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

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0165 • articolo sottoposto a peer review • pubblicato in anteprima il 17 set. 2024

Milena Antonella Rizzi – Federico Serini

Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano

I concetti di cybersicurezza e cyberresilienza hanno fatto ingresso nell'ordinamento giuridico nonostante i dubbi sul loro significato giuridico. Si tratta infatti di formulazioni composte da concetti che, se da una parte, come nel caso della sicurezza e della resilienza, sono di difficile concettualizzazione in senso legale, dall'altra, per quanto riguarda il cyberspazio, sono perfino inediti per l'ordinamento. Il presente contributo propone una riflessione sul significato giuridico di tali termini attraverso l'interpretazione e l'indagine delle questioni ad essi sottese dalla prospettiva di diritto pubblico, ragionando sia sulla dialogica autorità-libertà propria della sicurezza, sia sui poteri del "digitale" mediante lo spettro del potere normativo.

Cybersicurezza europea e nazionale – Cyberresilienza europea e nazionale – Ordinamento e normazione tecnica

A proposed study of cybersecurity and cyberresilience concepts from a legal view between European and Italian legal systems

Cybersecurity and cyberresilience entered the legal system despite doubts about their legal meaning. These formulations are composed of concepts that, while on the one hand, as in the case of security and resilience are difficult to conceptualize in a legal sense, on the other hand, as regarding cyberspace, are even novel to the legal system. This contribution proposes a reflection on the legal meaning of these terms through an interpretation and investigation of the issues underlying them from a public law perspective analysing the authority-freedom dialogic proper to security, and the "digital" powers from the normative power view.

European and national cybersecurity – European and national cyberresilience – Legal system and technical standards

Il Prefetto Milena Antonella Rizzi è direttore del Servizio Regolazione, già Autorità e Sanzioni dell'Agenzia per la Cybersicurezza Nazionale (ACN) e dottoranda di ricerca in Studi giuspubblicistici presso l'Università di Roma Tor Vergata. Le opinioni espresse in questo contributo sono esclusivamente attribuibili all'Autrice e non riflettono la posizione dell'Agenzia per la Cybersicurezza Nazionale

Federico Serini è dottore di ricerca in Diritto pubblico, comparato e internazionale, per il curriculum di Diritto pubblico dell'economia, presso Sapienza - Università di Roma. Il 30 maggio 2024 ha concluso il percorso di dottorato difendendo una tesi dal titolo *Mercato, sicurezza e rischio informatico. Standard e certificazione dei beni ICT per esigenze di cybersicurezza nel contesto europeo e nazionale*

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* a cura di Marina Pietrangelo

1. Premessa di studio

Le risorse informatiche sono un elemento essenziale per le democrazie. Tali strumenti non rappresentano solo il mezzo che consente agli individui di esprimere liberamente la propria personalità in nuove forme e modi tramite la rete[1] ma, a livello tecnico, sono anche i parametri di configurazione e funzionamento di molte infrastrutture che erogano servizi e funzioni essenziali per la società e l'economia (cc.dd. infrastrutture critiche)[2]. Si pensi agli apparati informatici in uso presso gli operatori attivi nei settori bancario e finanziario, energetico, dei trasporti, delle comunicazioni, quello sanitario nonché quelli in dotazione presso le pubbliche amministrazioni e le varie istituzioni statali.

Questi strumenti sono ormai indispensabili sia per lo Stato in sé, sia per le sue componenti, prime fra tutte gli individui e le imprese[3]. Tuttavia, allo stesso tempo, sono anche responsabili di aver trasferito i rischi del cyberspazio nel mondo reale. La "rete globale" interconnessa si caratterizza infatti per essere un sistema non concepito per obbedire a criteri di sicurezza, quanto piuttosto a quelli di libero accesso, interoperabilità e libero scambio delle informazioni. Principi questi che si scontrano oggi con le possibilità di *dual use*[4] della rete e dei servizi informatici, tanto che alcuni autori hanno avvertito che oggi «ogni società è tanto vulnerabile quanto è vulnerabile l'informatica di cui fa uso» e pertanto «più le società sono avanzate, più sono vulnerabili»[5].

Ciò spiega la recente introduzione dei concetti di cybersicurezza e cyberresilienza negli ordinamenti europeo e nazionale.

Si tratta di due specializzazioni, o "tipi", di sicurezza la cui trattazione in senso giuridico sottende al fondamentale interrogativo di cosa significhi per l'ordinamento garantire "sicurezza" e "resilienza" *nel/del* "cyberspazio". Questione di non trascurabile rilievo se si considera che i citati termini del dilemma sono caratterizzati da una obiettiva difficoltà nell'individuare una loro traduzione in termini giuridici.

Da una parte troviamo infatti la sicurezza. Nozione sfuggente, di difficile definizione, che può

1. Frosini 2010, pp. 40-41.
2. Gallotti 2022.
3. De Vergottini 2021, p. 28.
4. I prodotti *dual use* sono i prodotti, inclusi software e tecnologie informatiche, che possono avere un utilizzo sia civile sia militare. Tali beni sono disciplinati dal Regolamento (UE) 2021/821, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso.
5. Losano 2017, p. 22. Sugli effetti delle forme di connettività non solo dovute alle tecnologie ICT v. Barabàsi 2014. Analogamente v. anche Khanna 2016.

acquistare differenti significati in base ai diversi contesti ordinamentali e al momento storico di riferimento[6], nonché variare in base alle diverse sensibilità, da persona a persona.

Dall'altra il cyberspazio, concetto che nasce nella letteratura fantascientifica degli anni Ottanta del secolo scorso e che ha trovato utilizzo in un primo momento nella dottrina strategico-militare, fino a fare recente ingresso nelle disposizioni legislative per mezzo del lemma "cyber", apposto a fianco di concetti più o meno noti al diritto (come in questo caso quelli di "sicurezza" e "resilienza") quale implicito riferimento a questo nuovo spazio, pur non essendo stato definito in termini giuridici[7].

Il rapporto tra l'ordinamento giuridico e il cyberspazio è stato teorizzato da alcuni autori con l'introduzione del concetto di *cyberlaw*, branca del diritto specializzata nel cyberspazio.

Già nei primi anni Novanta del secolo scorso, nel periodo in cui si svolgeva un accanito dibattito sui profili di fattibilità, nonché di opportunità e legittimità di una disciplina giuridica del cyberspazio[8], il giudice Frank Easterbrooks, in un discorso tenuto presso l'Università di Chicago nel 1996, fece ricorso alla metafora della "law of the horse"[9] per argomentare la sua idea di inutilità della *cyberlaw*. In tale occasione il giudice ricordò gli insegnamenti del decano Gerhard Casper, il quale affermava che «il miglior modo per apprendere il diritto applicabile a specifici settori è quello di studiare le regole generali». In caso contrario, si andrebbe incontro ad un pericoloso rischio di dilettantismo multidisciplinare che porterebbe il "cieco" – ossia lo studioso specializzato in un solo settore – ad essere un pessimo pioniere.

Condividiamo questa impostazione, valida non solo per studiare il progresso tecnologico dalla prospettiva giuridica, ma, come insegna illustre dottrina, anche per lo studio della sicurezza che non può risolversi nella mera tassonomia dei "tipi" originati dalle esigenze via via avvertite nel tempo, ma piuttosto nella riconduzione e rilettura di questi tipi all'interno della riflessione sulla sicurezza in generale[10].

Pertanto, dopo una breve contestualizzazione delle questioni poste sullo sfondo (parr. 2 e 3), nel proseguo tenteremo di analizzare e ricondurre i concetti di cybersicurezza (par. 4) e cyberresilienza (par. 5) nell'alveo della sicurezza in generale. L'analisi ci darà così modo di ragionare sul rapporto tra le individuate cybersicurezze e i diritti nel cyberspazio (par. 6), e infine concluderemo la riflessione tornando sul dibattitto relativo alla dimensione politica e giuridica della sicurezza in riferimento alle mutazioni apportate dall'informatizzazione (par. 7).

2. Il cyberspazio tra Stato, mercato e norme tecniche

Il dibattito sul governo del cyberspazio, ossia, sull'interesse degli Stati a regolare e controllare questo nuovo e inedito spazio che ha la caratteristica di essere un "non territorio", è un tema che può essere interpretato più in generale come una prova della sovranità degli Stati al tempo della globalizzazione[11]. Il cyberspazio rappresenta infatti una sfida per l'esercizio dei pubblici poteri da sempre legati all'elemento materiale della territorialità[12].

Curiosa è la genesi di questa dimensione. Il cyberspazio è un fenomeno originariamente

6. Rothschild 1995.
7. Sul punto Monti 2023b, p. 66, ove l'A. scrive che «invenzioni letterarie come il "ciberspazio" e il suo corollario "virtuale" hanno influenzato negativamente la riflessione giuridica […] essi non sono né fictio juris (come la persona giuridica) né metafore giuridiche (come la nozione di fonti del diritto), necessarie al funzionamento del Sistema. Di conseguenza, pur mantenendo un'indubbia utilità per spiegare fenomeni sociologici, psicologici e anche economici – come appunto, il metaverso – "ciberspazio" e i suoi derivati non dovrebbero avere alcun ruolo nell'individuazione di obiettivi normativi e nella loro trasposizione in leggi e regolamenti». Più diffusamente sul punto v. anche Monti 2023a.
8. Pollicino–Bassini–De Gregorio 2022, p. 4 ss.
9. Esterbrook 1996, p. 207 ss.
10. Mosca 2021.
11. Per quanto riguarda la "sovranità digitale" v. Baldoni 2024.
12. Irti 2006, p. 4.

pubblico, nato con il progetto Arpanet, successivamente sviluppato e diffuso per mezzo dei privati, fuori dal controllo degli Stati[13]. Difatti, l'ingresso dell'informatica nel mercato e nella società è stato un evento di scarso interesse per il potere pubblico, il quale in questo primo momento si è limitato ad intervenire con norme volte a favorire l'economia e gli investimenti in questo settore, nonché la regolazione dei meccanismi di funzionamento tecnico della rete, senza mai interessarsi di intervenire sui risvolti "politici" dello stesso[14].

Dopo un primo periodo di indifferenza, la sempre maggiore rilevanza sociale ed economica di questo ambiente, appresa anche a seguito dei crescenti attacchi e malfunzionamenti dell'informatica, hanno portato i pubblici poteri a volgere l'attenzione verso questo spazio, dimostrando «non solo di [poterlo] regolamentare ma anche "iper-regolare"»[15].

