RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

diretta da Sebastiano Faro e Marina Pietrangelo

Anno II, n. 2/2020 • Periodicità semestrale
Direzione e Redazione: Istituto di Informatica Giuridica e Sistemi Giudiziari • Via dei Barucci 20 - 50127 Firenze

2
2020

Consiglio Nazionale delle Ricerche

Rivista italiana di informatica e diritto
Periodico internazionale del CNR-IGSG
Anno II • n. 2/2020 • Periodicità semestrale

Direzione
Sebastiano Faro e Marina Pietrangelo

Comitato di direzione
Federigo Bambi, Davide Carnevali, Gian Luca Conti, Rosa Maria Di Giorgi, Elio Fameli, Enrico Francesconi Erik Longo, Elisabetta Marinai, Stefano Pietropaoli, Francesco Romano, Giancarlo Taddei Elmi

Comitato scientifico nazionale
Laura Abba, Agata C. Amato Mangiameli, Andrea Cardone, Antonio Carcaterra, Paolo Caretti, Massimo Carli, Enrico Carloni, Adriana Ciancio, Renato Clarizia, Giuseppe Corasaniti, Pasquale Costanzo, Giovanna De Minico, Carla Faralli, Giusella Finocchiaro Tommaso E. Frosini, Mario Jori, Donato A. Limone, Aldo Loiodice, Luigi Lombardi Vallauri, Nicola Lupo, Nicoletta Maraschio, Paolo Moro, Monica Palmirani, Ugo Pagallo Giovanni Pascuzzi, Dianora Poletti, Oreste Pollicino, Giovanni Sartor, Andrea Simoncini Carlo Sorrentino, Lara Trucco, Stefano Trumpy, Alessandra Valastro, Franco Vallocchia Giovanni Ziccardi

Comitato scientifico dei corrispondenti stranieri
Y. Amoroso (C), T.J.M. Bench Capon (GB), D. Bourcier (F), W. 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. Maclntosh (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)

Comitato dei revisori esperti per la valutazione
Fulvia Abbondante, Enrico Albanesi, Maria Romana Allegri, Marco Bassini, Raffaella Brighi, Elda Brogi, Simone Calzolaio, Giuseppe Cammarota, Gianluigi Ciacci, Sofia Ciuffoletti, Maria Vittoria Dell'Anna, Fabio Dell'Aversana, Rossana Ducato, Paolo Galdieri, Riccardo Gualdo, Paolo Guarda, Antonio Iannuzzi, Alessandro Lovari, Daniele Marongiu, Paola Marsocci, Letizia Materassi, Erica Palmerini, Saulle Panizza, Anna Papa, Paolo Passaglia, Viviana Patti, Giovanni Piccirilli, Benedetto Ponti, Cecilia Robustelli, Andrea Rossetti, Simone Scagliarini, Caterina Sganga, Giuseppe Vaciago, Giulia Venturi

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
telefono 055 43995 • fax 055 4399605 • RivistaRIID@igsg.cnr.it
www.rivistaitalianadiinformaticaediritto.it/index.php/RIID

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

Indice

Studi e Ricerche

5 **Juan Sebastien Vanegas**
La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR

15 **Antonio A. Martino**
Chi teme i giudici robot

Note e Discussioni

27 **Serena Vantin**
La lama nella rete. Forme della violenza contro le donne sul web

35 **Tonye Clinton Jaja, Chantal Lamarre**
Application of information communication technology (ICT) to legislative drafting: case studies of legislative drafting assistant softwares in Nigeria and Canada

Recensioni

43 **Maria Romana Allegri**
Oltre la par condicio. Comunicazione politico-elettorale nei social media, fra diritto e autodisciplina, Milano, Franco Angeli, 2020

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

ISSN 2704-7318
Fascicolo 2-2020
DOI: 10.32091/RIID0020

La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR

Juan Sebastien Vanegas*

Allineare le misure di sicurezza informatica ai requisiti previsti dall'articolo 32 del GDPR costituisce una delle difficoltà principali che le organizzazioni devono affrontare nei loro processi di conformità complessiva al GDPR. Tale difficoltà è certamente giustificata da alcune criticità proprie del tema specifico delle misure di sicurezza, come ad esempio il vastissimo ambito in cui esse sono implementate, la grande diversità di misure implementabili e il necessario coinvolgimento di diverse figure professionali. L'articolo 32, inoltre, non precisa quali misure debbano essere implementate, né tantomeno quali misure possano considerarsi adeguate, ma si limita a fornire un elenco non esaustivo di possibili misure. Pertanto, un'analisi della giurisprudenza delle autorità di controllo europee può rappresentare un utile contributo sia per individuare con precisione le misure informatiche ritenute inadeguate (anche al fine di verificare l'applicazione uniforme dei criteri di sicurezza) che per accompagnare gli operatori di settore nei loro processi di conformità. Per raggiungere tale obiettivo, sono state analizzate diverse decisioni emesse da autorità di cinque paesi (Italia, Regno Unito, Spagna, Francia e Danimarca), e le vulnerabilità rilevate sono state raggruppate in macrocategorie: *accountability*, gestione degli accessi, utilizzo di applicazioni obsolete e protezione dei dati. Il quadro che emerge dall'analisi è un approccio sostanzialmente uniforme da parte delle autorità di controllo, le quali sembrano concordare sia sul carattere inadeguato di alcune misure rilevate sia sul carattere adeguato di misure alternative discusse nei provvedimenti. L'interesse sul tema potrebbe d'altronde essere esteso in un futuro lavoro all'analisi delle politiche sanzionatorie e correttive adottate dalle autorità.

GDPR – Misure di sicurezza – *Compliance* – Europa

Sommario: *1. Introduzione – 2.* Accountability *e sicurezza informatica – 3. Gestione degli accessi – 4. Utilizzo di applicazioni obsolete o non aggiornate – 5. La sicurezza dei dati – 6. Conclusioni*

1. Introduzione

Secondo un sondaggio condotto da una prestigiosa società, la difficoltà principale incontrata dalle imprese nel processo di adattamento al Regolamento (UE) 2016/679 (il "GDPR") è stata quella di allineare le proprie misure di sicurezza, predisposte a tutela dei dati personali trattati, ai parametri stabiliti dall'articolo 32 del GDPR[1]. Tale articolo, come noto, richiede ai titolari e ai responsabili del trattamento di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza del trattamento adeguato al rischio[2]. Se questo è vero, il recente anniversario dei due anni di entrata in vigore del GDPR rappresenta dunque una buona occasione sia per ripercorrere rapidamente le principali vulnerabilità informatiche rilevate fino ad oggi dalle autorità di controllo europee, sia per analizzare nel merito i corrispondenti provvedimenti correttivi e sanzionatori adottati da quest'ultime. Per

*J.S. Vanegas è collaboratore presso lo studio Eversheds-Sutherland, LL.M. Queen Mary College, Master Protezione dei Dati Personali Università di Roma Tre. L'Autore ringrazia per i preziosi commenti il prof. Andrea Rossetti, professore associato di filosofia del diritto all'università Bicocca di Milano, e gli avvocati Massimo Maioletti e Andrea Zincone. Le valutazioni espresse nel presente articolo sono esclusivamente dell'Autore.

contestualizzare storicamente la normativa oggetto della presente analisi, si ricorda che il GDPR ha sostituito il precedente regime fondato sulla direttiva 95/46/CE, il cui articolo 17 disciplinava gli obblighi di sicurezza del trattamento dei dati personali[3]. Benché la Commissione Europea abbia affermato nel memorandum esplicativo sul GDPR la sostanziale continuità normativa fra l'articolo 32 del GDPR e l'articolo 17 della direttiva 95/46/CE[4], quest'ultima è stata a suo tempo recepita dagli Stati membri con formulazioni e tecniche diverse. Ad esempio, mentre le leggi di recepimento francesi[5] e britanniche[6] avevano replicato nei rispettivi ordinamenti il requisito dell'adeguatezza delle misure di sicurezza, la legge italiana[7] aveva ulteriormente precisato tale requisito, tipizzando[8] per legge specifiche misure tecniche minime di sicurezza[9].

Da tale diversità di regime nazionale[10] è conseguita ovviamente una diversità di giurisprudenza amministrativa sulla sicurezza del trattamento: mentre alcune decisioni rese dalle autorità francesi e britanniche sulla base del regime anteriore possono ancora essere utilmente analizzate per precisare il contenuto dei requisiti di sicurezza previsti dal GDPR, tanto non può dirsi delle decisioni rese dall'autorità italiana, in quanto fondate su criteri specifici e tipizzati non più previsti dal GDPR[11]. Pertanto, nel presente articolo, oltre alle decisioni rese in vigenza del GDPR, verranno analizzate anche alcune decisioni rese nella vigenza del regime precedente, ma solo nella misura in cui sono idonee a precisare il concetto di adeguatezza previsto dall'articolo 32 del GDPR.

Fatta questa breve premessa storica, per delineare invece il contesto attuale nel quale si colloca la questione dell'adeguatezza delle misure di sicurezza, è utile ricordare una serie di difficoltà, sia pratiche che di natura legale, proprie di questa particolare tematica.

Innanzitutto, dal punto di vista legale, sin dalla pubblicazione del GDPR[12], l'interpretazione dei requisiti di sicurezza è apparsa particolarmente difficoltosa in ragione delle variabili cui il criterio di adeguatezza è sottoposto, che qui brevemente si richiamano: (i) lo stato dell'arte; (ii) i costi di attuazione (delle misure di sicurezza); (iii) la natura, l'oggetto, il contesto e le finalità del trattamento e (iv) il rischio di varia probabilità e gravità di compressione o violazione dei diritti e delle libertà delle persone fisiche. Naturalmente, l'eccessiva apertura e indeterminatezza di detti criteri mal si concilia con la necessità di certezza e precisione di cui gli esperti di sicurezza hanno bisogno nella fase di *design*, d'implementazione e di *auditing* delle misure di sicurezza. Inoltre, non tutte le autorità di controllo europee hanno intrapreso iniziative finalizzate ad accompagnare pienamente gli operatori nei loro processi di *compliance*[13] come, ad esempio, la pubblicazione di linee guida a carattere tecnico. Né, sino ad oggi, i provvedimenti emessi dalle varie autorità europee sono stati particolarmente illuminanti, stante l'assenza di uniformità nelle modalità di redazione, di dettagli tecnici relativi alle vulnerabilità di volta in volta rilevate, di indicazioni uniformi sui criteri utilizzati per valutare la gravità delle infrazioni, e di dettagli circa le misure correttive imposte alle organizzazioni. Tali fattori, sommati alla scarsa reperibilità dei testi delle decisioni in inglese, rendono l'analisi complessiva del merito delle decisioni particolarmente difficoltosa, anche nella prospettiva di un'interpretazione e applicazione uniforme dei criteri di sicurezza del trattamento dei dati personali da parte delle stesse autorità di controllo europee.

Per quanto riguarda, invece, le difficoltà pratiche, è necessario ricordare il vastissimo ambito applicativo delle misure di sicurezza richieste dal GDPR, che coinvolgono l'ambito informatico, quello organizzativo e quello fisico. La presente analisi si concentra particolarmente sulle misure informatiche, ma è opportuno precisare che le autorità di controllo attribuiscono pari importanza alle misure organizzative[14] e fisiche[15]. Inoltre, è necessario tenere presente che nel campo della sicurezza informatica la componente umana è di importanza fondamentale: come noto, una larga parte[16] di violazioni informatiche ha origine dallo sfruttamento di una vulnerabilità umana[17]. Pertanto, l'efficacia delle misure informatiche dipende in buona parte anche dall'implementazione di solide misure organizzative[18].

Un ulteriore elemento potenzialmente foriero di problematiche è poi dato dal fatto che l'individuazione e l'implementazione di misure di sicurezza informatiche coinvolge necessariamente figure professionali con competenze e approcci diversi e sovente impreparate a comprendere il linguaggio, il metodo e le esigenze altrui, rendendo dunque non agevole la collaborazione e il lavoro di sintesi. Tale contesto è aggravato dalla grande diversità di misure di sicurezza informatiche astrattamente implementabili, come, ad esempio, le misure relative alla rete, le misure di protezione delle applicazioni e le misure relative alla protezione dei dati archiviati o in trasmissione.

Infine, vale la pena aggiungere che il concetto di "sicurezza assoluta" di un sistema informatico è quantomeno utopistico. Il continuo sviluppo delle tecnologie, l'aggiornamento dei software, e i test costanti cui sono sottoposte le misure di sicurezza comportano, inevitabilmente, la scoperta di vulnerabilità e, quindi, la violazione di sistemi ritenuti fino a quel

momento "sicuri". Da un punto di vista giuridico, tale problematica sembra richiamare l'utilità della distinzione fra obbligazioni di mezzo e obbligazioni di risultato ai fini dell'accertamento e dell'imputazione di responsabilità civili e amministrative connesse a violazioni di sicurezza, questione certamente importante in ragione del costante aumento di dati compromessi[19].

Nonostante queste difficoltà, è anche opportuno sottolineare che l'implementazione di misure di sicurezza appropriate non consente solamente il rispetto dei requisiti di sicurezza previsti dalla normativa in tema di dati personali, ma anche di proteggere dati aziendali non personali. Pertanto, i costi di implementazione dovrebbero essere considerati anche come un investimento a tutela del business dell'organizzazione, e non solo come un semplice costo di *compliance*.

Tanto premesso, a due anni dall'entrata in vigore del GDPR è finalmente possibile tracciare un primo quadro delle azioni poste in essere dalle autorità di controllo dei vari paesi europei riguardo le misure di sicurezza informatiche. Come messo in luce da una recente decisione emessa nei confronti di una primaria compagnia aerea dall'ICO[20], autorità di controllo britannica, il percorso verso una protezione informatica adeguata sembra essere ancora lungo: tale decisione, infatti, ha sanzionato una serie di vulnerabilità di sicurezza particolarmente gravi ed in ambiti molto diversi, come ad esempio il controllo degli accessi, la protezione della rete, la cifratura dei dati e l'obsolescenza dei software e delle applicazioni, tanto da rappresentare un caso paradigmatico di mancanza di *compliance* rispetto ai requisiti di sicurezza previsti dalla normativa in tema di protezione dei dati personali.

L'obiettivo del presente articolo è quindi di analizzare analiticamente ma senza pretesa di esaustività le più comuni tipologie di vulnerabilità riscontrate dalle autorità europee, raggruppandole in quattro macrocategorie ed evidenziandone la gravità.

2. *Accountability* e sicurezza informatica

Per quanto si possa ritenere che l'*accountability*, espressamente prevista dall'articolo 5(2) e dall'articolo 24 del GDPR, e principio cardine della normativa sulla protezione dei dati personali[21], non costituisca una misura di sicurezza in sé, essa costituisce nondimeno un principio base attorno al quale qualsiasi misura di sicurezza, sia essa di natura tecnica o organizzativa, dovrebbe essere implementata. In ragione della sua importanza, è dunque opportuno richiamarne le principali caratteristiche.

Come noto, l'*accountability* è composta da due distinti adempimenti cumulativi: il primo è costituito dal rispetto di una disposizione, il secondo dalla capacità del titolare del trattamento di dimostrarne il rispetto[22]. Pertanto, per conformarsi a questo principio, il titolare del trattamento è di regola chiamato a predisporre e conservare una grande quantità di documenti e, dunque, a tenere un comportamento attivo[23]. Estendendo l'*accountability* all'ambito della sicurezza informatica, il primo adempimento sarà costituito dalla predisposizione e dall'implementazione di misure di sicurezza "adeguate", ai sensi dell'articolo 32 GDPR, mentre il secondo riguarderà la capacità di dimostrare l'adeguatezza di tali misure.

Prima di analizzare dettagliatamente i due adempimenti, occorre premettere che, come rilevato dall'ICO, la predisposizione di misure di sicurezza richiede la conoscenza da parte del titolare dell'architettura informatica implementata e, in particolare, il luogo e il supporto su cui sono custoditi i dati personali, informazione senza la quale è probabile che le misure implementate risultino inadeguate[24]. Tale conoscenza, che può apparire ovvia, non è purtroppo scontata, in particolar modo in organizzazioni complesse, dove può accadere che dispositivi informatici accesi o servizi attivi vengano "dimenticati" per lunghi periodi di tempo.

Quindi, considerando il criterio dell'adeguatezza di ciascuna misura di sicurezza, un sistema informatico non è più forte del suo componente più vulnerabile come una catena non è più forte del suo anello più debole. Infatti, una singola vulnerabilità è sufficiente a causare una violazione di dati personali[25]. Pertanto, l'articolo 32(1)(d) del GDPR richiede al titolare del trattamento di mettere in atto «una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento». Tra le tante misure possibili, in ambito informatico le autorità di controllo richiedono in particolare l'implementazione di misure di *auditing*[26] o, più nel dettaglio, *vulnerability scan* e *penetration test*[27].

Invece, per quanto attiene al requisito della dimostrazione dell'adeguatezza delle misure, il vantaggio dei sistemi e dei programmi informatici è che, *by default*, producono (o possono produrre) una grande quantità di informazioni riguardo il loro funzionamento (detti *log*). Allora, il comportamento richiesto al titolare è quello di impostare e conservare correttamente i messaggi di *log*. Come si vedrà più nel dettaglio, è importante che ciascuna misura di sicurezza produca *log* e che, in presenza di una infrastruttura informatica di grandi dimensioni, il titolare si doti di aggregatori di messaggi di *log*[28] al fine di avere co-

stantemente una panoramica d'insieme sul corretto funzionamento dei propri sistemi e programmi.

a) La conduzione di *vulnerability scan*

La conduzione di *vulnerability scan* permette ad un'organizzazione di identificare vulnerabilità di dominio pubblico[29] presenti sui propri sistemi, e costituisce uno strumento di sicurezza imprescindibile per organizzazioni di grandi dimensioni o per quelle che hanno server accessibili da Internet e che, dunque, espongono dati al pubblico. Infatti, è stato espressamente statuito che la conduzione di *vulnerability assessments* contribuisce ad assicurare un livello costantemente adeguato di protezione dei dati personali[30], e che l'assenza o l'inadeguatezza degli *scan* comporti un aumento dei rischi legati alla sicurezza dei dati[31].

Secondo l'ICO e il Garante italiano, i *vulnerability scan* dovrebbero essere effettuati regolarmente, ed, in ogni caso, a seguito di cambiamenti importanti[32]. Ovviamente, l'ICO ha giudicato non sufficiente un lasso di tempo di tre anni fra due test perché «in considerazione della quantità e della natura dei dati personali conservati da Cathay Pacific, e della velocità con la quale le minacce di cybersecurity si evolvono e diventano più sofisticate, questo è un periodo ingiustificatamente lungo senza un penetration test»[33].

b) La gestione dei messaggi di *log*

La conservazione e l'analisi dei messaggi di *log* costituisce una misura di sicurezza essenziale in quanto non solo permette al titolare di essere sempre a conoscenza degli eventi che si verificano nei propri sistemi (ad esempio, accessi o operazioni compiute dagli utenti)[34], ma soprattutto di essere sempre in grado di dimostrare l'adeguatezza delle misure di sicurezza implementate. Conseguentemente, la registrazione e la conservazione dei *log* è espressamente richiesta in diversi provvedimenti settoriali emanati dalle autorità di controllo[35]. In assenza di *log* non è possibile individuare vulnerabilità, né per quanto riguarda il titolare, né per quanto riguarda le autorità di controllo[36]. Inoltre, in assenza di *log*, non è possibile analizzare ex post le modalità di un attacco[37] e, soprattutto, le conseguenze con riguardo ai dati personali conservati. Pertanto, l'incertezza causata dall'assenza di *log* crea un rischio di sicurezza[38] come stabilito dal Garante, secondo il quale «il mancato completo tracciamento degli accessi al database [...] configura la violazione [...] dell'obbligo di assicurare più adeguate garanzie di riservatezza agli iscritti alla piattaforma medesima»[39].

Perciò, come ogni dato, e soprattutto nella misura in cui contengano dati personali, anche i *log* devono essere adeguatamente conservati e protetti. Ad esempio, secondo il Garante, l'inclusione nei *log* di informazioni non indispensabili per finalità di controllo e sicurezza può determinare una duplicazione di dati e quindi l'incremento del rischio di trattamento illecito[40].

