitalizzazione *ad hoc*, fatta su singoli documenti scelti prodotti dagli organi delle Nazioni Unite o su documenti emessi su argomenti specifici, e un programma di scansione regolare. La digitalizzazione *ad hoc* è stata effettuata solo nella lingua richiesta dal programma di digitalizzazione, mentre il programma di scansione regolare è stato garantito in tutte e sei le lingue ufficiali, se disponibili[54].

Come risultato di questo sforzo congiunto, nel maggio 2017 è stata lanciata la *United Nations Digital Library*. Il nuovo strumento ha sostituito i precedenti, perché più completo e curato dalla Biblioteca Dag Hammarskjöld. Nella *Digital Library* i metadati sono disponibili solo in inglese, ma l'accesso ai testi online è offerto in tutte le lingue ufficiali disponibili. I progetti di digitalizzazione sono ancora in corso, e i loro risultati sono ora direttamente disponibili attraverso la *Digital Library*[55].

La differenza principale tra la *Digital Library* e i precedenti database è che nella *Digital Library* non c'è solo il patrimonio culturale o tutti i documenti ufficiali a disposizione sia nati digitali o digitalizzati, ma anche il patrimonio di proprietà intellettuale, ovvero i documenti emessi da diversi organismi o istituzioni delle Nazioni Unite, che offrono analisi e approfondimenti, e che ricadono sotto la proprietà intellettuale delle Nazioni Unite e sono quindi ad accesso aperto.

Questi documenti erano a disposizione gratuitamente del pubblico anche nel passato, in quanto pubblicazioni ricevute dalle biblioteche di deposito, ed erano accessibili dalle diverse pagine Web dedicate alle pubblicazioni presenti nei siti ufficiali di gran parte degli organi ed istituzioni del Sistema delle Nazioni Unite. La novità è che oggi i periodici ad accesso

aperto (sono escluse le pubblicazioni per la vendita)[56] confluiscono direttamente nella *Digital Library*.

9. La trasmissione del patrimonio della Società delle Nazioni (1919-1946)

Anche la Biblioteca di Ginevra è attiva nella digitalizzazione e nella trasmissione del proprio patrimonio. In particolare, la Biblioteca di Ginevra è anche responsabile e custode degli Archivi della Società delle Nazioni.

La Biblioteca e l'Archivio di Ginevra hanno lanciato nel 2017 il progetto LONTAD – *Total Digital Access to the League of Nations Archives*, per la conservazione fisica e digitale e l'accesso online dell'intero archivio della Società delle Nazioni. Alla fine del progetto di digitalizzazione sarà dato accesso aperto ai fondi e alle collezioni gestite dalla Biblioteca e dall'Archivio delle Nazioni Unite di Ginevra, compresi gli archivi delle Nazioni Unite a Ginevra, della Società delle Nazioni (1919-1946), dei movimenti internazionali per la pace (dal 1870), e delle carte donate da privati. Il progetto in corso dal 2018 si concluderà nel 2022. Alla fine del progetto, 15 milioni di pagine saranno digitalizzati. Tutti i documenti sono allo stesso tempo restaurati, se necessario, e condizionati per una duratura conservazione[57].

Gran parte dei documenti presenti nell'Archivio è costituita da corrispondenza (ricevuta dal Segretariato), statistiche (la Società delle Nazioni iniziò la pratica di raccogliere statistiche dagli Stati membri), documenti parlamentari (o documenti preparatori di documenti ufficiali contenenti le registrazioni di tutte le riunioni del Consiglio, dell'Assemblea e di tutte le Commissioni tecniche e altri organismi attivi a Ginevra), documenti ufficiali, varie relazioni scritte da tutte le diverse sezioni del Segretariato della Società delle Nazioni (verbali, carte di lavoro e documenti), ma anche mappe allegate a questi documenti. Oltre ai documenti dell'Organizzazione sono presenti documenti di privati cittadini, sotto forma di archivi personali o documenti di altre organizzazioni, come le petizioni inviate alla Società delle Nazioni[58].