Tuttavia, l'elevato *expertise* richiesto nella regolazione di materie a contenuto tecnico-scientifico, nonché la mutabilità della tecnica in sé, sono i motivi per cui sempre più spesso si assiste ad una delegazione della competenza regolatoria da parte dei legislatori – attraverso i criteri del rinvio (fisso o mobile) e dell'incorporazione del contenuto di dette norme nella norma giuridica – agli enti di normalizzazione responsabili della produzione degli standard industriali.

Il dato è particolarmente significativo per quel che qui interessa. Come accennato, il cyberspazio è una dimensione che non appartiene ad alcun territorio ma che vive nei diversi elementi di cui è composto, di cui perlopiù, elementi fisici (gli hardware) e logici (i software), quali beni industriali che vengono scambiati nel mercato secondo le leggi della domanda e dell'offerta.

Da questa prospettiva, il cyberspazio può allora essere interpretato come un agglomerato di "merci", o meglio di prodotti, processi e servizi che attengono alle tecnologie dell'informazione e della comunicazione (beni ICT) – da qui la definizione che proponiamo di "cyberspazio merceologico"[16] – quale realtà in continua espansione in funzione degli sviluppi delle tecnologie informatiche che fanno ingresso nei mercati e che seguono pertanto le relative logiche e regole del mercato, nonché i relativi standard di produzione e di qualità.

Ciò è la ragione per cui il potere pubblico degli Stati in questa dimensione sembra cedere il passo alla normazione tecnica, quale strumento di regolazione che "parla" il linguaggio del mercato in quanto creata e sviluppata sulla scorta degli interessi degli stakeholder del settore.

Il tema ci porta quindi a riflettere sull'effettivo esercizio di potere nel cyberspazio attraverso lo spettro del potere normativo chiedendoci se questo risieda oggi negli Stati e nell'Unione europea o piuttosto nei privati che presenziano in questo settore, e soprattutto se la natura di questo potere sia politica o tecnica.

3. Cenni su normazione tecnica e ordinamento giuridico

Possiamo definire brevemente la normazione tecnica come quella «attività di produzione di norme atte ad individuare le caratteristiche tecniche, merceologiche e qualitative dei prodotti industriali da immettere sul mercato nonché, più recentemente, dei sistemi e processi industriali e dei servizi»[17].

L'innovazione e lo sviluppo tecnologico sono da sempre legati alla normazione di tipo tecnico[18]. Tuttavia, se fino all'età moderna tale regolazione risultava essere condotta in modo non sistematico[19], è a seguito della rivoluzione industriale che prende avvio l'attività di normazione nel senso

13. Bombelli 2017, p. 26; Della Morte 2018, p. 27, ove l'A. precisa che l'Internet è solo una regione del cyberspazio e pertanto i due termini non sono sinonimi.
14. O'Mara 2019.
15. Pollicino 2023, p. 415.
16. Sia concesso rinviare a Serini 2023.
17. Caia–Roversi Monaco 1995, p. 13.
18. Inkster 2008.
19. Si trattava di standard applicativi prodotti per ogni ambito dell'esistenza umana, dall'ingegneria edile alla produzione agricola e così via, ma senza avere un parametro di uniformazione su tali regole settoriali.

moderno del termine[20], ossia quando si afferma l'avvertita necessità di "unificare" tali norme[21].

Tale attività ha interessato diversi aspetti che vanno dall'uniformazione delle unità di misura, all'unificazione terminologica fino a quella dimensionale dei prodotti e delle loro componenti[22]. Ciò su cui concentreremo la nostra attenzione è l'evoluzione di tale normazione dal piano delle singole aziende a quello più ampio internazionale attraverso l'istituzione di appositi centri di formazione di dette norme.

La normazione tecnica nasce infatti nel contesto industriale dapprima dall'esigenza delle singole aziende di definire le caratteristiche costruttive e dimensionali dei propri prodotti come specifiche interne «custodite gelosamente», generando di conseguenza effetti di c.d. *vendor lock-in* che obbligavano i clienti a rivolgersi sempre allo stesso fabbricante[23].

In questo primo periodo, il ricorso alle norme tecniche è quindi prevalentemente orientato verso obiettivi individuali delle singole imprese. Il passaggio dall'utilizzo di tali strumenti a fini di mercato, anziché seguendo una logica produttiva strettamente individuale, è un processo che si è sviluppato gradualmente nel tempo. Tale evoluzione ha consentito di passare dall'utilizzo della normazione tecnica come strumento per guadagnare posizioni di potere nel mercato, secondo logiche di monopolio, a un ruolo chiave nella realizzazione di un mercato aperto e competitivo attraverso l'uniformazione.

È così che le attività di normazione tecnica vengono portate «fuori dagli ambiti aziendali (dove comunque permangono specifiche interne di qualità) e vengono convogliate in organismi indipendenti, a carattere settoriale o nazionale, di cui fanno parte, oltre ad esponenti delle industrie, rappresentanti delle pubbliche amministrazioni e delle università»[24].

Gli enti di normazione sono soggetti, spesso di natura privata, responsabili della produzione delle norme tecniche. Operano nel multilivello e, «per motivi essenziali storici», non sono più di tre: uno per il settore elettronico, uno per il settore delle telecomunicazioni e l'altro per tutti gli altri settori[25].

A livello internazionale sono presenti l'I*nternational Organization for Standardization* (ISO), l'*International Electrotechnical Commission* (IEC) e l'*International Telecommunication Union* (ITU). A livello europeo troviamo invece l'*European Committee for Standardization* (CEN), l'*European Committee for Electrotechnical Standardization* (CENELEC) e l'*European Telecommunications Standards Institute* (ETSI). In Italia gli organismi riconosciuti sono l'*Ente Nazionale Italiano di Unificazione* (UNI) e il *Comitato Elettrotecnico Italiano* (CEI).

Dal punto di vista giuridico, sebbene prendano il nome di "norme", tali strumenti non hanno natura giuridica in quanto la loro formazione non avviene per mezzo di un processo giuridico-politico, ma attraverso i ricordati alternativi centri di aggregazione di interessi non statuali – per l'appunto enti di normazione – il cui fine è quello di definire univocamente caratteristiche di prodotti, metodi e processi di produzione, nonché caratteristiche o metodi e criteri di valutazione circa la prestazione di un servizio.

Una recente dottrina ha raggruppato le diverse tipologie di norme tecniche in tre gruppi, ossia: norme originate da attori privati ma promulgate dai governi sovrani; norme originate e promulgate

20. Andreini 1995, p. 47.

21. A tal proposito si consideri che «[i]l termine "normazione" deriva dal latino "norma" e significa "regola". Fu poi tradotto con la parola "*standardization*" in inglese, "*normalisation*" in francese e "*Normung*" in tedesco, mentre il termine italiano "unificazione" fu coniato da Gabriele D'Annunzio, nel 1921, per indicare esattamente l'attività svolta dagli enti di normazione che cominciavano a nascere in Europa agli inizi del XX secolo, ovvero stabilire regole ed, appunto, unificare secondo un ordine riconosciuto e, come tale, accettato», cfr. UNI – Ente Nazionale Italiano di Unificazione 2012.

22. Andreini 1995, p. 47.

23. *Ivi*, p. 48.

24. *Ibidem*.

25. Andreini–Caia–Elias–Roversi Monaco 1995, p. 32.

da attori privati in seguito a delega governativa; e norme adottate da attori privati senza l'approvazione o l'applicazione governativa[26].

Sebbene elaborata in considerazione dei tipi di produzione delle norme tecniche negli Stati Uniti, riteniamo tale tripartizione utile anche nel nostro caso, permettendoci di distinguere norme tecniche vincolanti, norme volontarie e norme tecniche armonizzate.

Relativamente alle prime, precisiamo che le norme tecniche sono per loro stessa natura vincolanti, tuttavia nel caso in cui il loro contenuto venga riprodotto, trascritto, e materialmente recepito in un testo normativo (c.d. incorporazione) «la norma tecnica incorporata nella norma giuridica, [...] assume la stessa vigenza formale "ed entra perciò a far parte, come norma imperativa, dell'ordinamento"»[27].

A tal proposito precisiamo che l'ordinamento italiano, con legge 21 giugno 1986, n. 317, dando attuazione alla disciplina europea in materia di normazione e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, ha introdotto la c.d. "regola tecnica" definita come «una specificazione tecnica o altro requisito o una regola relativa ai servizi, comprese le disposizioni amministrative che ad esse si applicano, la cui osservanza è obbligatoria, de iure o de facto, per la commercializzazione, la prestazione di servizi, lo stabilimento di un fornitore di servizi o l'utilizzo degli stessi in uno Stato membro dell'Unione europea o in una parte importante di esso [...]»[28].

Le norme volontarie sono invece quelle elaborate e adottate dagli enti di normazione privati e, sebbene non siano obbligatorie, godono tuttavia di una vincolatività di fatto data dalla loro diffusa osservanza da parte degli attori economici di settore. Considerato che queste norme, originate fuori dal diritto degli Stati, sono (volontariamente) osservate da tali stakeholder di settore, riteniamo che queste norme siano espressione di un "diritto dei privati"[29].

All'interno di questa categoria rientra ad esempio la «norma europea», ossia «una norma adottata da un'organizzazione europea di normazione» (il CEN, CENELEC, o ETSI prima ricordati).

Infine, le norme armonizzate sono norme esistenti nel solo ordinamento europeo e sono state introdotte sulla scorta del Regolamento (UE) 1025/2012, che le definisce come norme europee adottate sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione.

Al pari delle norme volontarie, nonostante la non obbligatorietà di tali strumenti, la giurisprudenza della Corte di giustizia, ed in particolare da ultimo una pronuncia della Grande sezione[30], riconosce una vincolatività *de facto* di tali norme in quanto i prodotti che le rispettano beneficiano di una presunzione di conformità alle prescrizioni fondamentali relative a tali prodotti stabilite dalla pertinente legislazione dell'Unione sull'armonizzazione[31].

Ed in particolare, nel caso di specie, la Grande sezione concludeva che, sebbene il rispetto delle norme armonizzate non sia obbligatorio, la norma prodotta dal CEN è «manifestamente obbligatoria» poiché utile come metodo di prova per dimostrare la conformità dei prodotti[32].