3. Gestione degli accessi

Una seconda violazione delle misure di sicurezza frequentemente riscontrata dalle autorità di controllo riguarda la gestione degli accessi (c.d. *access control*). È opportuno notare che tale misura non è di natura esclusivamente informatica, ma, in primo luogo, di tipo organizzativo. Una corretta gestione degli accessi permette di limitare l'accesso a determinati dati (tra cui ovviamente anche dati personali) unicamente agli utenti che ne hanno bisogno per il compimento delle proprie funzioni o necessità. Inoltre, è opportuno notare che la gestione degli accessi non compie distinzioni tra categorie di persone che accedono ad un dato, e si applica tanto ad utenti interni ad un'organizzazione (come, ad esempio, dipendenti e consulenti) quanto ad utenti esterni (fornitori, clienti o semplici visitatori).

a) L'autenticazione degli utenti

In caso di controlli di accesso interni, l'autenticazione presuppone, di regola, che ciascun utente di un sistema sia dotato di un proprio account individuale, specialmente quando tale utente abbia responsabilità aziendali particolari. Tramite l'autenticazione è infatti possibile ricondurre con certezza le azioni compiute dall'account all'utente, facilitando il rispetto del principio di *accountability*. La connessione fra autenticazione e *accountability* è stata sottolineata dal Garante italiano, per il quale «la condivisione delle credenziali impedisce di attribuire le azioni compiute in un sistema informatico a un determinato incaricato, con pregiudizio anche per il titolare, privato della possibilità di controllare l'operato di figure tecniche così rilevanti»[41]. In conseguenza, «l'avvenuta condivisione delle credenziali di autenticazione tra più soggetti legittimati alla gestione della piattaforma rappresent[a] una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate»[42]. Tale adempimento è, d'altra parte, incluso negli standard di sicurezza pubblicati dalle organizzazioni internazionali più prestigiose[43], e non richiede alcun costo aggiuntivo, poiché la maggior parte dei sistemi e applicativi informatici prevedono la possibilità di creare e gestire facilmente i profili di autenticazione degli utenti.

In caso di accesso esterno, occorre che l'utente sia autenticato in modo corretto. Può accadere che un'errata o mancata configurazione di un'applicazio-

ne permetta la messa a disposizione di dati riservati a terzi non autorizzati (o, peggio ancora, al pubblico). La Commission Nationale Informatique & Libertés (CNIL), autorità di controllo francese, ha avuto modo di affrontare due casi di configurazione errata di un'applicazione web (di una società assicurativa in un caso, e di gestione immobiliare nell'altro) che consentiva l'accesso a dati personali contenuti in aree clienti riservate a terzi non autorizzati. Dopo aver ricordato che «quando una richiesta di accesso a una risorsa è indirizzata ad un server, quest'ultimo deve verificare che il richiedente sia autorizzato ad accedere alle risorse richieste»[44], la CNIL ha qualificato tali accessi non autorizzati come violazione grave delle norme di sicurezza in quanto astrattamente sfruttabile da qualunque persona, anche non esperta in informatica.

È quindi nell'ambito delle modalità di autenticazione che sembra possibile rilevare un primo disallineamento fra i requisiti di sicurezza ritenuti adeguati dalle diverse autorità di controllo europee. Premesso che ai fini di un'autenticazione sicura può essere opportuno prevedere più di un fattore di autenticazione[45], come d'altronde già previsto da alcune normative settoriali[46], i requisiti di robustezza delle password individuati dalle diverse autorità non sembrano pienamente corrispondere. Infatti, se l'autorità italiana stabilisce che la lunghezza minima di una password debba essere di 8 caratteri, con un controllo automatico di qualità che impedisca l'uso di password costituite da parole reperibili in dizionari[47], l'autorità francese, in assenza di un sistema di autenticazione in grado di prevenire attacchi *brute-force*, richiede una lunghezza minima di 12 caratteri alfanumerici, con carattere maiuscolo, minuscolo e un carattere speciale[48]. Ancor diversamente, secondo le linee guida dell'autorità britannica, la lunghezza minima della password dovrebbe essere di 10 caratteri, senza necessariamente richiedere un carattere speciale. Tale difformità applicativa, seppur minima e priva di conseguenze particolari, dimostra nondimeno la possibilità astratta che possano in futuro verificarsi nuovamente divergenze su requisiti tecnici specifici. Al fine di assicurare uniformità di applicazione, il buon funzionamento del meccanismo di cooperazione e coerenza previsto dal GDPR[49] sarà di fondamentale importanza al fine di evitare tali asimmetrie applicative[50].

In ogni caso, l'assegnazione di account individuali o l'autenticazione di un utente costituisce solo una prima misura di sicurezza, che deve essere naturalmente seguita dall'individuazione delle categorie di dati accessibili dagli account rilevanti, e, dunque, dalle autorizzazioni assegnate.

b) L'autorizzazione degli utenti

La necessità di prevedere autorizzazioni specifiche (quantomeno interne ad un'organizzazione) emerge implicitamente[51] dall'articolo 29 GDPR, ai sensi del quale chi agisce sotto l'autorità del titolare o del responsabile non può trattare dati personali se non è istruito in tal senso.

Tale misura di sicurezza consente di restringere l'accesso ai soli dati essenziali per i quali viene effettuato l'accesso, ed è importante quanto l'autenticazione, in quanto quest'ultima sarebbe inutile se tutti gli utenti fossero autorizzati ad accedere a tutti i dati, circostanza che, secondo la CNIL, costituisce una violazione dell'art. 32 del GDPR[52]. In maniera similare, secondo il Garante italiano, la mancata implementazione di sistemi di autorizzazione integra la violazione dell'articolo 5(1)(f) del GDPR[53].

A livello informatico, l'autorizzazione all'accesso a dati viene di regola impostata sulla base dell'appartenenza di un utente ad un determinato gruppo[54], ma altre tecniche possono essere implementate, come ad esempio la restrizione di accesso al di fuori di determinati orari[55]. Secondo il Garante italiano, «la mancata definizione e configurazione dei differenti profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari nei diversi ambiti di operatività»[56] configura una violazione dell'obbligo di predisposizione di misure tecniche adeguate.

Ovviamente, lo scopo dell'autorizzazione può essere vanificato ove troppi utenti vengano autorizzati ad accedere a documenti sensibili o quando utenti siano dotati di autorizzazioni particolarmente ampie, fenomeno che tende a verificarsi frequentemente in particolar modo con riguardo a profili di amministratori di sistema[57] (spesso per comodità e rapidità di assistenza ed intervento a distanza). Secondo l'ICO, pertanto, occorre valutare il rischio di aggiungere utenti al gruppo di amministratori di dominio e mantenere un numero limitato di autorizzazioni.

4. Utilizzo di applicazioni obsolete o non aggiornate

Una terza categoria di vulnerabilità affrontata dalle autorità di controllo riguarda l'utilizzo di applicazioni non aggiornate o obsolete. Può accadere che successivamente al rilascio di un'applicazione vengano scoperte vulnerabilità[58] che rendono le applicazioni non sicure. In tali casi, solitamente gli sviluppatori rilasciano un aggiornamento che, una volta installato, corregge la vulnerabilità identificata. Se l'aggiornamento non viene effettuato, il sistema rimane estremamente vulnerabile, non solo perché presenta una vulnerabilità, ma soprattutto

perché quest'ultima diventa di dominio pubblico e, dunque, facilmente sfruttabile da un grande numero di malintenzionati.

Al termine del ciclo vita di un'applicazione, gli aggiornamenti di sicurezza vengono sospesi dallo sviluppatore ed in conseguenza qualsiasi vulnerabilità successivamente individuata non viene di regola più corretta. Pertanto, l'applicazione, benché ancora utilizzabile rimane vulnerabile, a meno che sviluppatori interni procedano autonomamente alla sua manutenzione, cosa di regola dispendiosa e riservata a personale esperto.

a) Utilizzo di applicazioni non aggiornate

Il continuo aggiornamento delle applicazioni costituisce una misura di sicurezza idonea a correggere vulnerabilità di volta in volta rese note al pubblico e corrette dagli sviluppatori. Per dare un'idea della frequenza con cui dovrebbero essere aggiornati i sistemi, l'ICO ha rilevato in un procedimento sanzionatorio che in un periodo di 8 mesi sono stati rilasciati 17 aggiornamenti che risolvevano vulnerabilità note per un server, e che se il titolare avesse implementato una gestione delle *patch* più efficace, gli hacker avrebbero avuto meno opportunità di sfruttare tali vulnerabilità[59]. A dire il vero, emerge dai provvedimenti analizzati una grave negligenza da parte dei titolari che risulta a volte da vulnerabilità presenti nei sistemi IT addirittura per più di 4 anni[60]. Pertanto, se necessario, in aggiunta alla regolare installazione di *patch* e aggiornamenti, può essere opportuno implementare una procedura di tipo organizzativo che permetta di verificare il regolare e corretto svolgimento di tali operazioni[61].

b) Utilizzo di applicazioni obsolete

L'assenza di aggiornamenti di sicurezza per applicazioni o sistemi obsoleti crea un rischio aggiuntivo di sicurezza che rende tali sistemi un obbiettivo ovvio per degli *hacker*[62].

Ove venissero usate applicazioni obsolete, pertanto, il rischio di compromissione di un sistema IT[63] sarebbe incrementato, perché, in assenza di supporto da parte degli sviluppatori ufficiali, sarebbe necessario l'intervento ad hoc degli sviluppatori del titolare del trattamento per correggere le vulnerabilità eventualmente individuate, che, però, potrebbe non essere tempestivo[64]. Perciò, anche l'utilizzo di applicazioni obsolete è idoneo a configurare una violazione dei criteri di sicurezza del trattamento dei dati personali.

5. La sicurezza dei dati

L'ultima categoria di vulnerabilità frequentemente identificata dalle autorità di controllo è quella relativa alla sicurezza dei dati, in particolare per quanto riguarda le modalità della loro conservazione e condivisione. Nonostante esista una grandissima varietà di misure di sicurezza implementabili per proteggere i dati, come ad esempio la pseudonimizzazione o la cifratura, che sono espressamente previste dall'articolo 32(1)(a) del GDPR, per motivi pratici o tecnici non sempre è possibile implementarle o garantire il massimo livello di sicurezza possibile. Ad esempio, benché la cifratura asimmetrica sia ritenuta più sicura della crittografia simmetrica, essa richiede una potenza di calcolo per cifrare e decifrare un dato molto superiore rispetto alla seconda, rendendola inadeguata alla cifratura di grandi quantità di dati in trasmissione[65]. Sicché, la tecnica di protezione dei dati dovrebbe essere adeguata al trattamento dei dati che viene effettuato.

Occorre premettere che nell'ambito della sicurezza informatica si suole catalogare i dati a seconda che siano correntemente usati nelle operazioni quotidiane, che siano in trasmissione a terzi, o che siano invece archiviati[66]. Tale distinzione, che è stata riconosciuta a livello normativo dall'EBA nelle linee guida sul *risk management* in ambito bancario[67], non sembra esser stata ad oggi condivisa da nessuna autorità di controllo[68], ma è importante perché i sistemi di protezione dei dati presentano ciascuno specifici vantaggi ed inconvenienti in funzione dello stato in cui si trova il dato da proteggere, e non possono essere applicati universalmente.

Poiché è evidente che i dati trattati attivamente da un'azienda non possano essere né pseudonimizzati né cifrati (essendo necessario utilizzare i dati, essi devono spesso essere disponibili "in chiaro", preferendosi in tali casi misure di sicurezza relative all'accesso ai dati), la maggior parte delle decisioni delle autorità si sono focalizzate sulla sicurezza della trasmissione dei dati e sulla loro archiviazione.

a) La protezione dei dati trasmessi a terzi

Quando un dato viene condiviso con terzi, vi è il rischio di una violazione di confidenzialità. Ove il dato venga trasmesso su Internet, chiunque sia in grado di intercettare la comunicazione elettronica può, in assenza di misure di cifratura, accedere al dato in chiaro. Benché la maggior parte delle comunicazioni via Internet avvenga ormai tramite modalità criptate, esistono ancora servizi che non prevedono la cifratura dei dati, come ad esempio il protocollo *http*, il quale ovviamente «non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato»[69]. Pertanto, in generale, il Garante stabilisce che «il mancato utilizzo di strumenti di crittografia per il trasporto dei dati si pone in contrasto con l'ar-

ticolo 32 del Regolamento». Tale argomento si applica, ovviamente, anche alle e-mail. Secondo l'autorità danese, l'utilizzo di protocolli di cifratura, come il protocollo TLS e la cifratura end-to-end delle e-mail in trasmissione costituisce una misura di sicurezza adeguata ai sensi dell'articolo 32 del GDPR[70].

b) La protezione dei dati archiviati

Quando un dato, a seguito del trattamento attivo, deve essere conservato, deve essere adeguatamente protetto.

Sul punto è opportuno menzionare che la prima misura di sicurezza implementabile può essere certamente costituita dall'implementazione e dal rispetto di una *data retention policy* perché eliminando dati non più necessari da un sistema è possibile eliminare il corrispondente di rischio di violazione o, quantomeno, è possibile ridurre la quantità di dati esposti alla violazione[71].

In secondo luogo, anche i dati personali archiviati e non attivamente utilizzati dovrebbero essere criptati. Ad esempio, secondo l'autorità danese, l'assenza di cifratura di un hard disk di un computer portatile che contiene dati personali costituisce una vulnerabilità che permette una facile violazione di dati[72]. Tale misura è sempre prescritta (e la sua assenza sanzionata) dalle autorità di controllo per quanto riguarda credenziali[73] e password[74] o dati identificativi[75].

Infine, la protezione dei dati con sistemi di cifratura è richiesta laddove il dato personale, per sua natura, sia particolarmente sensibile. Nel contesto della sicurezza informatica, però, il criterio di sensibilità del dato non segue necessariamente la distinzione operata dal GDPR fra categorie particolari di dati personali, dati relativi a condanne penali e altri dati. Mentre il Garante ad esempio ha emesso un provvedimento correttivo nel quale ha stabilito che la mancata protezione di dati relativi alla salute con una password costituisca una violazione dell'articolo 32 del GDPR[76], la CNIL ha recentemente esteso tale requisito anche ai dati bancari, che invece non rientrano in categorie particolari di dati[77].

6. Conclusioni

Analizzando le decisioni emesse dalle autorità europee da un punto di vista tecnico, emerge in modo chiaro che i provvedimenti hanno riguardato falle di sicurezza particolarmente gravi, benché di facile identificazione e gestione. Particolarmente significativa è l'affermazione fatta in questo senso dall'ICO che, nell'ambito di un provvedimento sanzionatorio, ha statuito che «è particolarmente preoccupante che una serie di inadeguatezze fossero relative a misure basiche e banali per tali sistemi [informatici]»[78] identificando tali misure in segregazione di rete, *patching*, testing delle vulnerabilità, attività di *logging*, gestione degli account[79], software obsoleti e assenza di antivirus[80]. Nessun provvedimento ha sanzionato una vulnerabilità non di dominio pubblico alla data della violazione[81]. Inoltre, la predisposizione di misure di sicurezza adeguate e la reazione immediata da parte del titolare del trattamento ha spesso costituito un'argomentazione valida per evitare un provvedimento correttivo o sanzionatorio[82].

Da un punto di vista più giuridico, invece, diverse considerazioni possono essere fatte. In primo luogo, occorre interrogarsi sul grado di certezza (e uniformità) del diritto offerto dall'impianto normativo dell'articolo 32 che, come detto, àncora l'adeguatezza delle misure di sicurezza a sei parametri diversi, di cui solamente uno di natura parzialmente oggettiva (lo stato dell'arte). In tale contesto, le autorità di controllo europee assumono una grande responsabilità, godendo di una discrezionalità estremamente ampia nell'interpretazione e nell'applicazione della norma. Delegare interamente alle autorità di controllo l'individuazione delle specifiche misure di sicurezza appropriate permette senz'altro di garantire una disciplina giuridica al passo con la costante evoluzione tecnologica sia dei rischi che delle corrispondenti misure di protezione, oltre a garantire un buon grado di flessibilità nell'applicazione della norma. Tuttavia, tale scelta presenta l'inconveniente di precludere un'informazione per le imprese facilmente accessibile sui requisiti di sicurezza applicabili, in particolare per quelle che, pur non essendo dotate di personale particolarmente qualificato, offrono servizi su canali telematici e vorrebbero conformarsi a dei requisiti giuridici chiari e precisi, senza dover incorrere in costi aggiuntivi. Inoltre, è teoricamente possibile che il giudizio di inadeguatezza di una misura di sicurezza espresso da un'autorità di controllo possa confliggere con quello di un'altra autorità, o essere (eventualmente a ragione) contestato da un punto di vista strettamente tecnico in sede di ricorso. Ad oggi, tale scenario non sembra ancora essersi presentato, ma la giurisprudenza relativa all'adeguatezza delle misure di sicurezza informatica sembra certamente destinata a mantenere un'importanza primaria nella precisazione del contenuto della norma e, probabilmente, anche ad assumere il ruolo di guida per le future politiche legislative relative alla sicurezza informatica.

Sempre in ottica futura, non può non rilevarsi una profonda distinzione nella tecnica normativa usata per quanto riguarda la sicurezza informatica fra il regime previsto dal GDPR e quello della direttiva PSD2 sui servizi di pagamento, fondato invece su linee guida emanate dall'Autorità bancaria europea

(EBA) che includono requisiti di sicurezza specifici, seppur *high level*. Tale soluzione, che lascia agli operatori un margine discrezionale sulle modalità concrete dell'implementazione delle misure, fornisce allo stesso tempo indicazioni tecniche chiare cui attenersi, facilitando i processi di *compliance* delle organizzazioni. Su questo punto è doveroso rilevare che tutti i principi espressi dalle autorità di controllo nelle decisioni analizzate trovano preciso riscontro normativo nelle linee guida dell'EBA[83]. Benché l'ambito di applicazione particolarmente ampio del GDPR[84] rappresenti certamente un inconveniente significativo all'adozione di tale sistema, in quanto non si può pretendere un livello di sicurezza omogeneo fra organizzazioni radicalmente diverse, come multinazionali e piccole e medie imprese, una riflessione sulla migliore soluzione per implementare un impianto normativo relativo alla sicurezza informatica potrebbe essere utile, soprattutto in considerazione della sicura centralità ed importanza della sicurezza informatica nei prossimi anni.

In conclusione, è possibile rilevare una politica fino ad oggi complessivamente tollerante da parte delle autorità di controllo europee, soprattutto dal punto di vista sanzionatorio, rispetto a violazioni riscontrate particolarmente gravi. A fronte di servizi forniti ormai quasi esclusivamente via Internet, la sicurezza informatica sta rapidamente diventando un requisito legale di primaria importanza non solo nel contesto della normativa a protezione dei dati personali, ma trasversalmente in tutti i settori economici[85] e sociali[86], come testimoniato dalla pubblicazione del *Cybersecurity Act* europeo[87], che ha (re)istituito l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), rafforzandone notevolmente poteri e competenze. Dunque, diventa di fondamentale importanza per le organizzazioni approcciare la questione della sicurezza dei dati con la dovuta attenzione e con la massima responsabilità, sia in ottica di protezione dei propri beni aziendali che, soprattutto, dei dati personali dei propri dipendenti, collaboratori e clienti che con fiducia glieli affidano.

Note

[1]CISCO, *Data Privacy Benchmark Study 2019*, p. 5.

[2]La formulazione esatta dell'articolo 32 del Regolamento (UE) 2016/679 è: «1. 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare 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. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

[3]La formulazione esatta dell'articolo 17 della direttiva 95/46/CE era: «1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere. 2. Gli Stati membri dispongono che il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure. 3. L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente: - che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento; - che gli obblighi di cui al paragrafo 1, quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo. 4. A fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti concernenti le misure di cui al paragrafo 1 sono stipulati per iscritto o in altra forma equivalente».

[4]Commissione Europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio* concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) COM(2012) 11 final, par. 3.4.4.2.: «L'articolo 30 impone al responsabile del trattamento e all'incaricato del trattamento di mettere in atto misure adeguate per la sicurezza dei trattamenti, ai sensi dell'articolo 17, paragrafo 1, della direttiva 95/46/CE, estendendo l'obbligo agli incaricati del trattamento, indipendentemente dal contratto che hanno sottoscritto con il responsabile del trattamento».

[5]Legge no 78-17 del 6 gennaio 1978 e successive modifiche.

[6]Data Protection Act 1998.

[7]Decreto legislativo n. 196/2003.

[8]L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento Privacy Europeo*, Giuffrè, 2016, p. 409.

[9]Artt. 33, 34 e 35 del d.lgs. n. 196/2003 e Disciplinare Tecnico contenuto nell'Allegato B del Decreto.

[10]Sulle divergenze di implementazione tra Stati membri, si veda Parlamento europeo, *Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE)*, COM(2003) 265 final, 2004; sulla diversità tra il regime della direttiva trasposta in Italia e il GDPR nell'ambito della sicurezza del trattamento si veda G.M. Riccio, G. Scorza, E. Belisario, *GDPR e Normativa Privacy, Commentario*, Wolters Kluwer, 2018, I ed., pp. 300-301.

[11]*Ex multis*, Garante per la Protezione dei Dati Personali, *provv. n. 99, docweb n. 9429195*, 10 giugno 2020.

[12]Prima di esso, del regime previsto dalla *Direttiva 96/45/CE*.

[13]Tra le autorità che hanno intrapreso iniziative, si segnala l'Autorità di controllo francese: CNIL, *Security of personal data*, 2018.