10. Una "conversazione aperta" in corso per una governance della scienza aperta

La pandemia Covid ha introdotto nuove modalità di lavoro e soprattutto nuove opportunità di ricerca, questo vale non solo per le biblioteche, i ricercatori, ma anche per chiunque abbia a che fare con la trasmissione della conoscenza. La cooperazione scientifica che si è attivata per trovare soluzioni alla pandemia è stata un esempio concreto di scienza aperta; la sfida ora è quella di promuovere la scienza aperta in altri settori.

Per questo motivo, una "grande conversazione aperta" sulla scienza è necessaria per rendere la conoscenza scientifica un "servizio per l'umanità" e non perdere lo slancio che ha fatto sì che l'apertura nel processo scientifico raggiungesse risultati imprevisti[59].

Ma questo non basta, occorre anche l'esempio dei "pari" per far sì che il progresso della scienza aperta si sviluppi a livello mondiale. Le biblioteche all'interno del Sistema delle biblioteche depositarie hanno fatto scienza aperta fin dall'inizio del Programma, mettendo a disposizione delle comunità locali, quando le collezioni erano solo su carta, documenti ufficiali, documenti preparatori e periodici (sia pubblicazioni per la vendita che pubblicazioni libere delle Nazioni Unite) "gratuitamente" e "a orari ragionevoli"[60]. Grazie a tutti i progetti di digitalizzazione che sono stati fatti e sono ancora in corso, il materiale prodotto dalle Nazioni Unite, e prossimamente quello della Società delle Nazioni, è oggi a disposizione e accessibile online ancora una volta anche per mezzo del lavoro di mediazione e di servizio fornito dai bibliotecari, poiché «UN depository libraries are in a position to direct and advice researchers, policymakers, civil society groups, and the public on where to find UN information and data, and how to use numerous print and online resources, research tools, and database»[61].

Dal 2018, la Biblioteca Dag Hammarskjöld sta lavorando per diffondere la conoscenza e la discussione sull'accesso aperto, gli obiettivi di sviluppo sostenibile e la scienza aperta[62]. Nel 2019 durante la prima conferenza organizzata dalla biblioteca sul tema della scienza aperta un gruppo di esperti ha proposta la creazione del *Global Open Science commons*[63], ovvero di un "bene pubblico globale per la scienza aperta" e il raggiungimento degli Obiettivi di Sviluppo Sostenibile[64].

Ancora una volta è stato il Sistema delle biblioteche depositarie a proporre l'esempio e a sostenere nuove pratiche di scienza aperta, non resta che seguire e procedere in questo senso, come suggerito anche dalla raccomandazione UNESCO sulla scienza aperta e dal piano per la realizzazione dell'EOSC in Europa.

Note

[1] U. Allegretti, *Prefazione*, in F. Marcelli, P. Marsocci, M. Pietrangelo (a cura di), "La rete internet come spazio di

partecipazione politica. Una prospettiva giuridica", Editoriale Scientifica, 2015, pp. 7-10, citazione a p. 7.

[2]Per la traduzione in lingua italiana di stakeholder adottiamo qui quella di L. Abba, S. Trumpy, *La enhanced cooperation per le politiche pubbliche di gestione delle risorse critiche di Internet*, in "Informatica e diritto", 2009, n. 1, pp. 15-27, nota n. 2 a p. 15.

[3]U. Allegretti, *op. cit.*

[4]F. Marcelli, *Internet fra canale di partecipazione politica e strumento di controllo. Profili di diritto internazionale*, in F. Marcelli, P. Marsocci, M. Pietrangelo (a cura di), "op. cit.", pp. 11-37, citazione a p. 23.

[5]In merito si veda il contributo di T. Natoli, *Il ruolo delle organizzazioni internazionali nella gestione delle reti digitali globali*, in F. Marcelli, P. Marsocci, M. Pietrangelo (a cura di), "op. cit.", pp. 101-131.