Tra le normative tecniche e l'ordinamento giuridico sussiste una relazione. La norma tecnica acquista rilevanza per l'ordinamento giuridico ogni qualvolta questa venga "assunta" al suo interno, e tipicamente ciò avviene attraverso gli istituti dell'incorporazione e del rinvio (fisso e mobile).

26. Schwarcz 2002, p. 5
27. Salmoni 2002, p. 162. Sul punto v. inoltre Bachelet 1966, p. 86; Lugaresi 1995, p. 421, secondo cui con l'incorporazione «le norme tecniche assumono carattere imperativo per tutti i soggetti dell'ordinamento».
28. Art. 1, lett. *f*, legge 21 giugno 1986, n. 317, *Disposizioni di attuazione di disciplina europea in materia di normazione europea e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*.
29. Cesarini 1929.
30. CGUE, C-588/21, *Public.Resource.Org and Right to Know v Commission and Others*.
31. CGUE, C-588/21, pt. 74.
32. CGUE, C-588/21, pt. 79.

Vi è incorporazione quando il contenuto della norma tecnica viene trasposto *sic et sempliciter* all'interno di una fonte giuridica (generalmente primaria e/o secondaria), mentre il rinvio consiste nell'esplicito riferimento ad una norma tecnica puntualmente indicata (rinvio fisso o materiale), oppure nell'utilizzo di clausole generali all'interno di un disposto giuridico, come ad esempio il richiamo "alle migliori tecniche disponibili", "allo stato dell'arte" o piuttosto ai "migliori standard tecnici e di sicurezza", facenti riferimento al rispetto di normative tecniche quali presupposto di una buona pratica (rinvio mobile o formale)[33].

La norma tecnica viene così acquisita all'interno della norma giuridica, e quindi nell'ordinamento, suscitando non pochi interrogativi sulla natura di tali fonti una volta che siano state incorporate o richiamate.

Relativamente al primo caso, come anticipato, la dottrina maggioritaria è pacificamente concorde nel ritenere che la norma tecnica venga "giuridicizzata", costituendo parte integrante del disposto giuridico. Diversamente, maggiori difficoltà interpretative sono state ravvisate in relazione alla qualificazione della norma tecnica oggetto di rinvio, soprattutto se si considera che tali fonti, di natura privata, e protette da diritto d'autore, troverebbero una difficile cognizione e applicazione da parte di quei soggetti che non le abbiano acquistate.

Sul punto, alcuni autori hanno sostenuto che il «mero richiamo, in un documento ufficiale, del numero, titolo o data di applicazione della normativa» – ossia il rinvio materiale – porti alla «messa in corto circuito del diritto d'autore» poiché la norma tecnica così rinviata acquista rilevanza pubblicistica[34]. Il dubbio sembra infatti persistere relativamente al rinvio mobile, solitamente utilizzato nei casi in cui la norma giuridica si limita a dettare la disciplina generale di una materia, per poi lasciare ampio margine ai destinatari circa l'utilizzo delle norme tecniche utili a raggiungere il risultato "al meglio delle buone pratiche".

In conclusione, escluso quest'ultimo caso, in cui la norma tecnica conserva il suo carattere di fonte volontaria non cogente, l'incorporazione e il rinvio fisso trasformano la norma tecnica in un atto giuridico, facendole così assumere la denominazione di "norma tecnica pubblica" o "regola tecnica".

Tuttavia, come è stato precisato, il ricorso all'incorporazione e al rinvio non fanno dell'ordinamento tecnico un ordinamento giuridico, poiché i prodotti del primo acquistano forza normativa solo attraverso questo metodo di «selezione volontaria operata per il tramite della legge o di altro atto-fonte dell'ordinamento giuridico», conferendo quindi alla norma tecnica «non la qualificazione di fonte del diritto ma efficacia cogente»[35].

4. La normazione tecnica di cybersicurezza

La pretesa di sicurezza nel cyberspazio da parte degli Stati si scontra oggi con gli effetti derivanti dal ritardo con cui il potere pubblico ha attenzionato questa dimensione.

Non è un caso se le prime definizioni di cybersicurezza (*cybersecurity*), sicurezza informatica (*computer security*) e sicurezza delle informazioni (*information security*) hanno trovato formulazione nelle normative tecniche di settore.

Secondo la sociologia, il processo di globalizzazione ha portato ad una riarticolazione dello Stato che ha di fatto trasferito alcune sue funzioni ad attori privati[36], tra cui, col tempo, anche quella della sicurezza[37].

Dalla prospettiva giuridica ciò si è tradotto in una progressiva distinzione tra ruoli e funzioni appartenenti alla sicurezza pubblica (o primaria), che si esplicita nell'esercizio di poteri autoritativi e repressivi da parte delle pubbliche autorità, e forme di sicurezza secondaria o sussidiaria (a

33. Greco 1999, p. 37 ss.

34. Gigante 1997.

35. Iannuzzi 2018, p. 78 ss.

36. Sassen 2008.

37. Abrahamsen–Leander 2016. Sul punto si faccia riferimento alla *Confederation of European Security Services* (CoESS), unica organizzazione riconosciuta dalla Commissione europea e attiva in un costruttivo dialogo sociale settoriale con UNI Europa, l'organizzazione europea rappresentante i sindacati dei lavoratori nei settori dei servizi, rappresentativa delle realtà private che operano nel settore dei servizi di sicurezza.

sua volta distinta in sicurezza "complementare" e "comunitaria") ove partecipano anche soggetti privati a completamento, ausilio o integrazione della funzione di polizia[38].

Rispetto a questi fenomeni di "privatizzazione della sicurezza", la normazione tecnica nei settori della sicurezza risulta tuttavia essere espressione di una ulteriore evoluzione della materia che vede il coinvolgimento di soggetti privati, che nulla hanno a che fare con la sicurezza, ma che di fatto ne sono coinvolti[39].

Ecco, quindi, che la norma tecnica e gli enti di normazione che le producono acquistano particolare rilevanza in questo contesto, in quanto espressione delle esigenze di questi stessi attori privati operanti perlopiù nel settore Telco[40].

Prendendo in considerazione il panorama delle norme tecniche prodotte fino ad oggi è possibile distinguere almeno tre tipologie[41]. Le norme di primo tipo, con il quale sono stati regolati i processi produttivi al fine di garantire determinate caratteristiche dei prodotti. Le norme di secondo tipo, che hanno trovato spazio quando la normazione tecnica ha iniziato ad interessare la progettazione e le caratteristiche prestazionali dei prodotti. Infine, con l'introduzione della famiglia di norme ISO 9000, sono state introdotte le normative di terzo tipo, volte a normare l'intero sistema di produzione attraverso la formulazione dei cc.dd. sistemi di gestione della qualità.

Proprio all'interno di quest'ultima categoria, tra gli anni Ottanta e Novanta del secolo scorso, hanno iniziato a prendere forma le prime normative tecniche sulla sicurezza dei sistemi informativi e servizi informatici (*computer security*), nonché sulla sicurezza delle informazioni (*information security*)[42].

Per il loro significato, si faccia riferimento al bollettino dell'Agenzia statunitense competente nella gestione delle tecnologie, *National Institute of Standards and Technology* (NIST), ove per "sicurezza informatica" si intende «la protezione fornita ad un sistema informativo allo scopo di ottenere, come obiettivo applicabile, la conservazione dell'integrità, della disponibilità e della confidenzialità delle risorse del sistema informativo stesso (includendo hardware, software, firmware, dati e sistemi di telecomunicazione)» (NIST SP 800-14). Mentre la norma ISO/IEC 27000:2018, per "sicurezza delle informazioni", fa riferimento alla «preservazione della riservatezza, integrità e disponibilità delle informazioni», in qualsiasi forma esse siano rappresentate (digitale o materiale), o qualunque sia la loro modalità di trasmissione (comunicazione elettronica, corriere, ecc.).

Da ciò è possibile dedurre che il fine principale di tali normative è quello di preservare tre proprietà fondamentali delle risorse informatiche e delle informazioni affinché queste possano essere considerate sicure, spesso indicate con l'acronimo R.I.D (o C.I.A. in lingua inglese), ossia: la riservatezza (*confidentiality*), quale proprietà per cui tali risorse possono essere accedute solo da chi è stato autorizzato o ne abbia il diritto; l'integrità (*integrity*), che concerne la garanzia della correttezza, coerenza e affidabilità e quindi anche la certezza che il sistema informativo e l'informazione non siano stati alterati o modificati da soggetti non autorizzati; ed infine la disponibilità (*availability*), la proprietà secondo cui le risorse informatiche e le informazioni dovranno essere utilizzabili ed accessibili ogni qualvolta il soggetto autorizzato lo richieda.

4.1. Il concetto giuridico di cybersicurezza europea tra sicurezza del mercato unico e sicurezza dell'umano

La definizione di cybersicurezza a livello europeo è stata introdotta al culmine di un lungo processo

38. Mosca 2012, p. 26; v. anche Antonelli–Mattarella 2022, p. 131; nonché Aliquò 2023.
39. Farrand–Carrapico 2018, pp. 197-217.
40. Si rinvia al documento ENISA 2012, ove si dimostra che gli standard adottati nelle norme di cyberisucrezza europee per garantire la sicurezza e l'integrità delle informazioni sono fortemente basati su quelli utilizzati nel mercato europeo delle telecomunicazioni. Per quanto riguarda il coinvolgimento degli operatori Telco nella disciplina NIS sia concesso rinviare a Rizzi 2023, pp. 19-21.
41. Andreini 1995, p. 90 ss.
42. Gallotti 2022, p. 122.

che ha preso avvio con la disciplina sulla protezione delle infrastrutture critiche.

Già nel 2001 la Commissione europea adottava una Comunicazione sulla criminalità informatica ove veniva data la definizione di «sicurezza dei sistemi informatici e di rete» facendo riferimento alla «capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema», rinviando pertanto alle richiamate caratteristiche dell'informazione sicura.

Nel 2016 è stata emanata la Direttiva 2016/1148, anche nota come direttiva *Network and Information Security* - NIS, quale prima normativa in materia di sicurezza delle reti e dei sistemi informativi, oggi abrogata dalla Direttiva (UE) 2022/2555 (direttiva NIS II) entrata in vigore il 17 gennaio 2023 e che gli Stati membri sono tenuti a recepire entro il 18 ottobre 2024[43].