[14]Ad esempio, si pensi ai rapporti con i responsabili del trattamento e relativa *third-party compliance*, già analizzati dalla CNIL, *Décision n° MED 2019-025*, 5 novembre 2019 e dal Garante per la Protezione dei Dati Personali, *provv. n. 87, docweb n. 9104006*, 28 marzo 2019.

[15]Information Commissioner Office (ICO), *Penalty Notice to Doorstep Dispensaree Ltd*, 17 dicembre 2019, relativa ad un titolare sanzionato per conservazione di documenti sanitari in un cortile accessibile al pubblico.

[16]IBM Managed Security Services, *IBM Security Services 2014 - Cyber Security Intelligence Index*, p. 4.

[17]Tramite azioni di *social engineering*.

[18]L'interconnessione tra sicurezza informatica e misure organizzative è d'altronde evidenziata dalla previsione di specifici requisiti organizzativi in capo alle istituzioni finanziarie nel contesto della loro sicurezza ICT, previsti dalla European Banking Authority, *Guidelines on ICT and security risk management*, sez. 3.2 *Governance and Strategy*, 2019.

[19]Giunti, nel 2019, a 8.5 miliardi, in aumento del 200% rispetto al 2018, *IBM X-Force Incident Response and Intelligence Services, X-Force Threat Intelligence Index 2020*, 2020.

[20]ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, 10 febbraio 2020, p. 14

[21]Garante per la Protezione dei Dati Personali, *provv. n. 143, docweb n. 9435753*, 9 luglio 2020.

[22]Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010 sul principio di responsabilità*, 13 luglio 2010.

[23]G.M. Riccio, G. Scorza, E. Belisario, *op. cit.*, p. 237. Sulla necessità di dimostrare il rispetto delle disposizioni applicabili, si veda anche Garante per la Protezione dei Dati Personali, *provv. n. 143/2020*, cit.

[24]ICO, *Monetary Penalty Notice to the Carphone Warehouse Limited*, 8 gennaio 2018, p. 12; Id., *Monetary Penalty Notice to DSG Retail Limited*, 7 gennaio 2020, p. 21.

[25]Principio del *single point of failure*.

[26]Garante per la Protezione dei Dati Personali, *provv. n. 87/2019*, cit.

[27]Mentre un *vulnerability scan* ha l'obiettivo di testare l'efficacia di ciascuna misura di sicurezza, i *penetration test* hanno l'obiettivo di simulare un vero e proprio attacco, sfruttando qualsiasi vulnerabilità identificata per creare il maggior danno possibile all'organizzazione, e così individuare precisamente il danno potenziale che potrebbe essere causato dallo sfruttamento di una vulnerabilità.

[28]Garante per la Protezione dei Dati Personali, *provv. n. 83, docweb n. 9101974*, 4 aprile 2019.

[29]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 11.

[30]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[31]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 11.

[32]Id., *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 14.

[33]*Ibidem*.

[34]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[35]Tra gli altri, Id., *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, docweb n. 1577499*, 27 novembre 2008; Id., *Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie, docweb n. 1813953*, 12 maggio 2011.

[36]L'ICO è stata impossibilitata a verificare il corretto *patching* di un server a causa dell'assenza di *log* in ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 8.

[37]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[38]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 12.

[39]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[40]Id., *provv. n. 228, docweb n. 9283040*, 18 dicembre 2019.

[41]Id., *provv. n. 83/2019*, cit.

[42]*Ibidem*. Anche secondo l'ICO l'utilizzo del medesimo account e password da più membri dello staff costituisce una violazione delle misure di sicurezza adeguate, ICO, *Monetary Penalty Notice to the Carphone Warehouse Limited*, cit.

[43]ISO 27001:2013 A. 9.

[44]CNIL, *Délibération n° SAN-2019-007*, 18 luglio 2019; Id., *Délibération n° SAN-2019-005*, 28 maggio 2019.

[45]C.d. *multifactor authentication*.

[46]Ad esempio, un'autenticazione a due fattori è richiesta per l'autenticazione degli incaricati che trattano dati di traffico dei fornitori di servizi di comunicazione elettronica, Garante per la Protezione dei Dati Personali, *Allegato A, docweb n. 1538237*, 17 gennaio 2008. Nel contesto della direttiva PSD2, gli utenti dei servizi bancari devono essere autenticati con un'autenticazione a due fattori: European Banking Authority, *Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under article 98 of Directive 2015/2366 (PSD2)*.

[47]Garante per la Protezione dei Dati Personali, *provv. n. 548, docweb n. 7400401*, 21 dicembre 2017.

[48]CNIL, *Délibération n° SAN-2020-003*, 28 luglio 2020.

[49]Regolamento (UE) 2016/679, Capo VII.

[50]Il meccanismo di cooperazione sembra esser stato efficacemente usato nella decisione CNIL n. SAN-2020-003, nell'ambito del cui procedimento ha raccolto e incluso nel provvedimento finale le osservazioni delle autorità italiana, portoghese e della Bassa Sassonia.

[51]G.M. Riccio, G. Scorza, E. Belisario, op. cit., p. 276.

[52]CNIL, *Décision n° MED 2019-025*, 5 novembre 2019.

[53]Garante per la Protezione dei Dati Personali, *provv. n. 18, doc. web n. 9269629*, 23 febbraio 2020.

[54]Si pensi ad esempio ad uno scenario in cui il personale del dipartimento *marketing* non possa accedere ai dati di fatturazione cliente trattati dal dipartimento *finance*.

[55]Come suggerito dal Garante per la Protezione dei Dati Personali, *provv. n. 18/2020*, cit.

[56]Id., *provv. n. 83/2019*, cit.

[57]Ad esempio, in ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 13.

[58]Garante per la Protezione dei Dati Personali, *provv. n. 548/2017*, cit., secondo cui le vulnerabilità possono essere causate, ad esempio, da un'insufficiente metodologia di sviluppo software.

[59]ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 8.

[60]Si veda, ad esempio, Id., *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 10.

[61]Id., *Monetary Penalty Notice to the Carphone Warehouse Limited*, cit., pp. 8-9.

[62]Id., *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 10.

[63]Id., *Monetary Penalty Notice on DSG Retail Limited*, cit., p. 12.

[64]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[65]Sulla distinzione fra crittografia simmetrica e asimmetrica si veda, ad esempio, CNIL, *Comprendre les grands principes du chiffrement*, 2016.

[66]Rispettivamente tecnicamente definiti *active data*, *data in trasmission* e *data at rest*.

[67]European Banking Authority, *Guidelines on ICT and security risk management*, cit., sez. 3.4 *Information security*, p. 18.

[68]Seppure la CNIL impieghi una struttura tripartita di archiviazione di dati, distinguendo fra archiviazione di dati attivi, archiviazione intermedia e archiviazione definitiva, si veda CNIL, *Les durées de conservation des données*, 2020.

[69]Garante per la Protezione dei Dati Personali, *provv. n. 17, docweb n. 9269618*, 23 gennaio 2020; CNIL, *Décision n° MED 2019-025*, 5 novembre 2019.

[70]Datatilsynet, *Tilsyn med behandlingssikkerhed hos advokatfirma*, journalnummer 2019-41-0026; Id., *Tilsyn med behandlingssikkerhed hos revisionsfirma*, journalnummer 2019-41-0027.

[71]ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 14.

[72]Datatilsynet, *Gladsaxe og Horsholm Kommune*, 10 marzo 2020.

[73]Garante per la Protezione dei Dati Personali, *provv. n. 2282019*, cit.

[74]CNIL, *Délibération n° SAN-2018-011*, 19 dicembre 2018.

[75]Garante per la Protezione dei Dati Personali, *provv. n. 17/2020*, cit.

[76]Id., *provv. n. 142, docweb n. 9446166*, 9 luglio 2020.

[77]CNIL, *Délibération n° SAN-2020-003*, cit.

[78]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit.

[79]*Ibidem*.

[80]ICO, *Monetary Penalty Notice to the Carphone Warehouse Limited*, cit.

[81]*0 day vulnerability* in linguaggio tecnico.

[82]Agencia Espanola de Proteccion de Datos, *Procedimiento n. PS/00431/2018*, p. 3.

[83]In ordine di discussione, con corrispondente paragrafo del documento European Banking Authority, *Guidelines on ICT and security risk management*, cit., *vulnerability testing* alla sez. 3.4.6., *logging* alla sez. 3.4.2 (d), *autenticazione* alla sez. 3.4.2 (g), *autorizzazione* alla sez. 3.4.2 (a), *utilizzo di applicazioni obsolete* alla sez. 3.4.5.

[84] Che si applica indifferentemente ad organizzazioni di dimensioni e con interessi non comparabili.

[85]Ad esempio il settore bancario, già discusso; in ambito reti e sistemi informativi si pensi alla direttiva (UE) 2016/1148 "NIS".

[86]In tema di sicurezza nazionale si veda la direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

[87]Regolamento (UE) 2019/881.

* * *

Breach of security requirements under Article 32 of GDPR

Abstract: According to a recent survey, organizations revealed that the biggest challenge they face related to compliance with GDPR provisions is to align their security measures to the requirements established by Article 32 of the GDPR. This difficulty may derive from some particular aspects of security measures, such as their very broad implementation scope, the great diversity of existing measures to be implemented, and the need to engage several professionals with different backgrounds for their implementation. Among legal difficulties, it is argued that Article 32 of the GDPR does not identify specific measures to be implemented, or those which could be deemed appropriate, but only provides a list of recommended measures. In addition, the requirement of appropriateness of the security measures depends on a number of subjective factors, which therefore leaves broad discretion to European supervisory authorities to rule on which measures may be deemed appropriate and which may not. In order to provide precise guidance to organizations, the article conducts an analysis of the decisions of selected European supervisory authorities related to IT security to identify which measures were deemed appropriate and which inappropriate. The decisions were grouped based on the types of security measures analyzed by the authorities: accountability, access management, use of obsolete applications and protection of data. The analysis shows that European supervisory authorities adopt a uniform approach towards the definition of appropriateness of security measures. However, given the importance of cybersecurity in the near future and the importance of protection of personal data, such uniformity shall be preserved to ensure legal certainty and a uniform application of GDPR security requirements across Europe.

Keywords: GDPR – Security measures – Article 32 – Cybersecurity Compliance – Europe

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

ISSN 2704-7318
Fascicolo 2-2020
DOI: 10.32091/RIID0026

Chi teme i giudici robot

Antonio A. Martino*

Da più di quarant'anni il tema dell'intelligenza artificiale è studiato da diverse prospettive nel suo rapporto con il diritto e con i sistemi giudiziari. L'articolo propone alcune riflessioni sullo stato attuale di questo rapporto e sulla infondatezza della paura ancestrale che la macchina possa sopraffare l'uomo o comunque possa sostituirlo in tutte le attività nelle quali è necessaria la ragionevolezza e non solo la razionalità.

Intelligenza artificiale e diritto – Intelligenza artificiale e sistema giudiziario – Decisione giuridica e intelligenza artificiale – Robotica

Sommario: *1. Introduzione: alcuni dati di fatto – 2. Inseguendo la logica deontica abbiamo trovato l'intelligenza artificiale – 3. Quarant'anni dopo – 4. Il giudice robot – 5. Paure – 6. L'etica – 7. Bibliografia*

1. Introduzione: alcuni dati di fatto

Quando ho iniziato a occuparmi di intelligenza artificiale e diritto ho aggiunto, nella sistematica classica del diritto informatico, un settore che chiamavo "decisione legale"; in verità non era un titolo originale, poiché altri, prima di me, lo avevano usato. In una conferenza in Francia poi mi è stato chiesto di riformulare l'espressione e l'ho chiamato "supporto decisionale". Penso che questa sia stata una scelta opportuna, perché mentre il primo titolo aveva spaventato giudici e avvocati, il secondo ha trovato molti sostenitori.

Potrei quindi riformulare il titolo di questo contributo "Chi teme l'aiuto che un automa può fornire al giudice" e probabilmente ne guadagnerebbe in precisione e accettabilità.

Questa è la soluzione trovata dalle case produttrici di automobili autonome: l'acquirente deve firmare un accordo con cui s'impegna ad avere sempre al volante un autista umano che, in caso di incidenti, prende l'ultima decisione.

Tutto ciò è ragionevole ma anche fuorviante. Facciamo un passo alla volta.

Prima di tutto, consideriamo due aspetti: il primo, che avevano sottolineato già i critici al primo sistema esperto che avevo sviluppato nel 1987: le macchine possono calcolare molto bene, quindi sono razionali, non riescono invece a ponderare tra i valori in gioco, quindi non sono ragionevoli. Il secondo: la paura è connaturale alla vita umana; il fatto è se ci blocca o ci consente di andare avanti, anche con paura. La paura che le macchine sostituiscano l'uomo per il momento è esagerata anche se suggerita da una mente certamente colta ma che sa poco d'intelligenza artificiale[1]. Guardiamo ad alcuni dati di fatto.

1.1. Il 7 maggio 2016, negli Stati Uniti, su una strada dello Stato della Florida, si è verificato un incidente che ha portato alla morte di un automobilista quarantenne. A parte la delusione sempre legata alla morte di un essere umano, la notizia in sé non è di grande rilevanza dato che i morti negli Stati Uniti in incidenti stradali sono stati 35.200 nel 2015. Ma in questo caso si è trattato di qualcosa di speciale perché il conducente che guidava era un modello Tesla "S" con la "funzione autopilota" attivata. Que-

*La *Rivista* è felice di ospitare le riflessioni proposte in questo saggio da Antonio A. Martino, già direttore dell'IDG-CNR, oltre che professore di Scienze politiche dell'Università di Pisa, membro dell'Accademia di Diritto di Cordoba e professore emerito dell'Università del Salvador (Argentina).

sto primo incidente mortale ha rilanciato il dibattito sull'automazione e sul rapporto uomo-macchina e ha sollevato importanti questioni.

1.2. I computer hanno già componenti di intelligenza artificiale progettate per simulare qualsiasi tipo di reazione razionale al cambiamento delle circostanze. Ad esempio, Microsoft ha lanciato il "Project Scorpio", una consolle progettata per la realtà virtuale e i giochi 4K, nell'ambito della sua conferenza annuale sui videogiochi presso il Gale Center di Los Angeles.

1.3. BiroRobot, il robot che riduce il consumo di energia. Quante volte accendiamo la luce? Un termosifone perde? Una finestra provoca una perdita di calore? BiroRobot vi avvisa. È un robot che mette in discussione le nostre abitudini e l'uso di energia, sia termica sia elettrica, all'interno di una casa o di un'azienda. Dopo un periodo di osservazione di un mese, BiroRobot è pronto a suggerire come ridurre i rifiuti in casa e come gestire meglio l'energia.

1.4. L'umanoide R1 può essere un ottimo assistente in casa, un buon venditore o un assistente infermiere. Ultima creazione dell'IIT, Istituto Italiano di Tecnologia, R1 è un umanoide personale progettato per entrare nelle nostre case. Ha un'altezza che può variare da un metro e 25 cm fino a un metro e 45 cm, grazie al suo busto estensibile; ha braccia estensibili e il busto può essere diretto verso l'alto, verso il basso o lateralmente. La batteria permette un'autonomia di 3 ore, mentre la sua velocità massima, per motivi di sicurezza, è di 2 km/h. L'intelligenza artificiale di R1 si sviluppa direttamente sull'umanoide, a differenza di quanto accade di solito. Ciò significa che l'intelligenza del robot sviluppa in modo funzionale il corpo che lo ospita. Ne ho visto un altro simile alla Scuola Superiore Sant'Anna di Pisa, nel laboratorio di biorobotica di Pontedera, nel febbraio 2020. Non si caratterizza tanto per l'aspetto esteriore, ma è un compagno perfetto per le persone anziane o con difficoltà visive o acustiche. Il compagno deve potersi muovere da solo. Una cosa interessante è che vengono usati plastica e materiali riciclati al posto del classico metallo. E cosa più importante: robot morbidi anche realizzati con materiali di recupero e utilizzati per molte attività umane, a partire dall'agricoltura[2].

1.5. Il processo telematico. Nello Stato del Michigan, negli Stati Uniti, un avvocato potrebbe presto essere in grado di difendere un caso in tribunale dalla cucina della sua casa di New York, in pigiama, mentre fa colazione. Non avrebbe bisogno di mettere piede in Michigan. Almeno, questo è il piano. Per invogliare le aziende tecnologiche ad aprire un negozio in Michigan, il governatore John Engler vuole istituire un cyber tribunale separato per i casi che coinvolgono aziende *high-tech*, dove in sostanza tutto può essere risolto tramite computer piuttosto che di persona in tribunale. Le relazioni possono essere presentate online, le prove possono essere videoregistrate, le argomentazioni orali possono essere ascoltate in teleconferenza e le conferenze possono essere tenute via e-mail. Si potrà obbiettare che in Italia, in Spagna e in molti paesi europei già esiste il processo telematico. È vero, anche questo è un fatto, solo che nei paesi ad organizzazione federale come gli Stati Uniti, il Brasile e l'Argentina è più difficile organizzare i tribunali in processi telematici: per questa ragione è importante la situazione negli Stati Uniti[3].

1.6. *Entanglement*. Gli scienziati sostengono di aver dimostrato che un effetto chiamato *entanglement* (intreccio) è presente in otto unità d'informazione quantistica. L'intreccio è un passo fondamentale per la costruzione di una piattaforma operativa. I computer quantistici usano il principio della sovrapposizione o dell'intreccio. Un bit quantistico, *qubit*, ha maggiori possibilità di memorizzare informazioni perché, oltre ai due stati classici 1 e 0, si trova in una sovrapposizione di questi. In altre parole, può essere parzialmente in uno e l'altro allo stesso tempo. La gamma di possibilità varia continuamente da 0 a 1, con sovrapposizioni contenenti più o meno dei due stati classici[4]. Finora il problema delle macchine quantiche era la temperatura, molto alta, che non consentiva stati duraturi di frequenza. Ora ci sono già tre novità: Amazon dice di avere un computer quantico di 20 *qubit* e Google un altro di 80 *qubit*, ma quella più sorprendente è di IBM che dice di avere una macchina quantistica pronta per essere venduta. Sarebbe un cubo di due metri chiamato *Q System One*.

1.7. Ricerca. Non solo ci sono prodotti di IA giuridica in funzione, ma la ricerca continua ai massimi livelli. Tra le tante esperienze ce ne sono due. MIREL - *MIning and REasoning with Legal texts* è una ricerca finanziata dall'Unione europea. Il progetto MIREL creerà una rete internazionale e intersettoriale per definire un quadro formale per la traduzione di testi giuridici in rappresentazioni formali che possono essere utilizzate per la consultazione, la verifica della conformità e il supporto decisionale. Lo sviluppo del *framework* e degli strumenti MIREL sarà guidato dalle esigenze di tre partner industriali e convalidato da casi di studio di settore. MIREL promuove la mobilità e lo scambio di personale tra le PMI e il mondo accademico. Si tratta di un Consorzio interdisciplinare nelle aree del Diritto e dell'Intelligenza Artificiale, tra cui *Natural Language Processing*, Ontologie Informatiche, Argomentazione, Logica e Ra-

gionamento. Affronta sia le sfide concettuali, come il ruolo dell'interpretazione giuridica nel *data mining* e nel ragionamento, sia le sfide computazionali, come la gestione di big data giuridici, e la complessità della *compliance* normativa. Esso colma il divario tra la comunità che lavora sulle ontologie giuridiche e gli analisti nel NLP e la comunità che lavora sui metodi di ragionamento e sulla logica formale. È anche il primo progetto di questo tipo a coinvolgere i partner del settore nello sviluppo futuro di prodotti e servizi innovativi nel ragionamento giuridico e nella diffusione sul mercato.

Prometea è un programma creato da un team multidisciplinare della Procura della Città di Buenos Aires (CABA) per assistere il sistema giudiziario. Per raggiungere questo obiettivo, insieme a specialisti in intelligenza artificiale è stato sviluppato un sistema progettato per prevedere la soluzione di semplici casi legali. Il team che ha creato *Prometea* è guidato da due funzionari della giustizia di Buenos Aires: Juan Corvalán - vice procuratore generale nel contenzioso amministrativo presso la Procura della Repubblica - e Luis Cevasco - vice procuratore generale incaricato della procura generale. Il team è stato creato in una sezione della Facoltà di Giurisprudenza di Buenos Aires che si occupa di Intelligenza Artificiale applicata al diritto - IA Lab[5].

2. Inseguendo la logica deontica abbiamo trovato l'intelligenza artificiale

Quando abbiamo iniziato queste ricerche, più di quarant'anni fa, abbiamo avuto un grande vantaggio cognitivo: il nostro principale riferimento è stato Georg H. Von Wright, discepolo di Wittgenstein e successore della cattedra di filosofia all'Università di Cambridge. Layman E. Allen, professore di logica e filosofia all'Università di Ann Arbor, Miguel Sánchez Mazas, professore di logica e filosofia all'Università di Deusto, un gruppo di filosofia del diritto all'Università di Buenos Aires - Carlos E. Alchourrón, Eugenio Bulygin, Roberto Vernengo e io - eravamo tutti filosofi, filosofi del diritto, sapevamo di cosa parlavamo, scrivevamo o producevamo.