[6]United Nations, ITU (International Telecommunication Union), *Tunis Agenda for the Information Society*, 18 November 2005. Per un approfondimento sul processo che ha portato all'adozione della sopra menzionata definizione si veda L. Abba, S. Trumpy, *op. cit.* e A. Nicotra, *L'Internet Governance in Italia*, in "Informatica e diritto", 2009, n. 1, pp. 63-72.

[7]Council of the European Union, *Future governance of the European Research Area (ERA)*, Brussels, 26 November 2021. Si veda anche European Commission, *European Research Area Policy Agenda – Overview of actions for the period 2022-2024*, Brussels, November 2021, in particolare p. 4-5.

[8]Executive Board of the European Open Science Cloud (EOSC), *Strategic Implementation Plan*, Brussels, 2019, citazione a p. 4.

[9]Commission High Level Expert Group on the European Open Science Cloud, *A Cloud on the 2020 Horizon. Realising the European Open Science Cloud: first report and recommendations*, 20 June 2016; si veda in particolare il glossario alla fine del documento per la definizione citata di "bene pubblico".

[10]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Iniziativa europea per il cloud computing - Costruire un'economia competitiva dei dati e della conoscenza in Europa*, COM(2016) 178, 19 aprile 2016, citazione riportata a p. 6.

[11]UNESCO, *UNESCO recommendation on Open Science*, 2021.

[12]A. Peršić, *International Policy Framework for Open Science*, intervento all'OAI12 online Geneva Workshop "Innovations in Scholarly Communications" (6-10 settembre 2021). Ana Peršić è la Responsabile in carica della sezione *Science Policy and Partnerships at the Division of Science Policy and Capacity Building* presso il quartier generale dell'UNESCO a Parigi. Gli interventi possono essere ascoltati sul sito del Workshop.

[13]Cfr. EOSC *Working Groups*.

[14]Per un'analisi della teoria della governance sperimentale e una sua critica, cfr. S. Eckert, T.A. Börzel, *Experimentalist governance: an introduction*, p. 371-377; T.A. Börzel, *Experimentalist governance in the EU: the emperor's new clothes?*, p. 378-384; A. Verdun, *Experimentalist governance in the European Union: a commentary*, p. 385-393, tutti in "Regulation & Governance", vol. 6, 2012, n. 3.

[15]C.F. Sabel, J. Zeiltin, *Experimentalism in the EU: common ground and persistent differences*, *ivi*, p. 410-426, spec. p. 410.

[16]Id. (eds.), *Experimentalist Governance in the European Union: Towards a New Architecture*, Oxford University Press, 2010, spec. p. 6.

[17]J.E. Fossum, *Reflections on experimentalist governance*, in "Regulation & Governance", vol. 6, 2012, n. 3, p. 394-400, spec. p. 394.

[18]C.F. Sabel, J. Zeiltin, *Experimentalism in the EU: common ground and persistent differences*, cit., p. 411.

[19]*Ivi*, p. 424.

[20]J. Zeiltin, *Extending experimentalist governance? The European Union and Translational regulation*, Oxford Scholarship Online, 2015. Le citazioni sono tratte dalla versione bozza del capitolo 1 *Introduction: Theoretical Framework and Research Agenda*, distribuito durante la "GR:EEN Second Annual Conference. Networked learning in transnational governance" (Warwick, 8-9 November 2012).

[21]C.F. Sabel, J. Zeiltin (eds.), *Experimentalist Governance in the European Union: Towards a new Architecture*, cit., p. 3.

[22]S. Nair-Bedouelle, *Keynote speech* tenuto alla *Second Open Science online Conference* "From Tackling the Pandemic to Addressing Climate Change" (21-23 luglio 2021), organizzata dalla Biblioteca Dag Hammarskjöld e dal DESA - *Department of Economics and Social Affairs*. Shamila Nair-Bedouelle è vicedirettrice generale per le Scienze naturali dell'UNESCO. Per approfondimenti consultare il sito della Conferenza.

[23]Cfr. UNESCO, *UNESCO Global Open Science Partnership*.