Nonostante la rubricazione, dall'analisi dei testi emerge come il legislatore europeo abbia inteso coniugare ancora una volta la sicurezza informatica con la protezione delle infrastrutture critiche, senza dedicare una apposita disciplina alla cybersicurezza in generale. Difatti, parte delle prescrizioni volte a «garantire un livello comune elevato di cybersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno» (art. 1) consistono perlopiù in una serie di obblighi gravanti sui soggetti individuati nella direttiva come «soggetti essenziali» e «soggetti importanti»[44], che dovranno adempierli a pena di ingenti sanzioni amministrative pecuniarie[45].

Solo con il successivo Regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*), l'Unione europea è intervenuta su profili più ampi della materia, introducendo – per la prima volta all'interno di un atto normativo giuridico – la nozione di "cybersicurezza", definita all'art. 2, n. 1, come «insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

Questa formulazione non solo introduce nell'ordinamento giuridico (europeo) un concetto prima di allora esclusivamente tecnico, ma gli conferisce anche valore sociale e politico.

Ciò può essere dedotto dal fatto che nella prima parte della definizione, il riferimento alla protezione della rete e dei sistemi informativi si sostanzia nella garanzia del poc'anzi ricordato RID delle informazioni e del supporto che le contiene, quale caratteristica fondamentale della *information* e della *computer security*, già definite nelle prime norme tecniche di settore.

Tuttavia, è nella seconda parte che riscontriamo il tratto innovativo di questa definizione, ossia il riferimento alla "sicurezza dell'umano", inteso non solo come l'utente, la persona fisica che utilizza asset informatici e informativi, ma anche qualsiasi soggetto che anche non facendone uso può essere impattato negativamente dall'informatica o da minacce veicolate attraverso di essa.

A nostro modo di vedere, la scelta del legislatore europeo è stata quella di dirigere la cybersicurezza verso un fine pubblico di protezione delle persone fisiche (oltreché di sicurezza del mercato unico), superando lo scopo tipico delle norme tecniche di settore, solitamente dirette all'esclusiva garanzia del business delle organizzazioni che intendono osservarle e certificare la loro conformità a tali norme.

4.2. La cybersicurezza nazionale italiana

Il d.l. 14 giugno 2021, n. 82, recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, ha introdotto per la prima volta nell'ordinamento italiano, la nozione di "cybersicurezza nazionale" all'art. 1, co. 1, lett. *a*), definendola come

> l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti,

43. In particolare, nella legge di delegazione europea 2023, pubblicata nella *Gazzetta Ufficiale* n. 46 del 24 febbraio 2024, all'art. 3 sono individuati i principi e i criteri direttivi per l'implementazione della nuova disciplina che dovranno ispirare l'atto di recepimento della disciplina europea.
44. Cfr. art. 3, e Allegati I e II, direttiva NIS II.
45. Cfr. Capo VII, ed in particolare art. 34 direttiva NIS II.

> sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Precisiamo che l'inciso relativo alla «tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico» è stato introdotto nel corso dell'esame in sede referente delle Commissioni I e IX della Camera[46], per poi essere trasposto in sede di conversione nel testo della legge 4 agosto 2021 n. 109[47].

Come per la formulazione della cybersicurezza europea, anche la definizione di cybersicurezza nazionale è frutto di un processo di composizione ove è possibile individuare due anime: quella derivante dai principi e concetti elaborati nelle normative tecniche sulla sicurezza informatica e delle informazioni; e quella di carattere giuridico-politico, relativa alla collocazione della materia *anche* tra le attività dirette alla tutela della sicurezza e dell'interesse nazionale. Motivo per cui la citata aggiunta in sede referente ha conferito particolare rilievo alla formulazione, ma ha anche aperto a problemi interpretativi.

Come già anticipato (par. 1), il riferimento alla "sicurezza nazionale" nello "spazio cibernetico" costituisce un rinvio a due concetti su cui insistono, a loro volta, dubbi interpretativi.

Relativamente al primo, si tratta di un concetto che, sebbene sia stato oggetto di un processo di normativizzazione[48], resta tuttavia una nozione fondamentalmente politica, priva di autonomia giuridica, e tendenzialmente immune dal controllo giudiziario[49]. Caratteristiche che si è tentato di superare in parte con la proposta definitoria avanzata in sede referente del d.l. in merito ad

46. Il disegno di legge in questione è stato identificato con il progressivo "Atto Camera: 3161". Nello specifico si rinvia alla sezione Emendamenti del sito della Camera, ove è possibile scorrere le diverse proposte in sede referente (relative all'art.1 vi sono state otto proposte) che hanno portato all'attuale formulazione della disposizione. Gli emendamenti apportati dal Senato in sede di conversione, Atto Senato n. 2336, hanno invece interessato gli artt. 4 e successivi.
47. Si invita alla lettura del d.l. 14 giugno 2021, n. 82, coordinato con la legge di conversione 4 agosto 2021, n. 109, recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*.
48. Il riferimento è agli artt. 6 e 7 della legge 3 agosto 2007, n. 124, recanti rispettivamente disciplina delle Agenzie informazioni e sicurezza esterna (AISE) e interna (AISI), ove i disposti fanno riferimento alle nozioni di «difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica» (art. 6) nonché alla «sicurezza interna della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica» (art. 7), ove precisiamo che le richiamate nozioni di "sicurezza della Repubblica" e "sicurezza dello Stato" sono sinonimi di "sicurezza nazionale". In particolare, la prima è stata oggetto di discussione in sede parlamentare in occasione della riforma del sistema di *intelligence* avvenuta con la richiamata legge 124/2007, ove l'espressione sicurezza della Repubblica è stata preferita ad altre definizioni in quanto «concetto […] più ampio rispetto a quello di "Stato", utilizzato dalla legge 801/1977, che regolava in precedenza la materia» (*Dossier del Servizio studi della Camera sulla riforma dei servizi*, n. 115, del 18 dicembre 2007). Tuttavia, l'assimilazione del compito di tutela della sicurezza nazionale (*rectius* sicurezza della Repubblica) agli apparati di *intelligence* non deve far pensare che tale funzione sia esclusivamente rimessa a tali organismi. Come osserva autorevole dottrina, tale visione porterebbe ad una "semplificazione culturale" che non tiene conto del fatto che la tutela della sicurezza nazionale interseca diverse competenze che portano l'*intelligence* a collaborare con altri attori istituzionali i quali, in una «funzione non monopolista, ma pluralista», sono rappresentati dalle forze di polizia, le forze armate, la diplomazia, fino ad estendersi, di fatto, a tutta la pubblica amministrazione. (Valentini 2017, p. 56 ss). Secondo alcuni autori, l'estensione del concetto alla pubblica amministrazione può essere dedotta dall'interpretazione del dovere di difesa della Patria di cui all'art. 52 Cost., quale dovere di solidarietà politica che «non si riduce alla sola difesa in armi, [come difesa dal nemico esterno] essendo ben suscettibile di adempimenti attraverso la prestazione di adeguati comportamenti di impegno sociale non armato» (Ursi 2022, p. 56).
49. Così Monti 2020.

un eventuale art. 1, co. 1, lett. a-*bis* al decreto, ove la sicurezza nazionale veniva definita come «il dovere del Governo di proteggere e realizzare gli interessi nazionali nel rispetto dei principi costituzionali e delle prerogative del Parlamento»[50]. La proposta non ha poi trovato approvazione in sede di conversione.

Per quanto riguarda lo "spazio cibernetico" invece, oltre quanto già abbiamo tratteggiato in precedenza (par. 2), pare necessario osservare che questo concetto ha trovato definizione in alcuni documenti interni. In particolare, nel "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" del 2013 ove veniva definito come

> l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete.

Secondo alcuni autori la cybersicurezza nazionale è un concetto non completamente coincidente con quello di sicurezza nazionale, ma certamente vi rientra seppur solo relativamente ai beni e servizi di natura informatica[51]. Tale interpretazione ci sembra percorribile. Il riferimento è difatti all'inciso «ferm[e] restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124 [...]» che quindi distingue l'azione per fini di "cybersicurezza" da quello per la "sicurezza della Repubblica".

Tuttavia, l'orientamento delle azioni di mera sicurezza informatica e delle informazioni «anche» ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nel cyberspazio, ci permette di concludere che la cybersicurezza, quindi diversa dalla sicurezza nazionale, ne è comunque ricompresa e si esprime attraverso una estensione dell'azione di governo in questo settore.

Si pensi alla vicenda che ha interessato le tecnologie 5G e il settore delle Telco nel 2019, ove si è dimostrato come i poteri del Governo nell'ambito della (cyber)sicurezza nazionale non si limitino più soltanto all'apposizione del segreto di Stato[52]. Nel particolare caso citato, è stata difatti evidenziata la progressiva estensione dei poteri dell'esecutivo per motivi di sicurezza anche su beni prima di allora non ricompresi nell'ambito della sicurezza nazionale e della difesa[53], attraverso l'esercizio dei cc.dd. *golden powers*[54].

Tuttavia, non riteniamo di poter concludere che la cybersicurezza nazionale costituisca una *species* nel contesto delle "sicurezze" nazionali[55], piuttosto pare ragionevole sostenere, come già intuito in dottrina, che la cybersicurezza nazionale sia una componente trasversale alla difesa dello Stato e all'ordine e alla sicurezza pubblica, quale «articolazione tecnica avente natura ordinatoria e non gerarchica»[56].

Infine, il riferimento agli «obblighi derivanti da trattati internazionali», ribadisce che, come per la sicurezza in generale, tale concetto non può essere definito in sede meramente nazionale, ma deve tener conto del più ampio quadro dei diritti, doveri e libertà degli ordinamenti sovranazionali.

5. Il concetto di resilienza

Secondo le scienze sociali l'indeterminatezza della minaccia che caratterizza i tempi moderni, sarebbe riconducibile al fatto che lo sviluppo della vita associata e il crescente grado di complessità dei sistemi sociali hanno reso sempre più difficile per gli attori valutare le conseguenze dei propri

50. Vedi la proposta emendativa 0.1.7.2., dell'ex deputato Giovanni Luca Aresta, nelle commissioni riunite I-IX in sede referente riferita al C. 3161 0.1.7.2., pubblicata nel *Bollettino delle Giunte e Commissioni* del 15 luglio 2021.
51. Cfr. Pansa 2019, p. 34.
52. Sul punto si rinvia a Bobbio 2011; Brutti 2017, p. 193 ss. nonché Scandone 2008, p. 397 ss. Per una lettura aggiornata sul punto v. Scandone 2023, p. 269 ss.
53. Valensise 2020.
54. Fiorentino 2020, p. 57.
55. Cfr. art. 6, co. 2, e art. 7, co. 2, legge 124/2007 ove è previsto che l'azione delle Agenzie di informazione e sicurezza esterna (AISE) e interna (AISI), si svolge a protezione oltre degli interessi politici e militari, anche di interessi «[…] economici, scientifici e industriali dell'Italia» quali rientranti nella sicurezza della Repubblica.
56. Monti 2020, p. 6.

comportamenti[57], dando così vita a quella che Ulrick Beck ha definito la "società del rischio".