Tutto è iniziato con un articolo di Georg H. Von Wright, *Deontic Logic* nella rivista *Mind*, nel 1951. All'Istituto di Filosofia del diritto della Facoltà di Giurisprudenza dell'Università di Buenos Aires, il suo direttore, Ambrosio Lucas Gioja, promosse lo studio della filosofia analitica e portò a Buenos Aires diversi studiosi: Peter Strawson, Alf Ross e Georg H. Von Wright. Molti studi e incontri produssero una nuova visione del rapporto fra la logica e il diritto. Nel 1971 Carlos E. Alchourrón ed Eugenio Bulygin pubblicarono i *Sistemi Normativi* e provocarono un grande cambiamento negli studi di logica giuridica. Poi nel 1977/78 abbiamo pubblicato con Carlos E. Alchourrón *Logica senza Verità*. Ora, privata della sua dimensione semantica, la logica era sintattica, cioè un rapporto tra segni. Era esattamente quello che facevano gli informatici, quindi era possibile lavorare insieme senza paura di distorcere ciò che era detto.

Nel 1980 ero già nel Consiglio scientifico e poi mi è stata affidata la direzione dell'Istituto per la documentazione giuridica (IDG) del Consiglio Nazionale delle Ricerche, poi diventato ITTIG e successivamente IGSG, con sede a Firenze. Sono stato direttore per circa undici anni, dal 1982 al 1993, e lì ho avuto la possibilità di entrare in contatto con i migliori informatici giuridici del momento: L.E. Allen, P. Catala, R. Stamper, L.T. McCarty, Sheridan, G. Kalinowski, J. Bing, D. Bourcier, J.L. Bilon, M. Vivant, M. Bibent, L. Reisinger, A. Peczenick, H.-N. Castañeda, V. Knapp, J. Wróblewski, H. Fiedler, L. Aquist, A. Oskamp, C. De Bessonet, C.S. Saxon, H. Bauer-Bernet, R. Vernengo, W.R. Svoboda, S. Nagel, R.V. de Mulder, J. Thorne, V. Vrecion, M. Sánchez Mazas, G.P. Zarri, A. Gardner, R. Guibourg, C.H. Shyu, C.M. Fu, C.H. Lee, G.R. Cross, W.B. Huan, D. van der Merwe, R.E. Susskind, etc.

Dopo ci sono stati i 4 congressi *Logica, Informatica, Diritto* presso l'Istituto di Documentazione Giuridica nel 1981, 1985, 1989 e 1993, cioè ogni quattro anni, seguiti dalla pubblicazione dei relativi atti. Disponevamo di molte risorse per fare del nostro meglio, provenienti sia dal CNR, che ha stanziato ingenti somme di denaro per rendere indimenticabili questi convegni, sia dalla Corte di Cassazione con cui abbiamo lavorato allo sviluppo del sistema informativo Italgiure. Ma il denaro è solo una parte del rendere indimenticabile un convegno. Ci vuole la pazienza e la determinazione di tutti i ricercatori e dello staff di un Istituto per sfruttare al meglio ogni momento, ci vuole un po' di fortuna; eravamo a Firenze e tutti sono venuti volentieri in questa città d'arte. E un po' di astuzia. Abbiamo abbinato scienza e bellezza che è una cosa che si può fare solo in Italia.

3. Quarant'anni dopo

Sono passati più di 40 anni e molte cose sono cambiate.

Nella costruzione dei primi sistemi esperti utilizzavamo un metodo deduttivo, dall'alto verso il basso (*top down*). Oggi usiamo una tecnica di *bottom up*, dal basso verso l'alto di tipo induttivo che rende la programmazione molto più facile, ma a differen-

za della deduzione che è una teoria complessa, ma completa, l'induzione è una teoria incompleta.

Il ragionamento più sensato è in ogni caso quello di lavorare con l'approccio *bottom up* e poi controllare con criteri che operano dall'alto verso il basso. L'intelligenza artificiale è diventata di moda: tutti la usano, tutti la vogliono, anche quelli che non hanno la minima idea di cosa sia. Naturalmente le mode portano complicazioni. Dal momento che tutti la vogliono, molti produttori che non ce l'hanno utilizzano quello che hanno e lo vendono. Attualmente, per questo motivo, l'intelligenza artificiale è associata a prodotti che, interessanti nei loro campi, non hanno nulla a che fare con l'intelligenza artificiale.

Il primo è la *blockchain*. Al di là dell'uso sempre più frequente di questa tecnica sotto forma di *buzzword*, generalmente si tratta di dischi condivisi e distribuiti o "privati/centralizzati". Una delle proprietà più importanti è la non modificabilità degli "elementi/transazioni" che fanno parte della catena a blocchi del registro. Il fatto che non possano essere modificati è qualcosa di simile alla scoperta dell'acqua calda.

Le uniche differenze reali tra le varie tecnologie per la costruzione di una catena a blocchi si possono riassumere nel fatto che la distribuzione dei nodi (minatori) è pubblica e liberamente distribuita o privata/centralizzata/controllata. Chiunque può essere il minatore o solo alcuni. Ovviamente si possono "stampare" valute virtuali, autenticare contratti e transazioni notarili o convalidare una bella produzione musicale o un film porno o catene di processi e/o contratti tra aziende o all'interno di un'azienda.

Il vero limite di questa tecnologia è l'enorme spesa computazionale necessaria per bloccare le validazioni, perché più lunga è la catena e più i costi aumentano.

In ogni caso le competenze comuni, soprattutto di tipo crittografico, in uno specialista di tecnologia a catena di blocco e in uno specialista di intelligenza artificiale sono pari a zero.

Lo stesso si può dire di una tecnologia di rete che diventerà presto molto famosa e che ha poco a che fare con l'intelligenza artificiale ossia la tecnologia 5G.

L'intelligenza artificiale ha a che fare con l'implementazione informatica di procedimenti logici e di regole deduttive. I programmi con cui essa è realizzata sono cambiati nel tempo notevolmente e questo ne ha mutato molti aspetti.

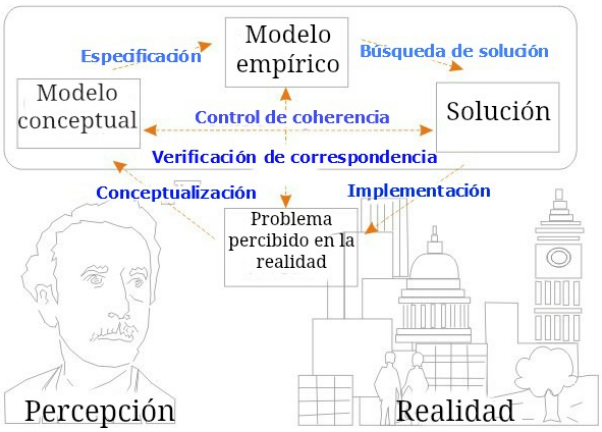
I software di aiuto alla decisione sono oggi numerosi. IBM ha creato *Watson* che in realtà e un insieme di software indirizzati soprattutto alla comprensione del linguaggio naturale che consente di sviluppare sistemi di aiuto per i giuristi[6].

Il software *Ross*, altamente sviluppato, è in grado di ascoltare il linguaggio umano, di tracciare oltre 10 mila pagine al secondo e di formulare una risposta molto più veloce di qualsiasi avvocato umano. Le risposte di *Ross* includono atti legali, suggeriscono le norme rilevanti da studiare e persino calcolano un tasso di fiducia per aiutare gli avvocati a preparare i casi. Inoltre, in linea con l'intelligenza artificiale, più dati riceve più impara e più diventa efficace. *Ross* impara dalla sua interazione con gli esseri umani. Questo software è stato creato da una startup canadese dell'Università di Toronto. I ricercatori hanno utilizzato la tecnologia *Watson*.

Bisogna ancora sottolineare che il ragionamento giuridico è retorico e non logico, ha a che fare con la volontà di convincere. È più simile alla retorica che alla logica. Sarebbe conveniente per avvocati e giudici sfruttare una vecchia materia delle università medievali: l'oratoria. Un programma che si occupa di questo è il *Project Debater* la cui base di conoscenza è costituita da circa 10 miliardi di frasi, tratte da giornali e riviste. In un dibattito dal vivo, il *Project Debater* discute un argomento sul quale non è mai stato addestrato riducendolo a una asserzione breve che descrive la mozione o l'istanza presentata. Il primo passo è quello di costruire un discorso per difendere o opporsi a questa mozione. *Project Debater* cerca brevi pezzi di testo in una massa di dati che possano servire a questo scopo. Ciò richiede una profonda comprensione del linguaggio umano e delle sue infinite sfumature, cosa non sempre facile per gli esseri umani e certamente molto difficile per i computer. Questo processo può portare ad alcune centinaia di segmenti di testo rilevanti. Per poter discutere efficacemente, il sistema deve costruire gli argomenti più forti e diversificati a sostegno della sua tesi. Il *Project Debater* fa questo, eliminando il testo argomentativo ridondante, selezionando le rimanenti affermazioni e prove più forti e organizzandole per argomento, creando la base della narrazione per sostenere o contestare una mozione. Utilizza anche una base di conoscenza che gli permette di trovare argomenti a sostegno dei dilemmi umani generali che sorgono nel dibattito, ad esempio, quando è giusto che il governo vincoli la libertà di scelta personale dei cittadini.

Il ragionamento giuridico non è lineare, non è nemmeno neutrale, è pieno di retorica perché si tratta di convincere il giudice, il procuratore, l'alta corte, la corte suprema, l'opinione pubblica. E la retorica ha una lunga tradizione, esempi e forme canoniche. Le norme giuridiche hanno una logica diversa da quella descrittiva o ordinaria che Georg H. von Wright chiamava "deontologia".

Vale la pena ricordare le somiglianze e le differenze tra uomo e macchina: l'intelligenza artificiale, tutti i programmi per ragionare, inclusi i robot, sono enormemente diversi dagli esseri viventi: gli organismi sono molto al di sopra delle macchine costruite dall'uomo. Per esempio, il corpo si riproduce continuamente. L'epitelio intestinale viene rinnovato ogni cinque giorni. Il fegato ogni due mesi. La pelle ogni sei settimane. Ogni anno il 98% degli atomi del nostro corpo viene sostituito. Questo incessante ricambio chimico, il metabolismo, è un segno inconfondibile della vita. I biologi cileni Humberto Maturana e Francisco Varela vedono nel metabolismo l'essenza di qualcosa di fondamentale per la vita: l'autopoiesi. Un'entità autopoietica metabolizza continuamente; si perpetua attraverso l'attività chimica. L'autopoiesi collega il dispendio di energia con la disorganizzazione[7]. Quando abbiamo iniziato a testare un nostro sistema esperto – chiamato SRL, Sistema di ragionamento legale – presso l'IDG, che allora dirigevo, abbiamo ovviamente chiamato degli esperti che hanno convalidato le decisioni o le conclusioni del nostro sistema, ma un giorno ci è stata fatta notare una cosa curiosa: il sistema calcolava tutte le conseguenze che si potevano ottenere dall'insieme di regole che avevamo inserito, comprese quelle che gli esperti non avevano preso in considerazione perché le consideravano estremamente rare o di scarsa importanza. Il sistema era totalmente razionale, non era ragionevole. Vale a dire esso calcolava troppo per gli esperti[8]. Tutto parte da un semplice modello di soluzione dei problemi.



Le decisioni programmate sono quelle che sono prese frequentemente, cioè sono ripetitive e diventano routine, come il tipo di problemi che risolvono, e si presentano con una certa regolarità; c'è un metodo di soluzione ben consolidato e quindi i passi per affrontare questo tipo di problemi sono già noti, per questo motivo queste sono anche chiamate decisioni strutturate. La persona che prende questo tipo di decisione non ha bisogno di progettare alcuna soluzione, ma semplicemente segue quella seguita in precedenza.

Tutti noi abbiamo alcuni criteri caratteristici della nostra personalità, che per alcuni sono chiamati pregiudizi[9]. Ed è difficile prescinderne e non è detto che nel preparare le nostre macchine di aiuto alla decisione non trasmettiamo loro anche i nostri pregiudizi cognitivi. Il rapporto uomo-macchina è un'interazione complessa con forti influenze reciproche. La tecnologia non può essere considerata semplicemente un prodotto dell'uomo, secondo una logica tradizionale di causa ed effetto, né è semplicemente il prodotto del lavoro umano, poiché è allo stesso tempo un produttore di lavoro. E se l'essere umano appare particolarmente refrattario a qualsiasi modificazione della natura etico-politica, indubbiamente sembra preferire il richiamo del carattere tecnologico, forse dimenticando talvolta la linea sottile che separa l'umanità dalle macchine.

Nel mondo sviluppato si parla da tempo di uno "svuotamento" del mercato del lavoro che impoverisce la classe media e aumenta le disuguaglianze salariali (e di reddito). Che cos'è questo svuotamento? Un calo dell'occupazione e del reddito relativo del lavoratore specializzato medio, poiché questi posti di lavoro sono sostituiti da programmi e robot. E se all'inizio l'automazione ha sostituito i compiti industriali, spostando i posti di lavoro nel settore dei servizi, oggi le macchine vengono realizzate anche per i lavori di assistenza, a partire, per ora, da quelli che richiedono una media – non elevata – competenza.

Per questo motivo, pur non essendo una novità (negli Stati Uniti va avanti da tre decenni), negli ultimi anni l'automazione ha portato a una sorta di macchinismo distopico di fronte all'accumulo di prove aneddotiche: procedure e traduzioni online, casse automatizzate nelle catene di supermercati, robotizzazione dei magazzini di giganti come Amazon. L'ansia non è solo americana: ad esempio, la grande scommessa cinese per recuperare competitività è la robotizzazione massiccia, come nel caso della società FoxConn, produttrice di iPhone.

Per gli ottimisti tecnologici, come i professori del MIT Erik Brynjolfsson e Andrew McAfee, la tecnologia digitale è per la nostra capacità mentale ciò che il motore a vapore è per la nostra capacità muscolare. Quindi, si dice, questo è il momento migliore per essere un lavoratore qualificato con la giusta educazione per usare la tecnologia per creare valore, e il momento peggiore per essere un lavoratore standard con basse abilità.

Personalmente credo che l'idea fondamentale sia quella di un sistema: se c'è un sistema, allora si può aggiungere tutta la tecnologia che si vuole. Ad esem-

pio, Thomas Twining ha aperto la prima sala da tè conosciuta al 216 Strand di Londra nel 1708 e questa è ancora in funzione. Il logo aziendale, creato nel 1787, è uno dei più antichi al mondo. Lì c'è un sistema di produzione, marketing e distribuzione, prima dei computer. Si può anche aggiungere tutta la tecnologia che vi viene in mente. Se esiste la tecnologia ma non il sistema, quando la tecnologia diventa obsoleta (presto) non si può andare oltre.

Basta pensare al mondo che ci lascia l'attuale pandemia, con una grande crisi economica e lo sviluppo accelerato delle soluzioni automatiche. Non siamo ancora in grado di valutare tutte le conseguenze, ma ce ne saranno certamente parecchie.

Si tratta di un cambiamento necessario nell'agenda dell'educazione: questa deve diventare un meccanismo di inclusione (sottolineando la cura della prima infanzia e la scolarizzazione) e un accumulo di capitale umano (cura della qualità e dell'istruzione terziaria).

Cosa si può fare per essere beneficiari e non vittime della rivoluzione tecnologica? Le raccomandazioni abituali sono quelle di riformare l'istruzione (più flessibile e orientata alla trasformazione e alla creatività), di incoraggiare l'innovazione, di investire in ricerca e sviluppo legati al settore produttivo e di finanziare i settori dinamici. In altre parole, un modello di produzione basato sulla conoscenza che ci permette di vendere il nostro lavoro ad un prezzo elevato. E anche se probabilmente non vinceremo mai completamente la gara con il robot e la disuguaglianza tecnologica dovrà essere compensata con beni pubblici o trasferimenti keynesiani, non c'è più margine per stare fermi.

4. Il giudice robot

L'Estonia è diventata l'eccezione che dimostra la regola. In generale, i governi non sono il miglior esempio di innovazione ICT o di applicazione di nuove tecnologie come l'intelligenza artificiale. Ott Velsberg, *chief data officer* del governo estone, ha rivoluzionato il paese all'età di 28 anni introducendo l'intelligenza artificiale e l'apprendimento automatico con un piano che interessa 1,3 milioni di cittadini.

Il governo estone ha assunto Velsberg per guidare un nuovo progetto di implementazione dell'intelligenza artificiale in diversi ministeri allo scopo di semplificare i servizi offerti alla popolazione, superando l'obiezione che la qualità del servizio possa diminuire in caso di riduzione del numero dei dipendenti.

L'Estonia stava già lavorando all'implementazione dell'intelligenza artificiale prima dell'assunzione di Velsberg. Siim Sikkut, *chief information officer* dell'Estonia, ha avviato diversi progetti pilota in materia nel 2017. Oggi l'Estonia ha già attuato 13 misure di intelligenza artificiale in cui i lavoratori vengono sostituiti per avere servizi più efficienti.

Il progetto più ambizioso e controverso del Paese riguarda la creazione di "giudici robot". Il Ministero estone ha chiesto a Velsberg e al suo team di implementare l'intelligenza artificiale nei processi più piccoli, quelli in cui ci sono controversie di valore non superiore a 7.000 euro. L'intelligenza artificiale permetterebbe di accelerare decine di casi arretrati che i giudici e i cancellieri non sono attualmente in grado di gestire.

I "giudici robot" sono ancora nella prima fase e un test pilota incentrato sulle controversie contrattuali è previsto a breve. La procedura sarà la seguente: entrambe le parti caricheranno i loro documenti e le informazioni rilevanti sul caso su una piattaforma, dove l'IA prenderà una decisione che potrà essere impugnata davanti a un giudice "umano". Il sistema è ancora in sperimentazione e Velsberg ha spiegato che potrebbe essere adattato in base ai commenti degli avvocati e dei giudici.

Il paese baltico è forse nella migliore situazione per implementare i "giudici robot". L'Estonia dispone di una banca dati di 1,3 milioni di cittadini con una carta d'identità nazionale per servizi online come il voto elettronico e l'archiviazione digitale delle tasse. I database governativi sono collegati tra loro da un sistema chiamato *X-road*, un'infrastruttura digitale che facilita lo scambio di dati. Inoltre, i cittadini stessi possono verificare chi ha avuto accesso alle loro informazioni, se lo desiderano. Per quanto riguarda la sicurezza, Tanel Tammet, professore di informatica alla Tallinn University of Technology, sottolinea che le informazioni private e riservate non sono nelle mani del governo, ma nelle mani delle banche e delle telecomunicazioni. David Engstrom (Stanford University), esperto di governance digitale, spiega che i cittadini estoni possono avere fiducia nell'uso dei dati digitali da parte del loro governo, ma che in futuro la situazione potrebbe cambiare qualora il processo decisionale basato sull'IA fallisse.

L'Estonia non è il primo paese a coniugare intelligenza artificiale e diritto, anche se potrebbe essere il primo a conferire alle applicazioni di IA l'autorità di prendere decisioni. Negli Stati Uniti, ad esempio, gli algoritmi sono utilizzati nelle corti di alcuni Stati. Il caso più noto è la *chatbox* alimentata da DoNotPay, con sede nel Regno Unito, che ha contribuito a cancellare 160.000 multe per divieto di sosta a Londra e New York negli ultimi anni.

Di particolare interesse è, poi, il caso cinese. Il gigante asiatico ha recentemente lanciato il cosiddet-

to *Beijing Internet Court*, un centro di contenzioso online dove un giudice donna con corpo, espressioni facciali, voce e gesti, tutto modellato su un essere umano che anche "respira", basato sull'intelligenza artificiale, risolverà semplici controversie. In questa prima fase lavorerà a sostegno dei giudici veri e propri. Il suddetto tribunale ha sviluppato un sistema in cui l'intero processo di estrazione e conservazione delle prove elettroniche può essere controllato per verificarne la tracciabilità e, quindi, la veridicità.

Inoltre, il giudice di intelligenza artificiale – che le autorità cinesi sostengono essere il primo del suo genere – ha la capacità di "studiare" i casi precedenti e di verificare la giurisprudenza in tempo reale. Nelle intenzioni dei suoi creatori, il giudice di intelligenza artificiale aiuterà i giudici dei tribunali a completare il lavoro ripetitivo di base, anche con l'uso di tecnologie intelligenti di sintesi vocale e di immagine che permetteranno ai professionisti di porre la loro piena attenzione sui procedimenti giudiziari.

In altre parole, ci sono già programmi concreti per avere giudici automatizzati e questo produce panico. Una cosa è il supporto decisionale e un'altra è il processo decisionale delle macchine, sia che si tratti di programmi sia che si tratti di robot.