[24]Cfr. UNESCO, *Open Science Advisory Committee*.

[25]A. Peršić, *op. cit.*

[26]*Ibidem*.

[27]S. Nair-Bedouelle, *op. cit.*

[28]*Ibidem*.

[29]*Ibidem*.

[30]Le sette aree sono: promozione di una comprensione comune della scienza aperta e dei benefici ad essa connessi, i diversi percorsi verso la scienza aperta, lo sviluppo e l'attuazione di un ambiente abilitante di policy per la scienza aperta, gli investimenti in infrastrutture e servizi che contribuiscano alla scienza aperta, gli investimenti in formazione, educazione, alfabetizzazione digitale e creazione di capacità, per permettere a ricercatori e ad altri portatori di interesse di partecipare alla scienza aperta, rafforzare una cultura della scienza aperta e allineare gli incentivi per la scienza aperta, promuovendo la cooperazione internazionale e dei molteplici portatori di interesse nel contesto della scienza aperta, con l'obiettivo di ridurre i divari digitali, tecnologici e di conoscenza. Cfr. UNESCO, *UNESCO sets ambitious international standards for open science*, 25 November 2021.

[31]Cfr. Id., *UNESCO recommendation on Open Science*, cit., p. 34.

[32]A. Peršić, *op. cit.*

[33]K. Amstrong, I. Begg, J. Zeiltin, *JCMS Symposium: EU Governance After Lisbon*, in "Journal of Common Market Studies", vol. 46, 2008, n. 2, p. 413-426. C.F. Sabel, J. Zeiltin, *Learning from Difference: The New Architecture of Experimentalist Governance in the EU*, in "European Law Journal", vol. 14, 2008, n. 3, p. 271-327.

[34]Commission High Level Expert Group on the European Open Science Cloud, *op. cit.*, p. 3.

[35]*The Vienna Declaration on the European Open Science Cloud*, Vienna, 23 November 2018.

[36]Executive Board of the European Open Science Cloud (EOSC), *op. cit.*, p. 10-11.

[37]Vedi anche il *Programma Europa digitale*, in vigore per il periodo 2021-2027.

[38]European Commission, *European Research Area Policy Agenda*, cit., in particolare p. 4-5.

[39]Di seguito i sei gruppi di lavoro. "Paesaggio", mappatura delle esistenti infrastrutture di ricerca potenzialmente parte

della futura struttura federativa dell'EOSC. "FAIR" (Findable Accessible Interoperable and Reusable) per l'attuazione dei principi FAIR attraverso la definizione di corrispondenti potenziali servizi da offrire tramite EOSC. "Architettura", definizione del quadro tecnico per la realizzazione e il sostegno del futuro sistema federale EOSC. "Regole di partecipazione", per definire e regolamentare diritti ed obblighi derivanti dagli impegni assunti all'interno dell'EOSC. "Capacità e formazione", per definire strumenti di formazione per facilitare l'operatività degli utenti in EOSC. Ed infine "Sostenibilità", ovvero una serie di raccomandazioni volte a permettere la sostenibilità della federazione EOSC nel lungo periodo.

[40]Commission High Level Expert Group on the European Open Science Cloud, *op. cit.*

[41]Cfr. la pagina tematica *The EOSC Secretariat*.

[42]Cfr. la pagina tematica *Association*.

[43]Cfr. la pagina tematica *EOSC governance*.

[44]Per un quadro di tali attività per il periodo 2019-2020 si veda Executive Board of the European Open Science Cloud (EOSC), *op. cit.*

[45]L'altra agenzia delle Nazioni Unite che ha partecipato attivamente al Partenariato dell'UNESCO è stata la United Nations IATT (*Inter-Agency Task Team on science technology and innovation for SDG*), che sostiene la realizzazione degli SDG (*Sustainable Development Goals*) attraverso la collaborazione di molteplici portatori di interesse e il partenariato con la società civile, il settore privato e la comunità scientifica.

[46]Cfr. il sito della Biblioteca.

[47]Cfr. il sito della Biblioteca.