Deve tuttavia osservarsi come in questo clima di incertezza, che renderebbe qualsiasi azione umana fonte di eventuali rischi/pericoli, l'azione di protezione da parte del potere pubblico potrebbe facilmente scivolare in una concezione di massima sicurezza e di difesa totale che andrebbe fortemente a limitare, se non addirittura negare, le libertà umane.

La gestione del rischio diventa quindi un tema particolarmente importante e sensibile nelle democrazie costituzionali volte a tutelare le libertà nelle società post-industriali, soprattutto in considerazione del fatto che il rischio non ha necessariamente una accezione negativa di possibile futuro danno, ma anche positiva, quale fattore che stimola la innovazione e progresso[58].

Come per la sicurezza, anche in questo caso il principio di proporzionalità gioca un ruolo fondamentale. I sistemi di gestione del rischio si basano infatti su processi che presuppongono il calcolo del rischio quale operazione che permette di rendere l'incertezza del danno calcolabile (seppur in termini stocastici), consentendo una gestione razionalizzata della crisi *ex ante* attraverso l'adozione di adeguate decisioni secondo una determinata scala di valori e stime.

Il rischio (R) è infatti determinato dal prodotto di due variabili date dall'impatto della minaccia su un determinato bene, persona o valore (I) tenuto conto del grado della probabilità (stocastica) che tale evento si verifichi (P) entrambe calcolate secondo una prestabilita unità di misura, pertanto in formula R = I x P.

L'introduzione del concetto di rischio ha quindi permesso all'uomo di procedere ad una razionalizzazione e misurazione del pericolo, venendo a creare un divario tra il «rischio tecnico», ossia il rischio che risponde a variabili oggettive ed è quindi calcolabile, e il «rischio percepito», che invece resta una sensazione soggettiva[59].

Abbiamo deciso di argomentare sul concetto di resilienza a seguito di tale breve introduzione sul rischio poiché, diversamente dalla sicurezza tradizionale che risponde a logiche ove la lesione del bene rappresenta un fallimento per le politiche di sicurezza, la resilienza si sviluppa invece su modelli di accettazione del rischio, quindi del futuro danno, e che contemplano strumenti volti a far fronte a scenari di crisi con l'obiettivo di preservare la continuità e il funzionamento di un determinato sistema[60].

La resilienza, si concentra infatti sulla prevenzione dalle minacce e sulla minimizzazione degli effetti derivanti dalla realizzazione della minaccia (danno) con un approccio di tipo proattivo[61].

Tuttavia, anche in questo caso riscontriamo l'assenza di una definizione univoca del concetto, nonostante i diffusi richiami all'interno di documenti politici e giuridici negli ultimi tempi[62].

Si tratta infatti di una nozione a cui fanno riferimento diversi campi del sapere che vanno dalle scienze dei materiali, alla psicologia, fino all'ecologia e all'economia[63]. Quindi la troviamo sia nelle scienze esatte (*hard science*) sia in quelle umanistiche. La distinzione ci è utile poiché migrando dalla scienza dei materiali, ove per resilienza si intende il grado di resistenza alla rottura o deformazione di un elemento (c.d. prova d'urto)[64], l'utilizzo di questo concetto in riferimento agli individui, alle comunità e alla società più in generale, ha assunto secondo alcuni autori almeno tre significati: «resilience as maintenance», ove è enfatizzato l'utilizzo della capacità di adattamento per mantenere lo *status quo*; «resilience as marginality», mirando a mantenere i cambiamenti prodotti da una crisi o

57. Nocifora 2010, p. 104 ss.

58. Giddens 2000, p. 38, ove l'A. scrive che «[…] una positiva assunzione di rischio sta alla base di quell'energia che crea la ricchezza in un'economia moderna».

59. Nocifora 2010, p. 107.

60. Cfr. Fjäder 2014.

61. Castaldo 2019.

62. Sul punto v. D'Onghia 2020.

63. Cfr. Walker–Cooper 2011, ove le Autrici fanno riferimento al concetto di resilienza negli studi di Crawford Stanley Holling, nell'ambito dell'ecologia e Friedrich August von Hayek, nel campo economico.

64. Cfr. "Resilienza" in *Enciclopedia della Scienza e della Tecnica*, Treccani, 2008.

uno shock in modo marginale al fine di preservare contro cambiamenti alle strutture o alle politiche esistenti; e «resilience as renewal», con l'obiettivo di trasformare, potenzialmente rimodellare, la struttura e le politiche esistenti, facendo affidamento sulla diversificazione tra molteplici strutture e istituzioni come riserve[65].

In riferimento alle scienze sociali, in prima approssimazione, possiamo quindi osservare che la nozione abbia acquistato il senso di capacità di un "sistema" di prepararsi, adattarsi e riprendersi da perturbazioni o eventi avversi tale da conservare una condizione di normalità. Accezione positiva, che si accompagna tuttavia al "lato oscuro" del concetto di resilienza quale forma di resistenza al cambiamento e quindi all'innovazione e al progresso, o come incapacità di adattamento[66].

Dal punto di vista dei *security studies*, e in particolare dalla prospettiva della Scuola di Copenaghen, nel paradigma di resilienza il decisore politico è parzialmente sollevato dal difficile compito di scegliere quali minacce prioritizzare[67], dato che tale modello è perlopiù concentrato sulla minimizzazione degli effetti delle minacce con un approccio *all hazard*, ossia considerando tutte le forme di minacce umane, tecniche e naturali, che vanno dal terrorismo e sabotaggio ai fallimenti dei sistemi tecnici e alle catastrofi naturali.

In termini giuridici non troviamo una definizione di questo concetto che, così come il lemma "cyber", ha fatto ingresso nell'ordinamento giuridico pur trovando origine in altri campi del sapere.

Ci si potrebbe tuttavia chiedere se questo non fosse già presente nell'ordinamento vivendo in altri istituti. Relativamente all'ordinamento italiano è il caso della "sicurezza civile", secondo alcuni autori assimilabile alla resilienza in quanto è anch'essa una forma di sicurezza che si sostanzia nella gestione degli eventi di crisi[68].

Ad ogni modo si tratta di una ulteriore specializzazione della sicurezza che, a nostro modo di vedere, è riconducibile nell'azione di polizia amministrativa definita nei primi del Novecento da Oreste Ranelletti come quella attività diretta alla sicurezza delle «cose o attività che hanno una funzione sociale […]», ossia una funzione che «deve interessare la società, in modo da permettere a questa di raggiungere alcuni suoi scopi di conservazione o di perfezionamento, se funziona bene; e in modo da danneggiare o non soddisfare la società medesima, se funziona male», tale per cui «[l]a funzione della cosa o l'attività, quindi, viene qui tutelata come un fatto sociale, non come un diritto»[69].

I riferimenti alla difesa dell'esistenza, all'integrità e funzione delle cose «al solo fine che queste cose, malamente esistendo o funzionando, non danneggino l'ordine giuridico esistente», paiano infatti sinonimi della capacità di un "sistema" di "resistere", "adattarsi", "riprendersi" alle "perturbazioni", "shock" o "crisi" in maniera tale da preservare la sua esistenza o la sua "continuità".

5.1. La cyberresilienza europea e italiana

Diversi documenti politici e giuridici menzionano i concetti di resilienza e cyberresilienza senza tuttavia darne una definizione. Tra questi rientrano anche gli atti dell'Unione europea ove, sebbene il concetto figuri nella denominazione del testo o venga spesso richiamato all'interno dell'atto, non è possibile individuare una definizione sul punto.

Ne è conferma l'analisi dei recenti atti che compongono la legislazione europea in tema di cybersicurezza: vedi la Direttiva NIS II, il Regolamento DORA (*Digital Operational Resilience Act*) e le proposte di Regolamento *Cyber Resilience Act* e *Cyber Solidarity Act*[70].

Tuttavia, pur in assenza di elementi definitori, è chiaro che tali misure siano volte ad aumentare i livelli di sicurezza delle infrastrutture critiche, dei servizi finanziari, dei beni ICT nonché a raggiungere il più generale obiettivo di «rafforzare le capacità nell'Unione per individuare, prepararsi e rispondere alle minacce e agli incidenti di

65. Bourdeau 2013.
66. Williams–Gruber–Sutcliffe et al. 2017, p. 756.
67. Dunn Cavelty–Eriksen–Scharte 2023.
68. Lega 2023, p. 371.
69. Ranelletti 1904, p. 305.
70. Sul punto v. Chiara–Brighi 2024, p. 7.

cybersicurezza»[71] per il solo fine di garantire il funzionamento o, meglio, la continuità, del "sistema" mercato unico europeo.

Per quanto riguarda l'Italia, nel processo di conversione del citato d.l. n. 82/2021, oltre al riferimento alla resilienza contenuto nella definizione di "cybersicurezza nazionale", è stata introdotta in sede referente, all'art. 1, co. 1, lett. *b*), anche la definizione di "Resilienza nazionale nello spazio cibernetico" che si riferisce a «le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131», da intendersi quindi come insieme di attività volte ad evitare un «danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale».

Diversamente dalla resilienza europea, diretta a preservare la continuità e il funzionamento delle reti per garantire a sua volta il funzionamento del mercato unico, il legislatore italiano per cyberresilienza nazionale ha inteso l'insieme di azioni volte a preservare il "continuo" funzionamento del "sistema" Stato facendo quindi riferimento alle funzioni o servizi essenziali rientranti nella disciplina sul Perimetro di Sicurezza Nazionale Cibernetica (PSNC).

Sul piano amministrativo, la cyberresilienza rientra tra gli obiettivi dell'Agenzia per la cybersicurezza nazionale (ACN) attraverso la promozione di azioni comuni dirette per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore[72].

L'implicito richiamo è quindi alle citate politiche e atti di diritto derivato europei in tema di protezione delle infrastrutture critiche e di sicurezza delle connessioni nonché di cybersicurezza dei beni ICT.