5. Paure

Ogni volta che l'umanità intraprende nuove strade, appaiono le paure profonde dell'ignoto. Ci sono paure che sono abbastanza ben studiate dagli specialisti. Una è la paura della miseria, che ha sempre accompagnato l'uomo, perché è quella che colpisce sempre di più. Una seconda paura chiaramente identificata è quella dell'altro. Infatti nelle tribù più antiche del pianeta il saluto è particolarmente lungo, per rassicurare l'altro che non si arriva con intenzioni aggressive; la paura dell'altro produce razzismo. C'è anche la paura delle pandemie che da sempre affliggono l'umanità come l'attuale coronavirus. La paura dell'ignoto attraversa tutta la nostra storia.

Nel settore giudiziario, i processi in molti paesi sono stati digitalizzati, con un notevole risparmio di tempo e di energia, eliminando lo scambio di documenti cartacei e riducendo le udienze processuali in presenza.

Questo ha portato ad accese dispute sul fatto che un robot sia accettabile come giudice. Si noti che non è necessario che sia un robot, è sufficiente un programma complesso, come quello di *Watson*, e specializzato.

L'idea del robot, ad esempio, accompagna le paure della comunità ebraica dall'idea del Golem. Poi venne l'idea di Frankenstein il mostro o nuovo Prometeo creato con pezzi di cadaveri. Inutile dire che è un personaggio di un romanzo creato da Mary Shelley, ma le nostre paure ataviche stanno alla base di questi personaggi di fantasia, oggi rappresentati dal robot, parola che "deriva" dal ceco e significa servitù o lavoro forzato, termine usato nell'Impero austro-ungarico a metà dell'Ottocento.

Il robot evoca paure ancestrali, a partire al Golem della tradizione ebraica che appare citato una sola volta nell'Antico Testamento, cioè nel Salmo 139, versetto 16, là dove si legge: «Ancora informe mi hanno visto i tuoi occhi e tutto era scritto nel tuo libro; i miei giorni erano fissati, quando ancora non ne esisteva uno». Quell'embrione, secondo una interpretazione, è il Golem, ma anche Adamo. In ebraico, la lingua originale dell'Antico Testamento, l'origine della figura del Golem si colloca dove la Cabbala (tradizione) cerca i suoi significati.

Nelle origini c'è una connessione etimologica tra Adamo, creato da Dio, e la terra, concepita come metonimia nella sua componente di polvere. Adamo davanti al suo Creatore arriva alla perfezione spirituale che lo rende una figura animata e dotata di intelletto, debitamente umano, è Adamo - terra - Golem. Il golem (golmi) è una forma aggettivale che nella Bibbia appare una sola volta nel salmo citato.

Le letture di Midrash soddisfano quindi la coniugazione tra l'aspetto umano (e paradigmatico) e l'aspetto non umano, inorganico e materiale.

Lo stato golemico è attribuito ad Adamo stesso. È importante percepire questa differenza: nello stato organico, primitivo, c'è la materia ma l'uomo non c'è ancora, verrà più tardi, traendo il suo respiro dall'alito divino. E questa stessa differenza si crede che si veda nei robot, che sono materia (che in alcuni casi possono avere una forma umanoide) ma mancano dell'azione che appare in seguito attraverso programmi speciali tra i quali ci sono anche programmi di apprendimento. E questo fa temere a chi non conosce la robotica e i limiti dell'intelligenza artificiale che il robot diventi gradualmente indipendente e più intelligente dell'uomo e finisca per dominarlo.

La filosofia ebraica medievale usa il Golem come termine per indicare la materia informe. C'è una predisposizione a passare alla trasmigrazione da cui apparirà l'aspetto delle sembianze umane di Adamo. Il più emblematico e famoso caso è nel romanzo *Der Golem* di Gustav Meyrink, 1914, ambientato nel ghetto di Praga. Qui il Golem è chiamato a rappresentare l'anima del gruppo che aggiunge in sé l'esperienza della paura e dell'oppressione e, in secondo luogo, il Golem è libero dalla materia da cui proviene. In ebraico la parola *ot* significa non solo lettera, nella sua forma femminile, ma anche segno, nella sua

forma maschile. Al plurale, la forma maschile *otot* indica segni divini, nel senso di prodigi, anche le lettere sono segni che provengono dalle loro cause, cioè dalle radici delle cose, e vengono rispediti ad esse. Il femminile al plurale *ottiyyot* può essere inteso come "ciò che sta arrivando". I segni sono impressioni che danno forma alla realtà a loro immagine. Il Golem è costruito e reso vitale dal corretto uso delle lettere (*otot*) del Nome Divino.

Dal Golem al Cyborg, giocatore di scacchi, si delinea il percorso di reindirizzamento della variegata tipologia di vita antropomorfa e artificiale alla "mera" fabbricazione di automi: il robot indica solo la macchina che esonera dal lavoro manuale (per lavorare, in ceco *roboti*).

Il Golem talmudico va in Europa orientale, utilizzando l'artificio della pseudoepigrafia. Una prima visione leggendaria, non lontana dalla magia, appare in Polonia da Elijah Ba'al Shem, rabbino di Chelm, che poi nell'ottocento passa in Germania. Vi è anche una seconda raccolta praghese nel Settecento dal Rabi Low e poi nel 1837 con le leggende ebraiche Sippurin: qui il conflitto è tra creatore e creato, la ribellione del Golem e la possibilità di dare e togliere la vita. Poi nel Novecento il Golem appare positivamente come salvatore del popolo ebraico.

C'è poi l'altro tema della introduzione di elementi inorganici per rendere l'organico più forte, abile, intelligente.

Il matrimonio tra organico e inorganico appare nelle discussioni socialmente e culturalmente accreditate del passato dell'Occidente prima di Mary Shelley (autrice di Frankenstein) e nelle preoccupazioni gotiche del romanticismo di Byron.

Il Golem rappresenta la necessità di difendere un popolo immerso in contesti nazionali minacciosi come quello del ghetto di Praga.

La vita artificiale, la moltiplicazione del potere umano attraverso una creatura che incarna una conoscenza magica esoterica, la difficoltà di controllare ciò che gli esseri umani hanno creato. La caratteristica positiva dei mezzi di produzione straordinari della creatura artificiale deriva dall'eccezionalità del popolo eletto rispetto a Dio: "ciò che noi israeliti facciamo è miracoloso e buono, ciò che voi pagani fate è magico ed è cattivo"[10].

Il nostro corpo è caratterizzato dalle sinergie che si sono sviluppate nel corso di miliardi di anni, sfruttando meccanismi biologici attualmente non riproducibili nei robot e il rapporto cervello-corpo. L'essere umano ha un sistema che si è ottimizzato in miliardi di anni di evoluzione, un periodo di tempo in cui l'essere umano ha sviluppato una straordinaria capacità di adattamento e di apprendimento. Il divario che la tecnologia deve colmare per poter competere con i risultati dell'evoluzione umana è ancora enorme. Il cervello umano lavora in sinergia con il corpo umano: lo stesso gruppo di neuroni che controlla la vista controlla anche la manipolazione; il gruppo che controlla il linguaggio controlla la comprensione del parlato, e così via. Attualmente, è impossibile trasferire le sinergie di attuazione della mente – tipiche dell'uomo – alle macchine, perché l'intelligenza elettronica e i corpi meccatronici funzionano con meccanismi diversi da quelli biologici.

È importante discutere di cose rilevanti per la vita umana, come il modo in cui l'uomo ha sempre usato la tecnologia per modificare l'ambiente e rendere la sua vita più facile. Nessuno ha mai pensato se una ruota sarebbe stata migliore o più importante di un contadino che l'ha usata. Il cervello umano è una "palla" del peso di circa 1.500 grammi, alimentata dal metabolismo degli zuccheri con poche decine di watt! Pertanto, con gli standard tecnologici odierni, è impossibile assumere un sistema semovente capace di pensare come gli esseri umani, con le stesse capacità mentali e biomeccaniche. Non abbiate paura, siamo lontani dal produrre macchine che possano guidare la nostra vita e domarla.

Dobbiamo anticipare e dirigere lo sviluppo etico dell'innovazione tecnologica. E possiamo farlo guardando a ciò che è realmente fattibile, privilegiando, all'interno di esso, ciò che è sostenibile dal punto di vista ambientale, poi ciò che è socialmente accettabile e poi, idealmente, scegliendo ciò che è socialmente preferibile e compatibile con la sostenibilità della biosfera, per cui la nostra attuale equazione è incompleta.

Abbiamo dimostrato che il processo decisionale è sempre più aiutato dai programmi digitali e che spesso possono farlo direttamente se c'è un controllo sufficiente prima, durante e dopo la decisione.

Abbiamo visto che il diritto è sempre stato vicino a formulazioni formalizzate, dalle epigrafi romane alla teoria dell'argomentazione, fino alla copiosa attività normalizzatrice del diritto degli ultimi quarant'anni.

La logica è stata uno strumento straordinario in questo passaggio e crediamo di aver dimostrato che la logica è puramente sintattica come i programmi per computer e questo spiega la capacità e la velocità del processo decisionale giuridico.

Viviamo in un'epoca di straordinaria crescita dell'informazione e della sua diffusione. L'espressione "big data" ha un significato specifico anche se non è trasparente per tutti. E qui appare la seconda caratteristica del nostro tempo: proprio come dopo Platone e molto di più dopo Gutenberg, il grande tema

era quello di rendere la popolazione alfabetizzata, oggi abbiamo un problema simile con la mancanza di conoscenza di una parte importante della popolazione dell'uso dei media informatici, che determinano la trasformazione di quasi tutte le attività e i servizi privati e pubblici (e-government).

Curiosamente, viviamo in un'epoca di cerniere in cui le tre culture coesistono sul pianeta Terra: orale, scritta e cibernetica. Ma quest'ultima ha una velocità di sviluppo e una forza di espansione che non consente i lunghi tempi di alfabetizzazione. Questo è un mondo esigente, ora! E il diritto e molte funzioni dello Stato non possono attendere tempi "ragionevoli" di conoscenza. Chi viene lasciato indietro sarà il *sottoproletario* del prossimo futuro: non nel 2100 ma nel 2050!

Il tema dell'intelligenza artificiale è diventato di moda, invadendo vari campi e innescando un ampio dibattito, ma è servito anche per un uso più diffuso delle relative applicazioni, anche se non senza critiche. Molte sono dovute a vecchie paure umane evocate dalla figura del Golem o da quella del Robot, ma alcune devono essere prese in considerazione perché il Robot non è buono solo perché è nuovo.

E, non meno importante, la diffusione della intelligenza artificiale si accompagna a problemi etici che non possiamo evitare.

Ovviamente dobbiamo occuparci adesso dei problemi etici o i nodi verranno al pettine più tardi. Smettiamola di discutere inutilmente se le macchine governeranno l'uomo, argomento per filosofi disoccupati, e occupiamoci di questioni concrete e molto vicine. Naturalmente qualsiasi programma, soprattutto se può imparare e ha direttive concrete relativamente al suo scopo, tenderà a realizzarlo sempre di più. Ma se si tratta di un software o, come l'immaginazione popolare vuole, un robot, il problema è che per realizzarlo occorre valutare i limiti etici che devono essere previsti[11].

6. L'etica

Il preferibile e il politicamente fattibile, e quindi, in ultima analisi, il giuridicamente applicabile, è ciò che gli agenti possono o non possono fare. A lungo termine, le persone (come utenti, consumatori, cittadini, pazienti, ecc.) sono limitate in ciò che possono o non possono fare; ad esempio, le aziende sono limitate dalla legge, ma quest'ultima è formata e limitata dall'etica, che è la prospettiva in cui le persone decidono in quale tipo di società vogliono vivere.

Purtroppo questa proliferazione normativa diventa evidente soprattutto quando c'è una reazione violenta, cioè, soprattutto in contesti negativi, quando il pubblico rifiuta alcune soluzioni, anche quando possono essere buone. Ne consegue che l'etica in generale e l'etica digitale in particolare non possono essere un semplice complemento, un ripensamento, un gufo di Minerva che vola solo quando le ombre della notte si radunano. Le questioni etiche sono importanti, riguardano tutti gli *stakeholder* interessati e, soprattutto, forniscono soluzioni condivise.

L'etica digitale deve informare le strategie per lo sviluppo e l'uso delle tecnologie digitali fin dall'inizio, deve indicare quando cambiare il corso delle azioni è più semplice e meno costoso, mescolando risorse e impatto. Deve essere portata al tavolo della politica e delle procedure decisionali fin dal primo giorno. Perché non solo dobbiamo pensare due volte, ma, cosa ancora più importante, dobbiamo pensare prima.

La direttiva europea del maggio 2019 (Direttiva 2009/770) sulle transazioni informatiche, dopo tre anni di discussioni e trattative, riempie un orizzonte non solo europeo ma anche globale, giacché viene presa sul serio nell'organizzazione delle transazioni in molti paesi. Ed è un contributo universale[12].

Prima di legiferare è necessario pensare seriamente a ciò che sarà permesso o proibito, la nostra paura del nuovo non può indurci a commettere gravi errori.

Invece di avere paure ancestrali di fatture, magie, creazione di Golem che poi non riusciamo a dominare, la ricetta oggi dovrebbe essere di studiare quanto si sta facendo e utilizzare il meglio per migliorare le condizioni della vita umana, compresa la garanzia di una giustizia agevole, rapida e affidabile dove l'uomo, giudice, procuratore, avvocato raggiunge il meglio delle sue conoscenze facendosi aiutare da quanti strumenti software o robotici ci sono e ci saranno. Aiutare a decidere meglio contribuirà anche a creare verso le istituzioni quella fiducia che oggi manca.

Ci serviremo e ci serviamo già di congegni d'intelligenza artificiale per prendere decisioni o aiutarci a prenderle in un mondo nel quale l'uomo adopera sempre di più le macchine, anche nel proprio corpo. La paura verso i robot e, in generale, i programmi di decisione o aiuto alla decisione proviene di solito da soggetti che sanno poco d'intelligenza artificiale e che esaltano tutto quello che non sanno.

Il tema è piuttosto quello di come aiutare l'umanità in questo periodo difficile di distruzione del pianeta, di crisi economica e di improduttività della amministrazione pubblica, compresa quella giudiziaria.

Tutto ciò è detto secondo la massima greca, che appare nell'oracolo di Delfi: ΜΗΔΕΝ ΑΓΑΝ (Χρόνου φείδου), *Niente di troppo*, che i romani esprimevano con l'espressione *Ne quid nimis*.

7. Bibliografia

Adams E.S., Farber D.A., *Beyond the Formalism Debate: Expert Reasoning, Fuzzy Logic, and Complex Statutes*, in "Vanderbilt Law Review", vol. 52, p. 1243-1340, 1999.

Agustí J., *El paradigma de la interacció*, in "Butlletí de l'Associació Catalana de Intelligència Artificial (ACIA)", vol. 20, p. 12-18, 2000.

Aibar E., *Inteligencia Artificial y Sistemas Expertos: nuevas perspectivas y viejos dogmas sobre el conocimiento*, in "Arbor", p. 69-92, 1992.

Aikenhead M., *The Uses and Abuses of Neural Networks in Law*, in "Santa Clara Computer and High Technology Law Journal", vol. 12, p. 31-70, 1996.

Alchourrón C.E., Martino A.A., *Lógica sin verdad*, in "Theoria", vol. 3, n. 7, 1978.

Allen L.E., Caldwell M.A., *Modern Logic and Judicial Decision Making; A Sketch of One View*, in "Law and Contemporary Problems", n. 28, p. 213-270, 1963.

Andreewsky E. *et al.*, *Systémique et cognition*, Dunod, 1991.

Andreewsky E., Fluhr C., *Apprentissage et analyse automatique du langage. Application à la documentation*, in "Documents de linguistique quantitative", n. 21, Dunod, 1972.

ATP-CNRS, *Responsabilité des dirigeants de sociétés dans trois pays de les Communautés européennes*, CNRS éditions, 1976.

Barragán J., *Informática y Decisión Jurídica*, Fontamara, 1994.

Barriuso Ruiz C., *Interacción del derecho y la informática*, Dykinson, 1996.

Berry M.J.A., Linoff G., *Data Mining for Marketing, Sales, and Costumer Support*, John Wiley & Sons, 1997.

Bauza M., *Informática jurídica en una Facultad de Derecho. Roles y perspectivas*, in "REDI. Revista electrónica de derecho informático", n. 6, 1999.

Bing J., *Text Retrieval in Norway*, in "Program", vol. 15, n. 3, p. 150, 1981.

Bing J., *Impact of legal information automatisation on the practice of an attorney*, in R. Denoix de Saint Marc (ed.), "Savoir innover en droit. Concepts, outils, systèmes. Hommage à Lucien Mehl", La Documentation Française, 1999.

Bourcier D., *De l'intelligence artificielle à la personne virtuelle: émergence d'une entité juridique*, in "Droit et Société", vol. 49, p. 847-871, 2001.

Bourcier D., Clergue G., *From a rule-based conception to dynamic patterns. Analyzing the self-organization of legal systems*, in "Artificial Intelligence and Law", n. 7, p. 211-225, 1999.

Bourcier D., Hassett P., Roquilly Ch. (eds.), *Droit et Intelligence artificielle. Une Révolution de la Connaissance Juridique*, Romillat, 2000.

Bourcier D., MacKay P. (eds.), *Lire le Droit. Texte, Langage, cognition. Droit et Société*, Librairie générale de droit et de jurisprudence, 1992.

Bourcier D., Thomasset C. (eds.), *L'écriture du droit. Législation et technologie de l'information*, Diderot Editeur, Arts et Sciences, 1996.

Bourcier D., van Andel P., *Serendipity and Abduction in Proofs, Presumptions, and Emerging Laws*, in "Cardozo Law Review", vol. 22, p. 1605-1620, 2001.

Cantú R., *La Informática Jurídica en las Facultades de Derecho de América Latina*, in "REDI. Revista electrónica de derecho informático", n. 12, 1999.

Cantú R., *Tendencias actuales de la Informática y el Derecho a nivel Internacional*, in "REDI. Revista electrónica de derecho informático", n. 18, 2000.

Casanovas P., Moreso J.J., *Argumentació i pragmàtica del dret*, Ediuoc, 1998.

Chouraqui A., *L'informatique au service du droit*, PUF, 1974.

Damasio A.R., *Descartes' Error: Emotion, Reason and the Human Brain*, Grosset/Putnam, 1994.

Ducrot O., *Le dire et le dit*, Minuit, 1984.

Feteris E.T., Prakken H., *Introduction: Dialectical legal argument: Formal and informal models*, in "Artificial Intelligence and Law", n. 8, p. 107-113, 2000.

Feteris E.T., *A dialogical theory of legal discussions: pragma-dialectical analysis and evaluation of legal argumentation*, in "Artificial Intelligence and Law", n. 8, p. 115-135, 2000.

Frissen P.H.A. *et al.* (eds.), *European Public Administration and Informatization*, IOS Press, 1992.

Galindo F., *Derecho e informática*, La Ley-Actualidad, 1998.

Garrido M., *Lógica simbólica*, Ariel, 1976.

Goldin D., Keil D., Wegner P., *A Historical Perspective of Interactive Computing*, 2002.

Grauband S.R., *El nuevo debate sobre la inteligencia artificial, sistemas simbólicos y redes neuronales*, Gedisa, 1993.

Gray G.B., Mac Lennan B.J., Nolt J.E., Ploch D.R., *Legal Expert System Building: A Semi-Intelligent Computer Program Makes It Easer*, in "John Marshall Journal of Computer & Information Law", p. 555-583, 1994.

Hassett P., *Technology Time Capsule: What Does the Future Hold*, in "Syracuse Law Review", vol. 50, p. 1223-1242, 2000.

Henry B. *Dal Golem al Cyborgs*, Salvatore Belforte, 2013.

Herberger M., *Applications of Information Technology in the Legal Field: Success, Failures and Priorities for the Future*, in Proceedings of the 26th Colloquy on European Law "Changes in Law and Information Technology: Policies, Strategies and People" (18-20 June, Stockholm, 1996), 1998.

Hess Ch., *Inteligencia Artificial y Derecho*, in "REDI. Revista Electrónica de Derecho e Informática", n. 39, 2000.

Hofstadter D., *Fluid Concepts and Creative Analogies. Computer Models and the Fundamental Mechanisms of Thought*, Basic Books, 1995.

Hollatz J., *Analogy making in legal reasoning with neural networks and fuzzy logic*, in "Artificial Intelligence and Law", n. 7, p. 289-301, 1999.

Hunter D., *Out of their minds: Legal theory in neural networks*, in "Artificial Intelligence and Law", n. 7, p. 129-151, 1999.

Kloosterhuis H., *Analogy argumentation in law: A dialectical perspective*, in "Artificial Intelligence and Law", n. 8, p. 173-187, 2000.