[48]Cfr. il Programma delle biblioteche depositarie.

[49]Introdotta nel 2017, la *Digital Library* è un catalogo online dei documenti ufficiali delle Nazioni Unite e delle pubblicazioni ad accesso aperto con testi disponibili (digitalizzati o nati digitali). La *United Nations Digital Library* nasce dalla collaborazione tra le istituzioni delle Nazioni Unite, in particolare le biblioteche delle Nazioni Unite stabilite a New York, Ginevra, Bangkok, Beirut, Vienna, e i Dipartimenti delle Nazioni Unite.

[50]Cfr. la pagina degli Archivi presso l'UNOG, Ufficio delle Nazioni Unite di Ginevra.

[51]Siano consentiti i richiami a D. Grbac, *La rete delle biblioteche depositarie delle Nazioni Unite e la sua evoluzione in "Open Community"*, in F. Boschetti, A.M. Del Grosso, E. Salvatori (a cura di), "AIUCD 2021 – DH per la società: e-guaglianza, partecipazione, diritti e valori nell'era digitale". Raccolta degli abstract estesi della X conferenza nazionale, pp. 510-514; Id., *The United Nations Depository Libraries System as an "open community". The ongoing evolution from a knowledge base to a knowledge network*, in "Umanistica Digitale", 2021, n. 11, p. 199-216.

[52]Cfr. il sito Web ODS (*Official Documents System*).

[53]Cfr. il database UNTS – *United Nations Treaty Series Collection*.

[54]Per una storia delle lingue ufficiali e di lavoro delle Nazioni Unite si può consultare la nota redatta dalla Biblioteca Dag Hammarskjöld.

[55]Per una storia dei progetti di digitalizzazione cfr. United Nations, *Update on UN Digitization Programme*.

[56]Le pubblicazioni per la vendita sono accessibili solo tramite sottoscrizione del *repository* istituzionale delle Nazioni Unite *Un-iLibrary*. Esso mette a disposizione gratuitamente la sola lettura a video delle pubblicazioni contenute.

[57]Per un approfondimento si consultino la pagina del progetto e la guida alla ricerca.

[58]Per approfondire la panoramica si vedano in dettaglio tutte le tipologie di documenti presenti negli archivi.

[59]United Nations, Dag Hammarskjöld Library, DESA, *In praise of the "Great Open Conversation of Science. A summary of key messages from the Second United Nations Open science Conference*, (21-23 July 2021), in particolare p. 1-2, 10-11.

[60]Cfr. la pagina relativa alle *Frequently Asked Question* redatta dallo staff della Biblioteca Dag Hammarskjöld Library, *What are the conditions for requesting UN depository status and what obligations do depository libraries have?*, 27 July 2021.

[61]*Ivi*, *What is the purpose of the United Nations Depository Libraries Programme and the participating libraries?*, 30 July 2021.

[62]La conferenza "Open Con 2018" si è tenuta presso il quartiere generale delle Nazioni Unite il 23 ottobre 2018 con il titolo *Access for all? Equity of access to information inclusion, and the UN 2030 Agenda*; per un approfondimento dei temi trattati si veda il programma.

[63]United Nations, Dag Hammarskjöld Library, *Towards Global Open Science: Core Enabler of the UN 2030 Agenda*. A Conference at the United Nations Headquarters, 19 November 2019. Concept Note.

[64]Id., *Roundtable Discussion on a Global Science Commons*. Outcome Document United Nations Headquarters, Monday, 18 November 2019.

* * *

United Nations' transmission of cultural and intellectual heritage online in the international context defining an ecosystem for Internet governance and in particular for Open science

Abstract: The United Nations Depository Library System has been active for several years in sharing documents, materials and best practices, thanks also to the digitization projects carried out by the two libraries located at the United Nations Headquarters in New York and the United Nations Office in Geneva. The libraries have, as a matter of facts, anticipated and accompanied the process of affirmation of Open Science and Open Science practices globally.

Keywords: Depository libraries – United Nations – Open Science – UNESCO – EOSC