Infine, ulteriore riferimento, questa volta espresso, è quello relativo alle «esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese»[73], a cui partecipano l'ACN e il Nucleo per la cybersicurezza (NC), quest'ultimo, eventualmente, anche in qualità di promotore e coordinatore[74].

Dal breve quadro tratteggiato, relativo ad entrambe le ipotesi definitorie, emerge come la cyberresilienza, ossia la preservazione della continuità del sistema, si riferisca perlopiù ad elementi non umani, e come i cittadini o la società in generale godano solo indirettamente di tale azione.

Il tema apre alla questione della (cyber)resilienza dell'umano quale recente campo di indagine di alcune analisi dei *security studies* propense a far ricomprendere nella nozione di "sistema" non solo il dominio fisico e quello informazionale del cyberspazio, ma anche il dominio cognitivo e sociale, al fine di sviluppare modelli di cyberresilienza che tengano conto anche di elementi riconducibili all'uomo quali la capacità di comprendere e far fronte psicologicamente ad una crisi[75]. Si tratta di una nuova prospettiva di studio che potrebbe certamente dirci molto sulla relazione fra rischio tecnico e rischio percepito poc'anzi richiamati.

6. La stabilità del cyberspazio: un bilanciamento tra continuità del servizio, libertà degli utenti e sicurezza

«Be conservative in what you do, be liberal in what you accept from others». Nel 1980, con questo postulato l'informatico statunitense Jon Postel, uno dei creatori di Internet, dettava il principio di

71. Art. 1, proposta Regolamento (UE) 2023/109.
72. Art. 7, co. 1, lett. *a*) del d.l. 82/2021.
73. Art. 7, co. 1, lett. *o*) del d.l. 82/2021.
74. Art. 9, co. 1, lett. *c*) del d.l. 82/2021.
75. Dunn Cavelty–Eriksen–Scharte 2023.

robustezza delle reti, anche noto in informatica come legge di Postel[76].

L'enunciato è particolarmente significativo in quanto sintetizza bene l'idea che ha portato alla creazione di Internet ai suoi albori, il cui valore è tuttavia ancora attuale. Si tratta infatti di uno dei principi che regolano la progettazione della trasmissione dei dati a pacchetto, che caratterizza per l'appunto il servizio Internet come lo conosciamo oggi, prevedendo che, quando si inviano dati o si sviluppano nuovi protocolli e applicazioni per Internet, si dovrebbe farlo in modo conservativo, cioè, seguendo rigorosamente gli standard e le specifiche esistenti. Dall'altro, quando si ricevono dati o si accettano connessioni, si dovrebbe essere più flessibili e tolleranti verso eventuali errori o variazioni dai protocolli standard.

L'assunto ci è utile poiché rende evidente la natura "aperta" e vulnerabile delle reti, orientate a preservare il libero flusso delle informazioni. A livello giuridico, derivati della legge di Postel sono i due principi di libero accesso e neutralità[77]. Principi che permettono non solo l'utilizzo di Internet, quale servizio universale[78], ma allo stesso tempo costituiscono anche i criteri di funzionamento dell'infrastruttura stessa.

Vi è quindi un punto di contatto tra le regole che disciplinano il funzionamento e l'esistenza della Rete (secondo l'accezione per cui è stata pensata sin dai suoi albori), e la tutela dei diritti fondamentali in Rete[79], tra cui il diritto di accesso alla stessa.

A ben vedere secondo alcuni autori il diritto di accesso non è un diritto fondamentale a sé stante, ma piuttosto è uno strumento di esercizio di altri diritti[80]. Al di là delle diverse interpretazioni, se l'accesso abbia valore meramente strumentale, o sia una libertà o un diritto sociale[81], il dato certo è che la Rete è indubbiamente uno strumento che consente agli individui di esprimere liberamente la propria personalità in nuove forme e modi per mezzo di essa e dei suoi diversi servizi[82].

La precisazione è d'obbligo poiché, come si comprenderà, parlare di sicurezza o resilienza *nel/del* cyberspazio, significa innanzitutto chiedersi in quali rapporti si pone l'esigenza di sicurezza rispetto alle libertà della Rete, e da quale punto di vista ci poniamo.

Si assiste spesso ad azioni che hanno l'effetto di rompere questo legame e frammentare la Rete, o il cyberspazio. Data l'incertezza del termine, la letteratura sul punto ha enucleato tre tipologie di frammentazione:

> Technical Fragmentation: conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data

76. Si rinvia alla RFC 761 (acronimo di "request of comments", si tratta di un'espressione utilizzata in telecomunicazioni e informatica indicante un documento pubblicato dalla *Internet Engineering Task Force*, che riporta informazioni specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico o, più nello specifico, di Internet) al link: https://www.rfc-editor.org/rfc/rfc793.
77. Per una definizione di neutralità della rete v. la pagina AGCOM (aggiornata al 25 giugno 2024) relativa a *La neutralità della Rete* ove questo concetto è definito come quel principio per cui «l'accesso ad Internet deve essere trattato in modo non discriminatorio, indipendentemente dal contenuto, dall'applicazione, dal servizio, dal terminale, nonché dal mittente e dal destinatario» (ultimo accesso 1 agosto 2024). Per una panoramica sulla definizione del principio della neutralità della rete, si veda De Filippi–Belli 2014.
78. Su Internet come patrimonio comune dell'umanità Ruotolo 2014, p. 556 ss.; Segura Serrano 2006; Spang–Hassen 2006.
79. Cfr. art. 1 della Dichiarazione di Paragi adottata in seno al *World Summit on Information Society* (WSIS) nel 2003 che pone come obiettivo la costruzione di una società dell'informazione a dimensione umana, aperta e caratterizzata dalla piena condivisibilità della medesima, individuando pertanto un legame con la dimensione della tutela dei diritti umani. Sul punto v. Oddenino 2008, p. 151 ss. Per un'ampia riflessione sul tema si rinvia al fascicolo monografico Calzolaio 2023.
80. Cerf 2012.
81. Per una efficace panoramica sull'accesso ad Internet e le relative implicazioni nel contesto nazionale ed internazionale si rinvia a Passaglia 2021.
82. Cfr. Frosini 2010, pp. 40-41.

> packets and of the Internet to function consistently at all end points.
> Governmental Fragmentation: Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.
> Commercial Fragmentation: Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources[83].

In tutte le ipotesi emerge come queste azioni possano essere perpetrate tanto da poteri pubblici quanto da attori privati. Relativamente ai primi, ne sono un esempio le pratiche di *zoning*, ossia la creazione di percorsi di rete alternativi a quello ordinario (l'Internet o cyberspazio globale) che, se portate all'eccesso, possono essere l'origine di un processo di balcanizzazione della Rete, e quindi di creazione di tante sotto-reti che hanno adottato criteri logici e di funzionamento diversi rispetto all'Internet mondo[84].

Tra i casi che invece possono essere annoverati alle azioni di frammentazione dei privati possiamo far riferimento alle pratiche di *vendor lock-in* attraverso la creazione di specifiche tecniche (standard) di prodotti e servizi ICT, che possono dare vita a vere e proprie guerre di standard per il dominio sui mercati[85], o anche essere guidate da fini e obiettivi politici estranei alle logiche di mercato[86].

Tuttavia, sono possibili azioni che interferiscono sui diritti e libertà dei soggetti interconnessi anche senza ricorrere a strumenti che hanno l'effetto di frammentare la Rete, come nel caso del filtraggio e del controllo dei contenuti.

In tutti questi casi si tratta di attività poste in essere per esigenze di sicurezza interna avvertite da singoli Paesi ma che possono incidere sul servizio universale Internet in sé, nonché anche su soggetti che risiedono al di fuori degli Stati che attuano tali politiche di sicurezza.

Come osservato da alcuni autori in considerazione della Dichiarazione universale dei diritti umani, in particolare gli artt. 19 e 29, emerge con chiarezza che «sono i governi a determinare cosa è contro la sicurezza nazionale e l'ordine pubblico nelle rispettive società [cosicché] un combattente per la libertà agli occhi di un governo potrebbe essere considerato un terrorista agli occhi di un altro paese»[87].

Il bilanciamento tra uno strumento di libertà e globale come il servizio Internet e le ragioni di sicurezza interna degli Stati può quindi variare da ordinamento a ordinamento a seconda della forma di Stato vigente, tra soluzioni che vanno dalla netta chiusura al controllo ad altre che invece privilegiano la proporzionalità.

Tuttavia, non solo i poteri pubblici hanno rilevanza in questo contesto. Ulteriore protagonista sono anche i privati che producono beni o erogano servizi ICT i quali possono anche produrre beni e servizi sul mercato, ispirati a principi non necessariamente coincidenti con quelli dello Stato presso cui sono utilizzati. Si faccia riferimento al recente caso posto in evidenza dalla stampa internazionale secondo cui Apple avrebbe notificato a dei giornalisti indipendenti indiani e ad alcuni politici dell'opposizione che il governo indiano avrebbe cercato di violare i loro iPhone[88].

Con queste brevi considerazioni abbiamo quindi cercato di ragionare sul rapporto autorità-libertà nel cyberspazio, cercando di cogliere aspetti che non si limitano solo alle forme di controllo dei contenuti che circolano in questa dimensione, ma anche a come il rapporto autorità-libertà possa

83. Drake–Cerf–Kleinwachter 2016, p. 4. Il contributo nasce dall'esigenza di chiarire l'argomento in questione al fine di facilitare il confronto in senso al *World Economic Forum's Multi-year Future of the Internet Initiative* (FII) dato che il concetto di "frammentazione" non ha univoco significato:«human rights lawyer, a trade economist and a network engineer might each give the term a special shade of meaning based on their respective priorities and experiences» (*ivi*, p. 11).

84. Cfr. Oddenino 2008, p. 74. A tal proposito è nota la "Great Firewall" adottata dal governo cinese, sul punto v. Wang 2019.

85. Shapiro–Varian 1999.

86. Nel caso della creazione di barriere commerciali nel settore delle ICT per ragioni di sicurezza interna v. Peng 2015.

87. Drake–Cerf–Kleinwachter 2016, p. 32.

88. Shih–Menn 2023.

incidere sull'infrastruttura stessa del cyberspazio, quale realtà fortemente legata alle dinamiche politiche e di mercato (par. 2).