Kort F., *Predicting Supreme Court Decision Mathematically: A Quantitative Analysis of the «Right» to Counsel «Cases»*, in "American Political Science Review", n. 51, 1957.

Lakoff G., *Women, Fire and Dangerous Things*, University of Chicago Press, 1987.

Loevinger L., *Jurimetrics: the next step forward*, in "Minnesota Law Review", n. 33, p. 455-493, 1949.

Loevinger L., *Jurimetrics: Science and Prediction in the Field of Law*, in "Minnesota Law Review", n. 46, 1961.

Losano M.G., *La informática y el análisis de los procedimientos jurídicos*, Centro de Estudios Constitucionales (Cuadernos y Debates, n. 33), 1991.

Martino A.A., *Sistemas expertos legales*, in "Revista de Informática y Derecho", vol. 1, 1987.

Martino A.A., *La nueva cultura digital, la política y el derecho. El futuro está aquí*, in "REDI. Revista electrónica de derecho informático", n. 6, 1999.

Martino A.A., *Expert Systems in law*, North Holland, 1992.

McJohn S.M., *Artificial Legal Intelligence*, in "Harvard Journal of Law and Technology", vol. 12, p. 241-261, 1998.

Minsky M., *La sociedad de la mente. La inteligencia humana a la luz de la inteligencia artificial*, Galápagos, 1986.

Newell A., *Inteligencia artificial y el concepto de mente*, Teorema, 1980.

Onn S., Tennenholtz M., *Determinaton of social laws for multi-agent mobilization*, in "Artificial Intelligence", n. 95, p. 155-167, 1997.

Pérez Luño A.E., *Manual de informática y derecho*, Ariel, 1996.

Philipps L., Sartor G., *Introduction: From legal theories to neural networks and fuzzy reasoning*, in "Artificial Intelligence and Law", n. 7, p. 115-128, 1999.

Simon D., *A Psychological Model of Judicial Decision Making*, in "Rutgers Law Journal", vol. 30, p. 1-142, 1998.

Simon H.A., *The Sciences of the Artificial*, MIT Press, 1991.

Simon H.A., Kaplan C., *Foundations of Cognitive Science*, in M.I. Posner (ed.), "Foundations of Cognitive Science", MIT Press, 1989.

Smith J.S., *Machine Intelligence and Legal Reasoning*, in "Chicago-Kent Law Review", vol. 73, p. 278-347, 1998.

Susskind R., *The Future of Law. Facing the Challenges of Information Technology*, Clarendon Press, 1996.

Susskind R., *Transforming the Law: Essays on Technology, Justice and the Legal Marketplace*, Oxford University Press, 2000.

Taruffo M., *Judicial Decisions and Artificial Intelligence*, in "Artificial Intelligence and Law", n. 6, p. 311-324, 2001.

Tennenholtz M., *On stable social laws and qualitative equilibria*, in "Artificial Intelligence", n. 102, p. 1-20, 1998.

Visser P.S., Bench-Capon T.J.M., *A Comparison of Four Ontologies for the Design of Legal Knowledge Systems*, in "Artificial Intelligence and Law", n. 6, p. 27-57, 1998.

Walton D., *The New Dialectics. Conversational Contexts of Argument*, University of Toronto Press, 1998.

Walton D., *One-Sided Arguments. A Dialectical Analysis of Bias*, State University of New York Press, 1999.

Note

[1]Se qualcuno pensa che mi riferisca a Youval Harari e al suo *21 lezioni per il XXI secolo*, Bompiani, 2018, ha perfettamente ragione. Però non mi riferisco solo a questo tipo di paura.

[2]I robot soffici sono i robot di ultima generazione che sono progettati alla Scuola Superiore Sant'Anna di Pisa da Cecilia Laschi e Barbara Mazzolai.

[3]Il 20 maggio 2020 per la prima volta una sessione della Corte Suprema americana è stata trasmessa on line.

[4]Il *qubit* si comporta in modo molto più complesso di quello classico. Questo definisce l'importanza dei sistemi quantistici per l'informatica. Possiamo immaginare un *qubit* come un vettore. La lunghezza di questo vettore è fissa, ma può puntare in qualsiasi direzione, a differenza del classico bit, che può solo puntare, diciamo, verso l'alto e verso il basso.

[5]*Prometea* è un sistema di IA creato nell'ambito della Procura della Repubblica del CABA. Con competenze che vanno dall'automazione alla previsione, è stato originariamente costruito pensando all'ottimizzazione della giustizia, anche se ha dimostrato che potrebbe essere interessante per altri settori. Utilizza tecniche di *machine learning* e *clustering* supervisionate; funziona come un sistema esperto per automatizzare la creazione di documenti, eseguire ricerche intelligenti e assistere nel controllo dei dati; ha un'interfaccia intuitiva e amichevole che permette di "parlare" al sistema o di chattare.

[6]Io stesso lo utilizzo per un prodotto che si chiama "ragionatore giuridico", ancora in fase di sviluppo finale, scritto con Python.

[7]Cfr. L. Margulis, D. Sagan, *¿Qué es la vida?*, Tusquest Editores, III ed., 2009.

[8]E questo mi fece capire due cose: (1) SRL o qualsiasi altro programma può dirsi razionale fin tanto che calcola correttamente, ma gli manca la capacità di ponderare tra l'importante e il secondario, tra ciò che ragionevolmente si verificherà e ciò che non si verificherà. Quindi non è ragionevole. (2) Non è corretto dire "questa è una conseguenza non voluta dalla legge". Una volta dettata la legge, le conseguenze stanno tutte nella norma.

[9]Un pregiudizio cognitivo è un effetto psicologico che produce una deviazione nell'elaborazione mentale, che porta a una distorsione, a un giudizio impreciso, a un'interpretazione illogica, o a quella che viene generalmente chiamata irrazionalità, che si verifica sulla base dell'interpretazione delle informazioni disponibili, anche se i dati non sono logici o non sono correlati tra loro.

[10]Questo e altri dati relativi sono dovuti al bel libro di B. Henry, *Dal Golem al Cyborgs*, Salvatore Belforte, 2013.

[11]Nel 2020 in Vaticano è stato firmato un accordo europeo per porre limiti etici all'intelligenza artificiale.

[12]Poiché oggi è facile profilare e prevedere gli errori sulla base delle ripetizioni di casi simili, esistono programmi che lo fanno in modo molto preciso. Purtroppo vi è una legge francese che lo vieta. È stupido come proibire la respirazione, continueranno a farlo come abbiamo sempre fatto noi, ricorrendo alla giurisprudenza, prima che il computer apparisse.

* * *

Who fears the robot judges

Abstract: The use of artificial intelligence in law has been analyzed from different point of view, one of the most interesting being that based on Georg H. von Wright seminal works that inspired also some research activities in the Institute for Legal Documentation (IDG) of the National Research Council of Italy in 1980s and 1990s. Forty years have been passed and many things have changed and brought new challenges. There is a large exploitation of electronic data and information in many areas of law and justice and there are very advanced ICT tools supporting legal professionals. Even there are doomsayers who predict the dominion of machines over men. They forget something that is constant and that cannot change: fear is connatural to human life, the fact is whether it blocks us or allows us to move forward, even with fear. The fear that machine will replace man for the time being is exaggerated.

Keywords: Artificial intelligence and law – Artificial intelligence and judicial system – Legal decision and artificial intelligence – Robotics

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

ISSN 2704-7318
Fascicolo 2-2020
DOI: 10.32091/RIID0025

La lama della rete. Forme della violenza contro le donne sul web

Serena Vantin*

In uno scenario sempre più connotato dall'impatto delle tecnologie su nozioni e processi giuridici, lo spazio virtuale non rappresenta una garanzia per la promozione dell'eguaglianza tra i generi. A questo proposito, il contributo si sofferma sulle nuove forme e articolazioni che la violenza contro le donne assume sul web, per giungere a delineare possibili strategie di contrasto nel solco della normativa vigente.

Eguaglianza di genere – Violenza – Violenza virtuale – "Codice Rosso"

Sommario: *1. Premessa – 2. Il mondo della rete – 3. Diseguaglianze e violenza – 4. Azioni di contrasto – 5. Il "Codice Rosso" – 6. Riflessioni conclusive*

1. Premessa

Lo scenario contemporaneo è fortemente connotato dall'impatto delle tecnologie su nozioni e processi giuridici, nonché sui fenomeni di una realtà sempre più "digitale" che il diritto cristallizza, disciplina e interpreta[1].

In questa cornice, lo spazio della rete non è un campo incontaminato, né una garanzia per la promozione dell'eguaglianza e della parità tra i generi. Si deve, in particolare, a Jo Freeman e Amanda Hess il merito di aver contribuito a diffondere la consapevolezza della soltanto apparente «assenza di struttura» del web[2]: nonostante i buoni propositi universalistici della Dichiarazione d'Indipendenza del Cyberspazio[3], la stessa "architettura" della rete sarebbe responsabile della marginalizzazione di alcuni utenti a vantaggio delle medesime gerarchie che strutturano la realtà sociale.

A questo proposito, dopo una breve premessa di inquadramento, nel corso del presente contributo proverò ad articolare una riflessione su alcuni rischi della rete, sia in termini di eguaglianza tra i sessi sia con riguardo alle nuove forme della violenza contro le donne all'epoca di internet, per giungere infine a presentare possibili strategie ed azioni di contrasto nel solco della normativa vigente.

2. Il mondo della rete

Com'è noto, non c'è aspetto della vita che non sia stato trasformato dalle tecnologie[4]. Il paradigma della "rete" è diventato un modello per tutte le forme dell'interazione umana, là dove la stessa separazione tra "mondo fisico" e "mondo virtuale" risulta ormai superata dalla nuova realtà cd. «on-life»[5], nella quale esseri umani, macchine e oggetti risultano perennemente connessi.

In una tale nuova realtà, l'unità psichica e fisica del soggetto razionale, personificata e personificabile, sta cedendo il passo a un nuovo sé "fluido", diviso in componenti inessenziali, pezzi (*bit*), dati, tracce, meta data, Big Data. Un "fiume", una "corrente" o un "flusso" sono, infatti, le metafore più appropriate per descrivere la nuova identità digitale, concepita

*Serena Vantin è assegnista di ricerca in Filosofia del diritto presso il Dipartimento di Giurisprudenza dell'Università di Modena e Reggio Emilia e Responsabile della Segreteria scientifico-organizzativa presso il CRID - Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità.

come un sistema informazionale complesso, composto di attività, ricordi e storie, la cui coscienza viene al contempo, costantemente, plasmata ed espressa[6].

In questo contesto, la rivoluzione digitale sembra in grado di offrire inediti spazi di libertà, autodeterminazione, autonomia e parità – si pensi all'opportunità di utilizzare il web in termini di *community building* e dunque di *empowerment*[7]. Al contempo, però, essa pare accrescere il novero delle forme del dominio alimentando diseguaglianze e violenza[8].

In particolare, quando rivolta contro le donne, la violenza è sovente declinata in aggressioni verbali, insulti, retoriche sessiste stereotipate, ricerca e pubblicazione online di informazioni personali e private (*doxing*), pornografia indesiderata, stigmatizzazione a sfondo sessuale, intimidazioni, minacce di aggressione e di morte, ma anche condotte e atteggiamenti misogini "punitivi" o comunque gravemente lesivi della reputazione e della dignità della vittima, quali atti di *cyberstalking*, pornografia non consensuale o di vendetta, offese e molestie basate sul genere, estorsione sessuale, trasmissione online di atti di aggressione sessuale e stupro, traffico di esseri umani perpetrato con adescamento in via elettronica, e così via[9].

Solo in tempi recenti, l'Istituto Europeo per l'Eguaglianza di Genere ha sollevato il problema della violenza cd. «virtuale» contro donne e ragazze[10], denunciando la difficoltà nel reperimento di dati disaggregati rispetto al genere ma anche enfatizzando l'altissima percentuale di vittime nonché la significativa gravità dei danni che ne derivano. Una ricerca del 2017 ha, inoltre, messo chiaramente in evidenza che la violenza in rete deve essere intesa come un «continuum» rispetto a quella fisica, da cui non va dissociata, anche perché capace di provocare ripercussioni «reali» sulla vita delle persone coinvolte[11]. Anche sul web, pertanto, il connubio tra diseguaglianze di genere e violenza contro le donne appare evidente.

3. Diseguaglianze e violenza

In primo luogo, è ormai dimostrata l'esistenza di un "digital gender divide", o divario digitale di genere, quale conseguenza di già consolidate differenze socioeconomiche tra i sessi (soprattutto in termini di occupazione e reddito), le quali renderebbero gli strumenti ICT più accessibili ai soggetti in condizioni già più avvantaggiate[12].

A tal riguardo, i dati divulgati annualmente dal World Economic Forum mediante i Global Gender Gap Reports sono per molti aspetti allarmanti. L'Italia, nel 2020, si è trovata al 76° posto (su 153 paesi), dopo Georgia e Thailandia e prima del Suriname[13]: le diseguaglianze tecnologiche andrebbero lette all'interno di questo più ampio quadro di svantaggio.

Roberta Bracciale descrive un tale scenario come segue: *i soggetti più "ricchi" di risorse personali accedono ai benefici dell'«effetto San Matteo», una moltiplicazione cumulativa dei vantaggi che segue la logica dell'«a chi ha verrà dato», i soggetti più "poveri", al contrario, soffrono di un processo di moltiplicazione cumulativa degli svantaggi, l'«effetto Matilda», che supporta l'argomentazione dell'«a chi non ha, verrà tolto anche quello che ha»*[14].

Inoltre, in aggiunta a diseguaglianze già consolidate, pare che il *gap* venga altresì supportato da "nuovi" fattori culturali e stereotipi di genere[15], che influenzerebbero le attitudini dei "soggetti tecnologici", indirizzando, sin dalla più giovane età, gli uni verso una maggiore propensione alla tecnologia, le altre verso una «fuga» dalla stessa[16].

Come sottolineano importanti studi[17], i pregiudizi che allontanano le donne dai settori tecnologici paiono profondamente radicati e comportano un alto rischio di ulteriori esclusioni, nonché un'esposizione a potenziali discriminazioni, nell'ambito di una sfera che ormai anche la giurisprudenza ha iniziato a considerare «fondamentale in ogni ambito della vita umana» (Giudice di Pace di Trieste, 587/2012[18]).

In secondo luogo, è drammaticamente risaputo che in rete vivono e proliferano "bolle" composte da gruppi, chat, forum, siti che incitano alla violenza contro le donne, alimentando un circuito sia generato sia sospinto da sentimenti sessisti di odio e disprezzo[19].

Ormai diverse ricerche rilevano che sarebbe proprio la conformazione del web, e degli spazi "chiusi" in esso celati, nonché la presunzione di agire coperti da anonimato, a potenziare ed esasperare il risentimento e l'odio[20].

Nel nostro Paese, l'Osservatorio Vox Diritti segnala che, nel 2019, il 63,1% dei tweet d'odio si è scatenato contro le donne[21]; mentre il "Barometro dell'odio" di Amnesty International registra che, quando il tema è "donne e diritti di genere", un commento online su tre ingenera *hate speech* e discorsi sessisti[22]. Un recente studio della American Psychological Association[23], anche citato dall'Osservatorio sulla Cyber Security dell'Eurispes[24], rileva che in caso di *revenge porn* – una forma di violenza sessista devastante per la reputazione e per l'integrità psichica della vittima[25] – il 51% delle donne contempla il ricorso al suicidio.

4. Azioni di contrasto

Il contrasto a questi fenomeni si inserisce nel quadro, ormai quarantennale, di una normativa internazionale scandita dagli auspici della "Convenzione per l'eliminazione di tutte le forme di discriminazione contro le donne" (CEDAW) del 1979 e, successivamente, dalla "Dichiarazione sull'eliminazione della violenza contro le donne" (1993) – auspici poi ribaditi dalla "Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica" del Consiglio d'Europa (c.d. Convenzione di Istanbul, 2011[26]).

Queste fonti hanno avuto il merito di evidenziare il nesso tra le discriminazioni contro le donne e le violenze da esse subìte, proponendo strumenti di contrasto, repressione ma anche di prevenzione. A tal riguardo, l'art. 3 della Convenzione di Istanbul qualifica, estensivamente, la violenza contro le donne come «qualsiasi violenza diretta contro una donna in quanto tale, o che colpisce le donne in modo sproporzionato»[27]: una disposizione che pare atta a includere anche le nuove articolazioni che misoginia e odio assumono negli spazi digitali.

Tuttavia, inquadrare e sanzionare la violenza digitale è un compito tutt'altro che semplice, soprattutto con riferimento alla violenza verbale, talvolta situata sulla soglia della tutela della libera espressione[28]. A tal proposito, la Corte di Cassazione ha stabilito che la critica diviene illecita quando comporta «un'aggressione gratuita e distruttiva dell'onore e della reputazione dell'interessato» (Cass. Civ. 12420/2008).

Su questo versante, profili estremamente problematici emergono con riferimento alla responsabilità dell'internet service provider rispetto a contenuti generati o diffusi dai propri utenti. Infatti, ai sensi della Direttiva europea sul commercio elettronico (2000/31/CE), recepita nel nostro ordinamento con il d. lgs. 70/2003, è possibile individuare una responsabilità extracontrattuale[29] in capo al provider (ex art. 2043 c.c.) ma è escluso un obbligo generale di sorveglianza o monitoraggio, sia *ex ante* sia *ex post* (cfr. anche Corte Appello di Milano, sent. 29/2015; Tribunale di Napoli Nord, ord. cautelare 3 novembre 2016). D'altra parte, le autorità giudiziarie o amministrative possono richiedere al provider l'inibizione di contenuti illeciti, anche con procedura d'urgenza, ed è previsto un obbligo di informare l'autorità giudiziaria o amministrativa nel caso in cui il provider giunga a conoscenza di contenuti illeciti, con conseguente responsabilità in caso di inadempienza[30].

Risulta, tuttavia, particolarmente insidiosa la qualificazione della responsabilità dei social network e dei motori di ricerca, i quali non si limitano a svolgere attività "neutrali" di semplice trasporto di informazioni (*mere conduit*), memorizzazione temporanea (*caching*) e memorizzazione duratura (*hosting*) ma, profilando i gusti e le preferenze degli utenti, ovvero mettendo in risalto specifiche informazioni, possono essere inquadrati come «hosting provider attivi» (Cass. Civ. 7708/2019)[31].

Questi particolari provider non sono assimilabili a direttori responsabili di pubblicazioni periodiche ovvero agli editori o stampatori di pubblicazioni non periodiche (ai sensi degli artt. da 57 a 58-bis c.p.), in base al principio del divieto di interpretazione analogica della legge penale (Cass. Pen. 35511/2010; 31022/2015)[32], eppure sono soggetti all'obbligo di rimozione dei contenuti manifestamente illeciti di cui siano giunti a conoscenza (Cass. Pen. 54946/2016; Cass. Civ. 7708/2019)[33].

Mediante la Risoluzione del 23 novembre 2016 del Parlamento Europeo "sulla strategia della comunicazione dell'Unione per contrastare la propaganda di terzi che possa essere lesiva della democrazia, dello Stato di diritto e del rispetto dei diritti umani e delle liberta fondamentali"[34], nonché la successiva Comunicazione della Commissione Europea n. 555 del 2017, l'Unione Europea ha portato l'attenzione sulla necessità di cooperazione e di *due diligence* da parte di tutti i soggetti coinvolti nei processi comunicativi online. Sono emersi, in particolare, i principi di auto-regolazione e di co-regolazione[35], cui i principali internet provider (a cominciare da Facebook, Microsoft, Twitter e YouTube) hanno ritenuto di doversi assoggettare, al fine di contrastare la violenza verbale, i discorsi d'odio e la diffusione di contenuti pregiudizievoli per individui o gruppi[36].

A titolo di esempio, Facebook[37] ha introdotto una *policy* intitolata "Standard della Community"[38] finalizzata ad inibire la violenza e i comportamenti criminali, l'istigazione alla violenza, la pubblicizzazione di atti criminali, i contenuti deplorevoli, e così via, sulla base di un sistema che beneficia anche delle segnalazioni degli stessi utenti[39], che devono essere esaminate nell'arco di ventiquattro ore.

Eppure, nonostante gli sforzi intrapresi, queste recenti misure hanno avuto un'efficacia limitata e non paiono adeguate ad intervenire in termini preventivi[40]. Più ampiamente, il ricorso al *soft-law* non può essere ritenuto sufficiente, soprattutto là dove all'operato di privati si attribuiscano finalità di natura pubblicistica, non siano previste sanzioni né criteri valutativi e non siano chiari i tempi di intervento successivi al vaglio della segnalazione[41].

5. Il "Codice Rosso"

In una tale cornice, la legge 19 luglio 2019, n. 69 (cd. "Codice Rosso"[42]) ha introdotto nel nostro Paese «modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica o di genere», configurando quattro nuovi delitti tra i quali quello di «diffusione illecita di immagini o video sessualmente espliciti», destinati a rimanere privati, senza il consenso delle persone rappresentate (art. 612 *ter* c.p.)[43].