7. Considerazioni conclusive sulle cybersicurezze tra giuridico, politico e tecnico

Giunti al termine di questa analisi, possiamo allora tentare di ricondurre le due cybersicurezze nella più ampia riflessione sulla sicurezza in generale, quale «condizione di chi e di ciò che è esente da pericoli o tutelato da possibili pericoli», che consente ai consociati di sentirsi «liberi di agire con certezza e libertà»[89].

Certezza e libertà, che non devono solo essere il frutto di uno stato di sicurezza percepita dall'individuo, ma sono anche il prodotto di un complesso e delicato bilanciamento tra autorità e libertà ove il quando e il come la sicurezza opera limitazioni alle libertà è stabilito dalla legge, nei casi in cui la Costituzione prevede che ciò possa accadere[90].

In questi termini la sicurezza tradizionale moderna si esprime come sicurezza giuridica di ispirazione *kelseniana*.

La dottrina sul punto ha distinto due coordinate quali quelle di sicurezza ottenuta *attraverso* il diritto, quale base legittimante l'azione del potere pubblico – oggi dovremmo dire anche privato – ed allo stesso tempo anche il suo limite (sicurezza giuridica rispetto al potere); e la sicurezza giuridica riferita al diritto stesso ("sicurezza nel diritto"), intesa non solo come garanzia della certezza e conoscibilità del diritto, ma anche il rispetto della procedura di formazione della norma da parte del legislatore[91].

Tuttavia, oltre all'aspetto di conformità formale dell'azione pubblica all'ordinamento, emerge anche il profilo decisionale – di ispirazione *schmittiana* – relativo alla scelta del decisore politico per motivi di sicurezza relativa non solo allo strumento più opportuno, ma anche al bilanciamento degli interessi che determinano il contenuto della decisione e, ancora prima, al "se" intervenire.

La dottrina ha già avuto modo di evidenziare, in relazione all'ordinamento italiano, come la sicurezza (nazionale) sia collocata in questo limbo tra politico e giuridico, data la carenza di una sua definizione[92].

Relativamente alle cybersicurezze, sia il legislatore italiano sia quello europeo hanno provveduto a definire questi concetti, e in entrambe le ipotesi lo hanno fatto con un implicito rinvio alle norme tecniche di sicurezza informatica e delle informazioni.

Considerato quanto appena accennato sulla sicurezza in generale, riteniamo che l'intervento della normazione tecnica nella disciplina delle cybersicurezze rappresenti una chiara evoluzione dello schema appena tracciato, ove oltre al potere "politico" e a quello "giuridico" si aggiunge anche quello "tecnico" che non possiamo più considerare neutrale.

Come evidenziato, si tratta di regole espressione di interessi privati di cui si osserva da tempo un utilizzo anche in settori di interesse pubblico[93], come in questo caso quello della sicurezza.

Precisiamo tuttavia che dall'analisi delle recenti discipline europee nel settore digitale, vedi il recente *IA Act*[94], emerge come l'Unione abbia posto attenzione su un particolare tipo di norma tecnica ossia la norma armonizzata che, come anticipato (par. 3), diversamente dalle altre norme tecniche, non è creata per volere degli stakeholder privati, ma è formulata dagli enti di normazione europei (CEN, CENELEC ed ETSI) su richiesta della Commissione europea. I tre enti europei possono anche rifiutare di adempiere a detta richiesta ma, qualora accettino, sono obbligati a rispettare il contenuto e i vincoli in essa contenuti. La Commissione si riserva a tal proposito di esercitare un ampio potere di controllo su tali enti, sia durante la fase di formulazione della norma, sia in fase di approvazione della stessa.

Riteniamo che con questa tipologia di norma l'Unione europea stia cercando di veicolare – come già intuito dalla definizione di cybersicurezza

89. Mosca 2012, p. 21.

90. Amato 2023, p. 162.

91. Peces Barba Martinez 1993, p. 226 ss. V. anche Pistorio 2021.

92. Valentini 2023, p. 60 ss., nonché Valentini 2017.

93. Shen–Faure 2021; Garcia 2011.

94. Volpato 2024.

europea – la normazione tecnica verso fini pubblici perseguendo obiettivi politici.

Considerati gli orientamenti interpretativi animati da diffidenza verso il progresso tecnologico, e le allusioni a futuri scenari tecno-deterministici[95] o tecnocratici[96] , ove l'umanità è passivamente relegata a subire gli effetti negativi di tali sviluppi in quanto la legge è troppo lenta per inseguire la tecnologia, riteniamo che il connubio norma giuridica e normazione tecnica costituisca certamente una via con la quale una istituzione pubblica come la Commissione europea, rappresentante interessi non solo particolari, possa regolare e guidare la tecnologia senza tuttavia arrestarne il libero sviluppo. Difatti «le norme non riguardano il *ritmo* ma la *direzione* dell'innovazione»[97].

Sorge tuttavia un problema di fondo circa la tutela delle garanzie. Sebbene a partire dalla sentenza *James Elliott Construction* del 2016 la Corte di giustizia abbia giudicato le norme armonizzate come parte integrante del diritto dell'Unione e, da ultimo, con la sentenza *Public.Resource.Org* del marzo 2024, la Corte ne abbia riconosciuto la gratuità e piena accessibilità al pubblico, è ancora dubbia la possibilità di poter far valere i diritti eventualmente lesi da dette norme con un ricorso giurisdizionale diretto avverso una norma armonizzata.

Considerata la sicurezza come limite ai diritti e alle libertà sulla base di un delicato bilanciamento giustiziabile nei profili della proporzionalità e ragionevolezza, sorgono quindi perplessità – allo stato attuale – circa l'utilizzo di detti strumenti per la tutela di interessi pubblici. Inoltre, come è stato rilevato in recente dottrina[98], si ravvisa una certa difficoltà da parte degli enti di normazione nel collaborare per la redazione delle norme tecniche nel settore della cybersicurezza, con il pericolo che ciò possa dar vita a sovrapposizioni o inutili ripetizioni che inficiano i principi di unificazione e coerenza della normazione tecnica[99], e che di conseguenza potrebbero incidere negativamente sulla corretta realizzazione ed esecuzione di politiche di cybersicurezza e cyberresilienza dettate dalla norma giuridica.

95. Il giusfilosofo Ugo Pagallo, in Pagallo 2014, spiega le tesi tecnodeterministe facendo cenno al noto paradosso di Zenone su Achille e la tartaruga, ove tuttavia in questo caso è la tartaruga, cioè il diritto, a non riuscire a raggiugere il piè veloce Achille, cioè la tecnologia. Difatti, le tesi tecno-deterministe assegnano al progresso tecnologico un assoluto potere incontrastabile al punto che «la corsa della tecnologia sarebbe troppo imperiosa e potente, per poter essere fermata da una semplice sentenza o editto» (*ivi*, p. 20), negando così la sussistenza di un rapporto dialettico tra diritto e tecnica. Esempio di tesi tecnodeterminista è la nota legge di Moore, la quale «a differenza delle leggi della fisica o della chimica, non è una vera e propria legge ma, piuttosto, è stata (ed è tuttora) una sorta di profezia che si auto-avvera; vale a dire una sfida, o un traguardo, che vede impegnati gli esperti nel ramo dei circuiti integrati e dei micro-processori in svariati laboratori del pianeta. […] La morale che si deve trarre da queste riflessioni è che possiamo accogliere la legge di Moore come un elemento cruciale dell'odierna rivoluzione tecnologica e, tuttavia, respingere le tesi estreme del tecno-determinismo» (*ivi*, p. 23).

96. Come distinto dalla magistrale dottrina di Natalino Irti, in Irti 2009, pp. 122-123, «non è arduo distinguere il tecnico dal tecnocrate: il tecnico non sceglie i fini, ma sta al servizio di fini decisi dagli altri, egli ha soltanto il potere conoscitivo dei mezzi; il tecnocrate, poiché attinge ed applica le leggi naturali dell'economia, ha il potere conoscitivo dei fini. Egli sa dove bisogna andare, e perciò rifiuta o spregia la decisione politica dei fini, i quali non sono – così argomenta – materia di disputa e di voto ma di conoscenza oggettiva e neutrale», ove per "neutralità" deve intendersi «estraneità al conflitto; e il conflitto – anche si argomenta – appartiene alla politica, e non alle leggi dell'economia, le quali, appunto come oggettive e neutrali, sono certe e incontrovertibili». In questo senso si rinvia alle ricostruzioni di Claude-Henri de Rouvroy, conte di Saint-Simon.

97. Floridi 2022, p. 86.

98. Kamara 2024.

99. In particolare, il riferimento è all'ETSI che era già stata oggetto di attenzioni da parte della Commissione europea nel documento *Una strategia dell'UE in materia di normazione Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale* pubblicato dalla Commissione europea nel febbraio 2022 (COM (2022) 31, 2 febbraio 2022) in merito alla procedura decisionale delineata nello statuto dell'ente, ritenuto non equilibrato. Pare infatti che questo conferisca a determinati interessi societari un potere di voto maggiore.