All'interno di questo reticolo di nuove e vecchie figure di reato, le cui pene sono state incrementate nel corso degli anni, il legislatore è andato inserendo nuove circostanze aggravanti, anche con l'obiettivo di adeguarsi alle richieste provenienti dalle fonti internazionali (*in primis*, dalla Convenzione di Istanbul)[44].

Per la verità, l'inasprimento delle pene, l'inserimento di circostanze aggravanti, come pure l'innalzamento delle cornici edittali, ovvero l'introduzione di limiti al giudizio di prevalenza di eventuali attenuanti concorrenti, hanno destato in letteratura non poche perplessità[45], dal momento che queste misure sembrano favorire una logica retributiva che pare perlopiù estranea alle donne vittime di quei reati, che dal sistema penale si aspettano prioritariamente una piena protezione là dove il fatto possa ripetersi in futuro[46].

Ad ogni modo, questi interventi normativi dovrebbero essere interpretati alla luce di quella cd. "funzione simbolica" del diritto[47] secondo la quale, in particolare per i fenomeni criminali più pervasivi e radicati, la risposta penale data al singolo episodio non esaurisce i suoi effetti nel caso concreto ma costituisce, anche agli occhi dei consociati, un tassello evidente di una strategia di contrasto più ampia, che deve essere portata avanti con convinzione *a più livelli*[48].

A quest'ultimo riguardo, restano decisivi gli indirizzi assunti dalla Convenzione di Istanbul, ed in particolare gli sforzi dedicati alla sensibilizzazione, all'educazione e alla formazione di figure professionali in materia, ma anche la previsione di una rete di servizi integrati di assistenza specializzata a supporto delle vittime[49].

Con specifico riferimento alla violenza virtuale, ciò risulta particolarmente urgente – là dove una serie di ricerche denunciano come del tutto inadeguate le risposte del settore della giustizia e delle forze dell'ordine in questo frangente, rivelando una tendenza alla minimizzazione o al trattamento individuale di ciascuna aggressione online piuttosto che una valutazione dell'impatto cumulativo degli abusi subìti[50].

Inoltre, con riferimento alle forme, peculiari, della violenza sulla rete, sembra necessario promuovere al più presto una organica specificazione delle misure preventive e di tutela. In particolare, occorre progettare, attivare e rendere capillarmente accessibili molteplici strumenti strutturali di prevenzione, tutela e protezione, capaci ad esempio di sensibilizzare le nuove generazioni di "nativi digitali"[51], ma anche di offrire assistenza psicologica e supporto tecnico a garanzia della cybersicurezza, oltreché di generare contro-narrazioni efficaci e riabilitative per la dignità delle vittime[52].

Infine, si ritiene essenziale colmare le lacune informative relative alla diffusione e alla gravità delle violenze contro donne e ragazze in rete, anche sviluppando ricerche volte ad individuare i fattori di rischio, al fine di attribuire priorità allo sviluppo di strumenti di misurazione e quantificazione di questi illeciti.

6. Riflessioni conclusive

In conclusione, la rivoluzione digitale e il mondo della rete, con il loro profondissimo impatto sulla realtà e sulla percezione del sé, hanno potenziato talune diseguaglianze di genere e forme della violenza sessista, rendendo ancor più profondo il discrimine tra dichiarazioni egalitarie di principio e realtà fattuale.

Nonostante alcuni recenti sforzi di carattere normativo, la complessità dei fenomeni ricordati rende evidente che, citando le parole di Luigi Ferrajoli, probabilmente «nessun meccanismo giuridico riuscirà da solo a garantire l'uguaglianza di fatto tra i sessi»[53]. Ciononostante, pare opportuno auspicare che la disciplina giuridica intenda mettere in cima alle sue priorità la lotta per il contrasto e la prevenzione della violenza di genere, anche nelle sue articolazioni virtuali.

Al momento, dal regime di responsabilità del provider sino alla riforma del "Codice Rosso", gli ambiti di intervento paiono ancora frastagliati e piuttosto disomogenei, poco inclini a cogliere le specificità dei fenomeni indagati, e, nel complesso, ancora incapaci di attuare una strategia uniforme. L'apertura al *soft-law*, nonché alla auto-regolazione di social network e motori di ricerca, in particolare, non deve rappresentare un alibi per ridimensionare il ruolo dell'ordinamento giuridico.

Note

[1]Una prima versione di questo testo è stata presentata nell'ambito della V edizione della Summer School di Marsala, il 26 agosto 2020, dove ho tenuto una relazione insieme al prof. Thomas Casadei, al quale si deve il titolo del contributo. Ringrazio per l'invito il prof. Giorgio Scichilone e la dr.ssa Luana Alagna dell'Univ. di Palermo. Ho presentato una successiva versione di questo studio in occasione del Convegno "Unimore contro la violenza. Violenza di genere, costi in termini di benessere e impatto della pandemia", il 25 novembre 2020 presso l'Università di Modena e Reggio Emilia. Ringrazio la prof.ssa Tindara Addabbo e la prof.ssa Claudia Canali per il coinvolgimento nell'iniziativa.

Ringrazio anche tutti i componenti dell'Officina Informatica "Diritto Etica e Tecnologie" del CRID – Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità dell'Università di Modena e Reggio Emilia per le numerose occasioni di confronto, e in particolare il prof. Gianfrancesco Zanetti, il prof. Thomas Casadei, il prof. Stefano Pietropaoli, il prof. Gianluigi Fioriglio, il prof. Michele Ferrazzano, il dott. Francesco De Vanna.

Per approfondimenti, si vedano, *inter alia* e in una letteratura in rapida espansione, S. Rodotà, *Il diritto di avere diritti*, Laterza, 2012; G. Ziccardi, *Resistance, Liberation, Technology and Human Rights in the Digital Age*, Springer, 2013; G. Peruginelli, M. Ragona, *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Edizioni Scientifiche Italiane, 2014; E. Stradella, E. Palmerini (eds.), *Law and Technology. The Challenge of Regulating Technological Development*, Pisa University Press, 2013; S. Rodotà, *Il mondo della rete. Quali diritti, quali vincoli*, Laterza, 2014; V. Colomba, *I diritti nel cyberspazio. Architetture e modelli di regolamentazione, con un saggio di L. Lessig*, Diabasis, 2016; G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Giappichelli, 2016; F. Faini, S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, Giappichelli, 2017; G. Fioriglio, *Trasformazioni del diritto. Alla ricerca di nuovi equilibri nell'esperienza giuridica contemporanea*, Giappichelli, 2017; A. Santosuosso, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, 2020; S. Amato, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, 2020; S. Faro, T.E. Frosini, G. Peruginelli, *Dati e algoritmi. Diritto e diritti nella società digitale*, Il Mulino, 2020; S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini, 2020.

[2]J. Freeman, *The Tyranny of Structurelessness*, 1971; A. Hess, *Why Does Hate Thrive Online? The Roots of Internet Culture Provide a Few Clues*, 2015.

[3]P.J. Barlow, A Declaration of the Independence of Cyberspace, 1996.

[4]Cfr. L. Floridi, *Pensare l'infosfera. La filosofia come design concettuale*, Raffaello Cortina, 2020, p. 219. Per ulteriori approfondimenti su questo tema, si rimanda al fascicolo Th. Casadei (a cura di), *Mondi della vita, rete, trasformazioni del diritto*, in "Ars interpretandi", 2017, n. 1.

[5]L. Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, 2014.

[6]Cfr. L. Floridi, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Raffaello Cortina, 2017, pp. 165-166.

[7]Sulle potenzialità liberatorie della rete e, più in generale, sui "Feminist Technology Studies" che si sono sviluppati valorizzando questo aspetto, cfr. D. Haraway, *A Cyborg Manifesto*, in "Socialist Review", 1985, pp. 65-108; J. Wajcman, *Feminism Confronts Technology*, Pennsylvania State University Press, 1991; C. Cockburn, *The Circuit of Technology: Gender, Identity and Power*, in R. Silverstone, E. Hirsch (eds.), "Consuming Technology: Media and Information in Domestic Spaces", Routledge, 1992, pp. 32-47; A. Balsamo, *Technologies of the Gendered Body: Reading Cyborg Women*, Duke University Press, 1998; W. Faulkner, *The Technology Question in Feminism: A View from Feminist Technology Studies*, in "Women's Studies International Forum", 2001, n. 1, pp. 79-95; J. Wajcman, *Technofeminism*, Polity Press, 2004; F. Bray, *Gender and Technology*, in "Annual Review of Anthropology", 2007, pp. 37-52; S. Puente, *From Cyberfeminism to Technofeminism: from an Essentialist Perspective to Social Cyberfeminism in Certain Feminist Practices in Spain*, in "Women's Studies International forum", 2008, n. 31, pp. 434-440; C. Åsberg, N. Lykke, *Feminist Technoscience Studies*, in "European Journal of Women's Studies", 2010, n. 4, pp. 299-305; M. Conceição Da Costa, R. Buzzo Feltrin, *Challenges of Intersectionality in Gender, Science and Technology*, in "Cadernos Pagu", 2016, n. 47, C. Cossutta, V. Greco, A. Mainardi, *Smagliature digitali. Corpi, generi e tecnologie*, Agenzia X, 2018; W.K. Bauchspies, M. Pig de la Bellacasa, *Feminist Science and Technology Studies: A Patchwork of Moving Subjectivities. An Interview with Geoffrey Bowker, Sandra Harding, Anne Marie Mol, Susan Leigh Star and Banu Subramaniam*, in "Subjectivity", 2009, n. 28, pp. 334-344.

[8]Cfr., su questi temi, A. Verza, *Aggredire attraverso l'immagine. Cristallizzazioni tecnologiche, genere e diniego di tutela nella logica disciplinante neoliberale*, in "Ragion Pratica", 2017, n. 2, pp. 467-492; A. Verza, *El mundo cibernético y las nuevas formas de violencia contra las mujeres*, in J.M. López Ulla, J. Sáez Gonzáles (eds.), "Combatiendo la violencia contra la mujer: experiencias europeas y americanas", Aranzadi, 2020, pp. 235-274. Si vedano anche, più ampiamente, *inter alia*, A. Pitino (a cura di), *Interventi di contrasto alla discriminazione e alla violenza sulle donne nella vita pubblica e privata. Un'analisi multidisciplinare*, Giappichelli, 2015; F. Rescigno (a cura di), *Percorsi di eguaglianza*, Giappichelli, 2016; S. De Vido, *Donne, violenza e diritto internazionale. La Convenzione di Istanbul del Consiglio d'Europa del 2011*, Mimesis, 2016; C. Pecorella (a cura di), *Donne e violenza. Materiali di studio*, Giappichelli, 2020. Si vedano anche i *report* curati dalla rete Di.Re – Donne in Rete contro la violenza.

[9]Su questi profili, si vedano G. Ziccardi, *L'odio online. Violenza verbale e ossessioni in rete*, Raffaello Cortina, 2016; G. Magistro, *Cyberbullismo*, Villaggio Maori, 2018; F. Di Tano, *Hate speech e molestie in rete. Profili giuridici e prospettive de iure condendo*, Aracne, 2019; A. Sorgato, *Revenge porn. Aspetti giuridici, informativi, psicologici*, Giuffrè, 2019; A. Di Rosa, *Hate speech e discriminazione. Un'analisi performativa tra diritti umani e teorie della libertà*, Mucchi, 2020.

[10]Cfr. EIGE, European Institute for Gender Equality, *Cyber Violence against Women and Girls*, 2017.

[11]*Ibidem*. Cfr. anche *Stop alla violenza online*, in "Amnesty International Italia", 2019.

[12]Si veda M. Hilbert, *Digital Gender Divide or Technologically Empowered Women in Developing Countries? A Typical Case of Lies, Damned Lies, and Statistics*, in "Women's Studies International Forum", 2011, n. 6, pp. 479-489.

[13]Cfr. World Economic Forum, *Global Gender Gap – Report 2020*, 2019.

[14]R. Bracciale, *Donne nella rete. Disuguaglianze digitali di genere*, Franco Angeli, 2010, p. 13.

[15]A questo riguardo, cfr. S. Pozzolo, R. Bencivenga, F. Bosco, *Genere e tecnologia: nuove capacitazioni o antichi pregiudizi mascherati?*, in "About Gender – Rivista internazionale di studi di genere", 2016, n. 9, pp. 1-14.

[16]Cfr. M. Hilbert, *op. cit.*, p. 482. Si veda anche M. Papastergiou, *Are Computer Science and Information Technology Still Masculine Fields? High School Students' Perceptions and Career Choices*, in "Computers & Education", 2008, n. 51, pp. 594-608.

[17]Cfr., *inter alia*, J. Wajcman, *Feminism Confronts Technology*, cit.; C. Cockburn, *op. cit.*; S. Pozzolo, R. Bencivenga, F. Bosco, *op. cit.*

[18]La sentenza n. 587/2012 del Giudice di Pace di Trieste, valutando il caso di una famiglia rimasta senza collegamento ADSL per un periodo di quattro mesi, qualificò internet come un bene fondamentale per ogni aspetto della vita quotidiana, individuando, in caso di violazione, non soltanto un danno patrimoniale ai sensi dell'art. 1226 c.c. ma anche un danno non patrimoniale cagionato dalle difficoltà conseguite al «danno esistenziale e morale [che aveva] inciso direttamente nella sfera emotiva e relazionale» degli interessati.

[19]La cd. *manosphere*: cfr. F. Pilla, R. Dolce, *Il web che odia le donne*, Ledizioni, 2019. Cfr. A. Sorgato, *op. cit.* Cfr. anche la campagna "End Revenge Porn" della *Cyber Civil Rights Initiative*.

[20]Cfr. F. Pilla, R. Dolce, *op. cit.* Si vedano anche Council of Europe, *Bookmarks. A Manual for Combating Hate Speech Online through Human Rights Education*, 2016; FRA - European Union Agency for Fundamental Rights, *Violence against Women: an EU-wide survey. Main Results*, 2014; Id., *Ensuring justice for hate crime victims: professional perspectives*, 2016; Id., *Incitement in media content and political discourse in EU Member States*, 2016.

[21]Cfr. Redazione Vox, *La mappa dell'intolleranza 2: l'odio contro le donne*, in "Vox - Osservatorio italiano sui diritti"; si veda anche Vox Diritti, *La mappa dell'intolleranza. Anno 4*, 2019.

[22]Cfr. *Barometro dell'odio: sessismo da tastiera*, in "Amnesty International Italia", 2020.

[23]Cfr. le statistiche pubblicate dalla End Revenge Porn della Cyber Civil Rights Iniziative.

[24]Cfr. Eurispes Osservatorio Cyber Security, *Revenge Porn: la vendetta può colpire chiunque*, 2019. Su questi temi, cfr. Commissione europea contro il razzismo e l'intolleranza (ECRI), *Raccomandazione di politica generale N° 15 dell'ECRI relativa alla lotta contro il discorso dell'odio. Adottata l'8 dicembre 2015*, 2016; Consiglio d'Europa, *Raccomandazione N. R (97) 20, su "Hate speech"*, 1997; Council of Europe Gender Equality Strategy, *Combating Sexist Hate Speech*, 2016.

[25]Si veda ancora A. Sorgato, *op. cit.*

[26]Per approfondire si vedano F. Poggi, *Violenza di genere e Convenzione di Istanbul: un'analisi concettuale*, in "Diritti umani e diritto internazionale", 2017, n. 1, pp. 51-76; P. Parolari, *La violenza contro le donne come questione (trans)culturale. Osservazioni sulla Convenzione di Istanbul*, in "Diritto e Questioni pubbliche", 2014, n. 14/3, pp. 859-890.

[27]Per ulteriori approfondimenti, sia consentito rimandare a S. Vantin, *Le violenze domestiche nelle riflessioni di Catharine MacKinnon. Un tentativo di applicazione entro il contesto legislativo e giurisprudenziale europeo*, in "Diritto & Questioni pubbliche", 2015, n. 15/1, pp. 236-241.

[28]Cfr. G. Alpa, *Autonomia privata, diritti fondamentali e "linguaggio dell'odio"*, in "Contratto e impresa", 2018, pp. 45-80.

[29]Cfr. G. Facci, *La responsabilità extracontrattuale dell'Internet Provider*, in "Responsabilità civile e Previdenza", 2002, n. 1, pp. 265-291; L. Bugiolacchi, *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'internet provider. Una sintesi di diritto comparato*, in "Diritto dell'informazione e dell'informatica", 2000, pp. 829-867.

[30]Cfr. L. Bugiolacchi, *(Dis)orientamenti giurisprudenziali in tema di responsabilità (ovvero del difficile rapporto tra assenza di obblighi di controllo e conoscenza dell'illecito)*, in "Responsabilità civile e previdenza", 2010, pp. 1568-1599; L. Bugiolacchi, *Ascesa e declino della figura del provider "attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilita dell'hosting provider*, in "Responsabilità civile e previdenza", 2015, n. 4, pp. 1261-1275; L. Bugiolacchi, *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'Hosting provider tra interpretazione giurisprudenziale e dettato normativo*, in "Responsabilità civile e Previdenza", 2017, n. 2, pp. 536-561. Sul tema della pedopornografia, si vedano, *inter alia*, D. Dell'Orto, *Pedopornografia on line e indagini informatiche. Complessita e peculiarita tecnico-giuridiche della materia*, in "Cassazione penale", 2007, n. 7-8, pp. 3042-3063; P. Perri, *Profili informatico-giuridici della diffusione, mediante strumenti telematici, di materiale pedopornografico*, in "Cassazione penale", 2008, n. 9, pp. 3466-3479; G. Amarelli, *Pornografia minorile. Le Sezioni Unite elidono retroattivamente il pericolo di diffusione*, in "Giurisprudenza italiana", 2019, pp. 1207-1215.

[31]Cfr. G. Belli, *La responsabilità civile dei service providers*, in "Informatica giuridica e diritto dell'informatica", 2011, pp. 693-697; F. Di Ciommo, *La responsabilità civile in internet: prove di governo dell'anarchia tecnocratica*, in "Informatica giuridica e diritto dell'informatica", 2006, n. 3, pp. 548-563; C. Novelli, *La Cassazione su responsabilità del provider e contenuto della notifica*, in "Diritto dell'informazione e dell'informatica", 2019, n. 2, pp. 500-513; R. Bocchini, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, in "Giurisprudenza italiana", 2019, n. 12, pp. 2606-2616; L. Tormen, *La linea dura della Cassazione in materia di responsabilità dell'hosting provider (attivo e passivo)*, in "La nuova giurisprudenza civile commentata", 2019, n. 2, pp. 1039-1054.

[32]Cfr. M.R. Allegri, *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Franco Angeli, 2018, in particolare pp. 131-158. Sopra queste questioni è stata chiamata in causa anche la Corte Europea di Giustizia, ad esempio nelle sentenze *Delfi v. Estonia* (2013 e 2015), *MTE e Index v. Ungheria* (2016) e *Pihl v. Svezia* (2017).

[33]Come sottolinea M. Montanari, *La responsabilità delle piattaforme on-line (il caso Rosanna Cantone)*, in "Diritto dell'informazione e dell'informatica", 2017, n. 2, pp. 254-283: «se la spinta alla revisione della regolamentazione della responsabilità degli ISP in principio appariva prevalentemente legata alla necessità di consentire regole di tutela del diritto d'autore – e cioè veniva per lo più alimentata da rivendicazioni patrimoniali a cui si contrapponeva spesso una certa retorica della libertà delle comunicazioni internet – sempre più spesso, più di recente, hanno acquistato maggiore rilevanza, tra i nuovi illeciti di internet, quelle condotte capaci di cagionare danni alla persona (privacy, onore, reputazione, vita di relazione etc.)».

[34]Cfr. la *Risoluzione del Parlamento europeo del 23 novembre 2016 sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi*.

[35]A questo riguardo, si veda anche V. De Rosa, *La formazione di regole giuridiche per il "Cyberspazio"*, in "Diritto dell'informazione e dell'informatica", 2003, n. 2, pp. 361-400; A. Mantelero, *Regole tecniche e regole giuridiche: interazioni e sinergie nella disciplina di internet*, in "Contratto e impresa", 2005, pp. 658-686.

[36]Si veda anche il *Code of Practice of Disinformation* (2018, rivisto nel 2019), dedicato agli effetti sui processi democratici della disinformazione sulla rete, nonché il Protocollo d'intesa stilato il 14 settembre 2017, a cura del Consiglio Nazionale

Forense, tra le Avvocature appartenenti ai Paesi del G7 (Italia, Francia, Germania, Regno Unito, Giappone e Stati Uniti d'America) al fine di promuovere comportamenti etici nell'uso di Internet, lo sradicamento di pregiudizi espressi con affermazioni che contengono espressioni lesive, per affermare il ruolo degli avvocati nella difesa dei diritti lesi, nell'eseguire un ruolo di intermediazione tra le autorità giudiziarie e i media. Su questi temi, si rimanda a G. Alpa, *op. cit.*

[37]Cfr. A. Colaruotolo, *Facebook e Hyperlinking illecito degli utenti. L'inerzia ingiustificata del prestatore dei servizi è fonte di responsabilità civile e risarcitoria*, in "Rivista di diritto industriale", 2019, n. 4-5, pp. 308-342.