Riferimenti bibliografici

R. Abrahamsen, A. Leander (2016), *Handbook of private security studies*, Routledge, 2016

AGCOM (2024), *La neutralità della Rete*, aggiornata al 25 giugno 2024

G. Aliquò (2024), *Sicurezza pubblica e sicurezze private*, in "Polizia moderna", 9 gennaio 2024

G. Amato (2023), *Sicurezza, fra autorità e libertà*, in M. Valentini, G. Melis, "*Pro bono communi*. Scritti in onore di Carlo Mosca", Editoriale Scientifica, 2023

P. Andreini (1995), *La normativa tecnica tra sfera pubblica e privata*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di) (1995), *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, il Mulino, 1995

V. Antonelli, B.G. Mattarella (2022), *Carlo Mosca uomo della Costituzione*, Editoriale Scientifica, 2022

V. Bachelet (1966), *L'attività tecnica della pubblica amministrazione*, Giuffrè, 1966

R. Baldoni (2024), *Charting digital sovereignity. A survival playbook*, Independently published, 2024

A.L. Barabàsi (2014), *Linked. How everything is connected to everything else and what it means for business, science, and everyday life*, Basic books, 2014

N. Bobbio (2011), *Democrazia e segreto*, Einaudi, 2011

G. Bombelli (2017), *Dal moderno all'"ultramoderno"? Intorno al nesso diritto-tecnica-sicurezza*, in F. Pizzolato, P. Costa (a cura di), "Sicurezza e tecnologia", Giuffrè, 2017

P. Bourdeau (2013), *Resiliencism: premises and promises in securitisation research*, in "Resilience: International Policies, Practices, and Discourses", vol. 1, 2013, n. 1

M. Brutti (2017), Arcana imperii. *Sulla generalogia del segreto*, in L. Forni, T. Vettor (a cura di), "Sicurezza e libertà in tempi di terrorismo globale", Giappichelli, 2017

G. Caia, F.A. Roversi Monaco (1995), *Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

S. Calzolaio (2023), *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Castaldo (2019), *Dalla cyber defence alla cyber resilience dell'infrastruttura critica. Alcune implicazioni strategiche e organizzative*, in "Rivista di economia e politica dei trasporti", 2019, n. 3

V.G. Cerf (2012), *Internet Access Is Not a Human Right*, in "The New York Times", January 4, 2012

O.W. Cesarini (1929), *Il diritto dei privati*, Quodlibet, 1929

P.G. Chiara, R. Brighi (2024), *La dimensione della "resilienza" nel diritto UE della cybersicurezza*, in "Ragion pratica", 2024, n. 63

P. De Filippi, L. Belli (2014), *Network Neutrality: An Unfinished Debate,* in P. de Filippi, L. Belli, (a cura di), "Network Neutrality: an Ongoing Regulatory Debate", 2014

G. Della Morte (2018), Big data *e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale Scientifica, 2018

G. De Vergottini (2021), *Sicurezza e i diritti fondamentali*, in L. Efrén Ríos Vega, L. Scaffardi, I. Spigno (a cura di), "I diritti fondamentali nell'era della *digital mass surveillance*", Editoriale Scientifica, 2021

M.V. D'Onghia (2020), *Resilienza, una parola alla moda*, in "Treccani", 16 ottobre 2020

W.J. Drake, V.G. Cerf, W. Kleinwachter (2016), *Internet Fragmentation: An overview*, World Economic Forum, 2016

M. Dunn Cavelty, C. Eriksen, B. Scharte (2023), *Making cyber security more resilient: adding social considerations to technological fixes*, in "Journal of Risk Research", vol. 26, 2023, n. 7

ENISA (2012), *Shortlisting network and information security standards and good practices*, 2012

F. Esterbrook (1996), *Cyberspace and the Law of the Horse*, University of Chicago Legal Forum, 1996

B. Farrand, H. Carrapico (2018), *Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism*, in O. Bures, H. Carrapico (eds.), "Security Privatization. How non-security-related Private Businesses Shape Security Governance", Springer, 2018

C. Fjäder (2014), *The nation-state, national security and resilience in the age of globalisation*, in "Resilience: International Policies, Practices, and Discourses", vol. 2, 2014, n. 2

L. Fiorentino (2020), *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. Della Cananea, L. Fiorentino (a cura di), "I 'poteri speciali' del Governo nei settori strategici", Editoriale Scientifica, 2020

L. Floridi (2022), *Etica dell'intelligenza artificiale. Sviluppi, opportunità e sfide*, Raffaello Cortina Editore, 2022

V. Frosini (2010), *La democrazia nel XXI secolo*, Liberilibri, 2010

C. Gallotti (2022), *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione per la sicurezza delle informazioni. La norma ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*, Lulu press, 2022

L. Garcia (2011), *Governments, the Public Interest, and Standards Setting*, in L. DeNardis (ed.), "Opening Standards: The Global Politics of Interoperability," The MIT Press, 2011

A. Giddens (2000), *Il mondo che cambia. Come la globalizzazione ridisegna la nostra vita*, il Mulino, 2000

M. Gigante (1997), *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle «norme armonizzate»*, in "Rivista italiana di diritto pubblico comunitario", 1997, n. 1

N. Greco (1999), *Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale*, in AA.VV., "Crisi del diritto, produzione normativa e democrazia degli interessi", Edistudio, 1999

I. Kamara (2024), *European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience, Innovation*, in "Innovation: The European Journal of Social Science Research", 2024

P. Khanna (2016), *Connectography. Le mappe del futuro ordine mondiale*, Fazi, 2016

A. Iannuzzi (2018), *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, 2018

I. Inkster (ed.) (2008), *History of technology*, vol. 28, Continuum, 2008

N. Irti (2009), *L'ordine giuridico del mercato*, Laterza, 2009

N. Irti (2006), *Norma e luoghi*, Laterza, 2006

L. Lega (2023), *Sicurezza civile. Un sistema complesso che guarda alle crisi*, in M. Valentini, G. Melis, "*Pro bono communi*. Scritti in onore di Carlo Mosca", Editoriale Scientifica, 2023

M.G. Losano (2017), *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. Forni, T. Vettor (a cura di), "Sicurezza e libertà in tempi di terrorismo globale", Giappichelli, 2017

N. Lugaresi (1995), *Profili comparatistici della norma tecnica: l'esperienza francese dell'AFNOR*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

A. Monti (2023a), *Digital rights delusion: humans, machines and the technology of information*, Routledge, 2023

A. Monti (2023b), *Metaverso e convergenza tecnologica: aspetti (geo)politici, giuridici e regolamentari*, in G. Cassano, G. Scorza (a cura di), "Metaverso: diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini Giuridica, 2023

A. Monti (2020), *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema*, in "1° Quaderno Speciale CASD – Scenari globali e interessi nazionali: pandemia, continuità, cambiamento", 18 dicembre 2020

C. Mosca (2021), *La sicurezza. Valori, modelli e prassi istituzionali*, Editoriale Scientifica, 2021

C. Mosca (2012), *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Cedam, 2012

E. Nocifora (2010), *Sociologia della sicurezza, rischio e legalità democratica*, in AA.VV., "Sicurezza e democrazia", Scriptaweb, 2010

M. O'Mara (2019), *The Code: Silicon Valley and the Remaking of America*, Penguin Press, 2019

A. Oddenino (2008), *La governance di Internet fra autoregolazione, sovranità statale e diritto internazionale*, Giappichelli, 2008

U. Pagallo (2014), *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, 2014

A. Pansa (2019), *La sicurezza nazionale. Innovazione e nuovi limiti*, in "Gnosis", 2019, n. 1

P. Passaglia (2021), *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in "MediaLaws. Rivista di Diritto dei Media", 2021, n. 3

G. Peces Barba Martinez (1993), *Teoria dei diritti fondamentali*, Giuffrè, 1993

S. Peng (2015), *Standards as a Means to Technological Leadership? China's ICT Standards in the Context of the International Economic Order*, in L. Toohey, C.B. Picker, J. Greenacre (eds.), "China in the International Economic Order: New Directions and Changing Paradigms", Cambridge University Press, 2015

G. Pistorio (2021), *La sicurezza giuridica: profili attuali di un problema antico*, Editoriale Scientifica, 2021

O. Pollicino (2023), *Potere digitale*, Estratto da "I Tematici, V-2023 – Potere e Costituzione", in "Enciclopedia del diritto", 2023

O. Pollicino, M. Bassini, G. De Gregorio (2022), *Internet Law and Protection of Fundamental Rights*, Bocconi University Press, 2022

O. Ranelletti (1904), *La polizia di sicurezza*, in V.E. Orlando (a cura di), "Primo trattato completo di diritto amministrativo italiano", vol. IV, Società Editrice Libraria, 1904

M.A. Rizzi (2023), *L'evoluzione del panorama regolamentare cyber e l'avvento della Direttiva NIS2 nel settore delle telecomunicazioni*, in "Cyber Magazine – Cyber Think Tank Assintel", sett-ott. 2023

E. Rothschild (1995), *What is security?*, in "Daedalus", vol. 124, 1995, n. 3

G.M. Ruotolo (2014), *Internet (diritto internazionale)*, in "Enciclopedia del diritto", Annali VII, Giuffrè, 2014

F. Salmoni (2001), *Le norme tecniche*, Giuffrè, 2001

S. Sassen (2008), *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton University Press, 2008

G. Scandone (2023), *Il segreto di Stato e la difesa della Repubblica. L'insegnamento dei recenti eventi internazionali*, in M. Valentini, G. Melis, "*Pro bono communi*. Scritti in onore di Carlo Mosca", Editoriale Scientifica, 2023

G. Scandone (2008), *Il segreto di Stato*, in C. Mosca, G. Scandone, S. Gambacurta, M. Valentini, "I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)", Giuffrè, 2008

S.L. Schwarcz (2002), *Private Ordering*, in "Northwestern University Law Review", vol. 97, 2002, n. 1

A. Segura Serrano (2006), *Internet Regulation and the Role of International Law*, in "Max Planck Yearbook of United Nations Law", vol. 10, 2006

F. Serini (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in "Rivista italiana di informatica e diritto", 2023, n. 2

C. Shapiro, H.R. Varian (1999), *The Art of Standards Wars*, in "California Management Review", vol. 41, 1999, n. 2

Y. Shen, M. Faure (2021), *Private standards for the public interest? Evidence from environmental standardization in China*, in "Review of European, Comparative and International Environmental Law", vol. 30, 2021, n. 3

G. Shih, J. Menn (2023), *India targets Apple over its phone hacking notifications*, in "The Washington Post", December 27, 2023

H. Spang-Hassen (2006), *Public International Computer Network Law Issues*, Djoef Publishing, 2006

UNI – Ente Nazionale Italiano di Unificazione (2012), *Le regole del gioco*, UNI, 2012

R. Ursi (2022), *La sicurezza pubblica*, il Mulino, 2022

B. Valensise (2020), *I settori strategici dopo la Riforma*, in G. Della Cananea, L. Fiorentino (a cura di), "I 'poteri speciali' del Governo nei settori strategici", Editoriale Scientifica, 2020

M. Valentini (2023), *Sicurezza della Repubblica tra politico e giuridico* (prima parte), in "Amministrazione Pubblica. Rivista di Cultura Istituzionale dei Funzionari dell'Amministrazione Civile dell'Interno", 2023, n. 113

M. Valentini (2017), *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Editoriale Scientifica, 2017

A. Volpato (2024), *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in "Quaderni AISDUE", fasc. speciale, 2024, n. 2

J. Walker, M. Cooper (2011), *Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation*, in "Security Dialogue", vol. 42, 2011, n. 2

X. Wang (2019), *The Great Firewall of China and Its Implications for Political Information Systems*, 2019

T.A. Williams, D.A. Gruber, K.M. Sutcliffe et al. (2017), *Organizational response to adversity: Fusing crisis management and resilience research streams*, in "Academy of Management Annals", vol. 11, 2017, n. 2