[38]Cfr. la pagina sugli *Standard della community* di facebook.

[39]Con riferimento all'autoregolazione relativa ai contenuti politici, cfr. P. Bonini, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in "Federalismi.it", 11, 2020, pp. 265-281.

[40]*Ibidem.*

[41]G. Alpa, *op. cit.*

[42]A. Lorenzetti, B. Pezzini (a cura di), *La violenza di genere dal Codice Rocco al Codice Rosso. Un itinerario di riflessione plurale attraverso la complessità del fenomeno*, Giappichelli, 2020.

[43]Con riferimento agli aspetti processuali e penalistici, si vedano A. Massaro, G. Baffa, A. Laurito, *Violenza assistita e maltrattamenti in famiglia: le modifiche introdotte dal c.d. codice rosso*, in "Giurisprudenza penale", 2020, n. 3; P. Pittaro, *Il c.d. "Codice rosso" sulla tutela delle vittime di violenza domestica e di genere*, in "Famiglia e diritto", 2020, n. 7, pp. 735-741; A. Valsecchi, *"Codice rosso" e diritto penale sostanziale: le principali novità*, in "Diritto penale e processo", 2020, n. 2, pp. 165-173; C. Pecorella, *Violenza di genere e sistema penale*, in "Diritto penale e processo", 2019, n. 9, pp. 1181-1187.

[44]C. Pecorella, *Violenza di genere e sistema penale*, cit., p. 1183.

[45]Cfr. A. Valsecchi, *"Codice rosso" e diritto penale sostanziale: le principali novità*, cit., pp. 173-174; P. Pittaro, *op. cit.*, p. 741; ma anche M. Bouchard, *Sulla vulnerabilità nel processo penale*, in "Diritto penale e Uomo", 2019, n. 12; F. Filice, *Femminicidi di Bologna e Genova: perché quelle sentenze potrebbero sbagliare*, 2019; D. Russo, *Emergenza "codice rosso"*, in "Sistema penale", 2020, n. 1, pp. 5-20.

[46]C. Pecorella, *Violenza di genere e sistema penale*, cit., p. 1184. Si veda a questo proposito il caso *Talpis v. Italia* (Application no. 41237/14), in cui la Corte Europea dei Diritti dell'Uomo ha condannato l'Italia per non aver assicurato una tutela effettiva alla ricorrente, vittima di ripetute violenze da parte del marito, a causa dei ritardi nella procedura e della mancata adozione di misure idonee a prevenire il ripetersi delle aggressioni denunciate dalla donna.

[47]Sia consentito, a tal proposito, rinviare a S. Vantin, *La funzione simbolica del diritto nelle riflessioni di MacKinnon a partire da "Le donne sono umane?". Il caso della pornografia*, in "Jura gentium. Rivista di filosofia del diritto internazionale e della politica globale", 2014, n. 1, pp. 85-94. Più ampiamente, si rimanda agli scritti di Catharine MacKinnon, in particolare: *Sexual Harassment of Working Women: A Case of Sex Discrimination*, Yale University Press, 1979; *Feminism Unmodified. Discourses on life and law*, Harvard University Press, 1987; *Towards a Feminist Theory of the State*, Harvard University Press, 1989; *Only Words*, Harvard University Press, 1993; *Sex Equality*, Foundation Press, 2001; *Women's Lives, Men's Laws*, Harvard University Press, 2005; *Are Women Human? And Other International Dialogues*, Harvard University Press, 2006; *Sex Equality* (2nd edition), Foundation Press, 2007; *Traite, Prostitution, Inégalité*, Editions M., 2014; *Sex Equality Controversies. The Formosa Lectures*, National Taiwan University Press, 2015; *Sex Equality* (3rd edition), Foundation Press, 2016; *Butterfly Politics*, Harvard University Press, 2017; *Gender in Constitutional Law. Theoretical, Historical, and Empirical Analysis*, Edward Elgar Publishing, 2018.

[48]C. Pecorella, *Violenza di genere e sistema penale*, cit., p. 1186.

[49]Quali case rifugio, linee telefoniche di sostegno, la protezione e il supporto dei bambini testimoni di violenza, nonché il sistema di segnalazioni da parte di testimoni o di figure professionali che possano venire a conoscenza della violenza subìta.

[50]Cfr. EIGE, European Institute for Gender Equality, *op. cit.*

[51]A questo riguardo, a titolo esemplificativo, si vedano gli esiti del Progetto LOG-In: Centro documentazione donna e Assessorato alle pari opportunità del Comune di Modena (a cura di), *Violenza di genere e uso responsabile dei social network*.

[52]Si vedano il quadro informativo ISTAT in collaborazione con il Dipartimento delle Pari Opportunità della Presidenza del Consiglio (a cura di), *La violenza sulle donne*, ma anche le indagini condotte da Amnesty International sul monitoraggio della tossicità della rete *Twitter non rispetta i diritti delle donne: aumentano le molestie online*, in "Amnesty International Italia", 2018. Per un inquadramento teorico, J. Waldron, *The Harm in Hate Speech*, Harvard University Press, 2014; I. Gagliardone, D. Gal, T. Alves, G. Martinez, *Combattre les discours de haine sur internet*, 2015.

[53]L. Ferrajoli, *La differenza sessuale e le garanzie dell'eguaglianza*, in "Democrazia e diritto", 1993, n. 2, pp. 49-73, in part. p. 73.

* * *

Sharp blades. Forms of violence against women on the web

Abstract: In a scenario which is characterized by the increasingly impact of technologies on legal notions and processes, virtual spaces do not represent a guarantee for the promotion of gender equality. Along these lines, the paper focuses on the new forms and articulations that violence against women has taken on the web, in order to outline possible strategies to combat them in the wake of the current legislation.

Keywords: Gender Equality – Violence – On-line Violence – "Red Code"

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

ISSN 2704-7318
Fascicolo 2-2020
DOI: 10.32091/RIID0024

Application of information communication technology (ICT) to legislative drafting: case studies of legislative drafting assistant softwares in Nigeria and Canada

Tonye Clinton Jaja • Chantal Lamarre*

This paper examines the application of Information Communication Technology (ICT) tools by lawyers to simplify the task of legislative drafting of Bills and legislation. Using case studies in Nigeria and Canada some examples of the application of ICT to legislative drafting are examined. The idea of use and application of ICT tools for legislative drafting in Nigeria was first mooted in Nigeria in 1992 by the late Professor Keith Patchett during the Nigerian course in Legislative Drafting held in London. The lawyers that participated in the said course returned to Nigeria and trained other lawyers including Dr. Tonye Clinton Jaja, who led a team of computer experts to design a simple software for legislative drafting. Regarding Canada, Chantal Lamarre explains how the application of ICT for legislative drafting can improve the overall legislative process.

Information and Communication Technology (ICT) – Legislative Drafting

Summary: *1. Introduction – 2. Statement of the Problem and Background to the Research – 3. The Contents of the Legislative Drafting software – 4. How to use the Manual – 5. Checklist 1 - Definitions and Principles of a good Bill – 6. Checklist 2 - Principles of a good Bill – 7. Checklist 3 - Benchmarks for Structure of a Bill – 8. Using legislative information management software to facilitate the drafting, consolidating and publishing processes: the examples of Canada and other federal, provincial and municipal jurisdictions*

1. Introduction

"*Every [legislative] drafting office needs a practice or style manual* and a mechanism to keep it under review. This is worth the labour regardless of the size of the [drafting] office. Production of such a manual requires a careful and critical review of existing practices and this exercise is itself likely to result in improvements.... In addition to a style manual, every drafting office needs a system for noting useful precedents and other helpful materials. *An established procedure for sharing experience and knowledge can contribute hugely to the effectiveness* and to the contentedness of the office"[1]. The above statement underlines the importance of a Bill Drafting Manual. By implication, the above statement also provides justification for each drafting office to apply information communication technology (ICT) tools for performance of legislative drafting duties.

The history of emergence and development of legislative drafting as a sub-discipline of the legal profession would not be complete without a mention of the progressive application of ICT tools. Broadly speaking, the application of ICT to the legal profession is now well developed to a full-fledged discipline that is now referred to as "legal informatics" whereas the application of ICT to judicial is called "jurimetrics".

*Tonye Clinton Jaja is Senior Research Fellow, National Institute for Legislative and Democratic Studies (NILDS), Chantal Lamarre works at Irosoft Inc., Canada; T.C. Jaja is author of paragraphs 1-7, C. Lamarre is author of paragraph 8.

As far back as the year 1992, when the pioneer legislative drafters from Nigeria attended a Royal Institute of Public Administration (RIPA) course on legislative drafting, the course lecturer the late Professor Keith W. Patchett dedicated an entire chapter to "Computer-Based Drafting"[2]. However, ever since the year 1992 there has not been any published significant break-through in the application of ICT to legislative drafting in Nigeria until the year 2020 when Dr. Tonye Clinton Jaja led a team of indigenous Nigerian lawyers and computer experts to design and develop a computer-assisted legislative drafting programme. Dr. Tonye Clinton Jaja is a Nigerian citizen with a Master of Laws (LLM) and PhD in legislative drafting degrees respectively.

This legislative drafting assistant software was inspired by the search to provide solution to the problem of legislative drafting in Nigeria which is presented in the sub-heading below.

2. Statement of the Problem and Background to the Research

In the year 2014, Dr. Jaja undertook an empirical research to determine whether there is a problem with legislative drafting or not in Nigeria.

In a nutshell, that empirical study revealed and provided evidence that there is a dearth of personnel, knowledge and application of ICT tools for legislative drafting in Nigeria.

The empirical evidence was collated during a national workshop on legislative drafting held at the National Institute for Legislative Studies in Abuja. The conference was attended by the staff of the thirty-six (36) State Houses of Assembly.

3. The Contents of the Legislative Drafting software

As mentioned at the outset, there is a need for each Drafting Office to produce its own in-house legislative drafting manual and by implication the ICT tools that it will apply to perform its Legislative drafting style.

For example, the House of Representatives is vested with the power and authority by virtue of Section 60, Constitution of Federal Republic of Nigeria (CFRN), 1999 (as amended) which states that: "Subject to the provisions of this Constitution the Senate or the House of Representatives shall have power to regulate its own procedure. . . .". Drawing from this power, a legislative Bill drafting manual was produced for the House of Representatives in the year 2019. The said Manual is by implication a demonstration of the House of Representatives' application of its powers to regulate its procedure for drafting of Bills in exercise of the broad powers conferred upon it under section 60 of the CFRN, 1999.

As one of the legislative drafting consultants for the said Manual, Dr. Jaja conducted further research, modified and adapted some of the contents of the said Manual to produce this legislative drafting assistant software.

The design and development of the said legislative drafting manual was underpinned by the desire to simplify the art and science of legislative drafting to the extent that even a "layperson" without any knowledge of the law could draft a Bill using the said legislative drafting assistant software.

To achieve this cardinal objective, the legislative drafting assistant software provides samples and precedents, examples of the four principal parts of a Bill namely (1) Preliminary (2) Principal (3) Miscellaneous and (4) Final Provisions.

This makes it easier for the user to choose and adapt the text by copying and pasting to suit the current Bill that the user is drafting. At the beginning of the software the user is also prompted to choose whether it is a "Fresh" Bill or "Amendment" Bill. Depending on the choice, the software provides the user with a structure for each different kind of Bill.

The preparation and consideration of a Bill is a multi-stage process, which begins with preliminary preparation and ends with the entry into force of the Act, its implementation and follow-up[3]. This Manual therefore provides general guidance for drafting and analysis of Bills in order to ensure consistency and standardization in the language, structure and style of Bills. The imperative for consistency and standardization in the language and structure of Bills is based on the fact that section 58 (1) of the Constitution of the Federal Republic of Nigeria states that the power of the National Assembly to make laws shall be exercised by Bills passed by both the Senate and House of Representatives.

Hence, the objectives of the Manual are to:

1. eliminate as much as possible, inconsistency and deficiency in the form, language and structure of Bills,
2. ensure standardization in drafting and structuring of Bills,
3. facilitate the work of drafting Bills by serving as toolkit, and
4. ensure that Bills are drafted in the language and structure that make them clear, certain, concise, consistent, correlated, complete and comprehensible to the public.

4. How to use the Manual

The Manual is designed for use by legislators, legislative support staff and consultants, etc. It is to be used as a standard measure of checking whether any proposed Bill complies with the basic requirements of a Bill.

The Manual contains series of "checklists"[4] and "templates" on drafting of Bills which should be complied with. Each checklist contains a list of "benchmark of minimum standards".

The checklists in the Manual are numbered from 1 to 10 in 4 chapters. It is recommended that the user begins by reviewing the Bill clause-by-clause using Checklist 1 before proceeding to use Checklist 2 and so on. While undertaking the clause-by-clause review of the Bill using the Checklist as a parameter, the users can make marginal notes or comments to confirm whether or not the clause complies with each of the items in the basic benchmarks. At the end of this Manual there is an Appendix containing some samples and Templates of Bills and other items.

5. Checklist 1 - Definitions and Principles of a good Bill

A Bill is a legislative proposal. Bills must be drafted in such a way that when passed into law, can be «effective, clear, precise, intelligible and capable of only one interpretation, which is the true purpose and intent of the policy as envisaged by the policy initiators»[5]. It should also be noted that Bill drafting is an area of specialist legal practice[6].

In order to undertake an overall view of the Bill, the drafter should be guided by the need for effectiveness. «Effectiveness means that the legislation manages to introduce mechanisms capable of producing the desired... results.»[7] Elements of "effectiveness" are as follows:

- Clarity (easily perceived or understood)
- Precision (exactness of expression and detail)
- Unambiguity (certain or exact meaning)
- Plain language (non-legalese)
- Gender-Neutral language.

These elements of effectiveness in Bill drafting are in line with the seven C's of a good Bill, which are (i) Clarity; (ii) Certainty; (iii) Conciseness; (iv) Consistency; (v) Correlation; (vi) Completeness; (vii) Comprehensibility.

In terms of conciseness the drafter should not use unnecessary or repetitious words or phrases. The Bill should cover all reasonably foreseeable circumstances likely to arise. The drafter should use the same style throughout to achieve consistency while the legislative intention being communicated should be certain so that those to be affected are not left in doubt as to the extent of their duties, obligations, powers, discretions or rights. The drafter should ensure that the legislation is drafted in the language and structure that the reader does not only understand, but must be seen to understand.

6. Checklist 2 - Principles of a good Bill

- Use short sentences
- Every paragraph should start with the topic sentence
- Use the active voices
- Avoid legal jargons (hereof, thereof, hereunder, null and void)
- Refer to all people and companies by name
- Avoid abbreviations
- Use punctuation marks properly
- Avoid the use of archaic words
- Avoid the use of passive language
- Avoid verboseness.

7. Checklist 3 - Benchmarks for Structure of a Bill

Legislative drafting requires a systematic application of a range of analytical and writing skills[8]. Broadly, a Bill is composed of four major parts namely: Preliminary provisions; Principal provisions; Miscellaneous provisions and Final provisions.

- Preliminary provisions
  - Long title
  - Preamble (in Nigeria, preambles are only used in Bills that are domestication of Treaties)
  - Enacting clause
  - Purpose Clause (for civil law jurisdictions)
  - Commencement
  - Duration/Expiry
  - Application
- Principal provisions
  - Substantive provisions
  - Administrative provisions
- Miscellaneous
  - Offences and provisions ancillary to offences such as time limit for prosecution, continuing offences, offences by corporations, and vicarious responsibility Miscellaneous and supplementary provisions such as evidentiary provisions, a power to make subordinate legislation, service of notices, powers of entry and search, seizure and arrest.
- Final Provisions

- Savings and transitional (these may also be placed in a schedule if they are long)
  - Repeals
  - Consequential amendments (these may be placed in an annex especially if the repeals and consequential amendments are numerous and can conveniently be presented in a tabular form)
  - Definitions
  - Interpretation
  - Short title
  - Explanatory Memorandum
  - Schedules

Long Title. Every Bill has a long title. The purpose of the long title is to provide a concise but comprehensive statement of the subject matter of the Bill, by describing the nature of the proposed Bill or legislation. As a general Rule of interpretation of Statutes, the long title does not form part of the Bill or legislation but it is useful for discerning the intention of the legislature. The title, generally referred to as the long title, is prefixed to the Bill and retained in the Act, and is different from the short title. Care must be taken to ensure that the title is sufficiently wide to cover all the provisions of the Bill, and that it is not vague, otherwise it may invite amendments. For instance, the long title is usually expressed as follows: "A Bill for an Act to Provide for the establishment of the National Transport Commission as an independent Multi-Model Economic Regulator for the Transport Industry and for Other Related Matters".

Enacting Formula. The enacting formula states the authority by which legislation is made. For instance, an enacting formula for a federal legislation is usually stated as follows: "The National Assembly of the Federal Republic of Nigeria enacts:". The enacting formula for a legislation by a State House of Assembly would be: "The Kaduna State House of Assembly enacts:". The enacting formula for a Local Government would be as follows: "I, Dr. Nasiru Tijani, Chairman of Bwari Local Government Area of Niger State, by virtue of the powers conferred upon me by the Local Government Law of Nigeria State, 2009, do make the following:".

Purpose Clause. In civil law jurisdictions and in some common law jurisdictions such as New Zealand, there is usually a "Purpose Clause" that provides a statement of the object, goal and purpose of the Bill or legislation. In Nigeria, in recent times, certain legislation are copying this trend by commencing with a statement of the goals and objectives of the Bill or legislation. For example, section 1 of the Environmental Impact Assessment Act, Chapter E12, Laws of the Federation of Nigeria, 2004 reads: "Goals and objectives of Environmental Impact Assessment". In Nigeria, the Explanatory Memorandum serves as the equivalent of the Purpose Clause.

Application Clause. A law passed by Parliament is applicable throughout the country except where it is otherwise expressly provided for in the Statute itself. It is, however, usual and convenient and at times necessary to specify the extent explicitly. It gives an indication of an area of application of an Act. For instance the application clause is usually expressed thus: "This Act shall apply to the provision or use of transport and related services in marine, rail and road transport in Nigeria". An extent or application clause may, however, be rendered unnecessary by the nature of the Act when it indicates the areas to which it will apply, or denotes the persons who will be subject to it, or signifies things which will come under its purview. In Nigeria, all laws made by the National Assembly in respect of matters contained in the Exclusive Legislative List apply throughout the federation. However, some laws made by the National Assembly, have limited application to the Federal Capital Territory (FCT) alone because the National Assembly is the legislature of the FCT.

Commencement Clause. The commencement clause forms an important provision of a Bill. The general rule regarding the coming into operation of enactments is that in the absence of any express provision to the contrary an Act comes into operation on the day on which it receives the assent of the President. In view of the above general provision, Acts which are intended to take effect at once need not, and do not usually, have a commencement clause. In some cases, it is necessary to give retrospective effect to an enactment but note that there is a constitutional prohibition on giving retrospective effect to criminal legislation in Nigeria[9].

Interpretation or Definition Clause. Where the expressions defined occur only in a single section, the definitions are given in that section and where the definitions are necessary only for a particular part or chapter, they are given in that part of chapter. Definitions are required to avoid tedious paraphrases, explain terms which are of ambiguous or uncertain meaning, give to a term which has been judicially interpreted or a sense other than that given by such interpretation or include or exclude, for the purposes of the Act, something in regard to the inclusion or exclusion of which there might otherwise be doubt. The definitions are arranged in alphabetical order. In Nigeria, as a general rule, the Interpretation Clause or section is usually placed towards the end of the Bill or legislation. However, whenever a legislation deals with a technical subject-matter, the

Interpretation section usually occurs at the beginning of the Bill[10].

Duration Clause. Certain laws are of limited duration and are enacted for a short stipulated period. Such enactments cease to be effective after the expiry of the period stipulated. The duration clause is embodied as one of the sub-clauses in the clause of a Bill. The form used may be different in different Bills, as the situation demands[11].

Marginal notes. A marginal note, also called "statutory footnote", is a brief summation of a provision of a statute. They are useful as editorial flags and for ease of the readers of the Bill or legislation. Marginal notes are important in statutory construction as they provide insights into the nitty-gritty of the provision.

Rule-making Clause. Some legislation includes provisions delegating the power to the officials of the Executive to make subsidiary legislation such as rules, and regulations for administering the principal Act (legislation). This provision is contained in the rule-making clause of a Bill.

Repeals, Consequential Amendments and Savings Clause. The provisions regarding both repeal and savings are embodied in the same clause. The clause is placed at the end of a Bill. When an enactment is repealed, the repeal, unless a different intention appears from the context, does not (i) revive anything not in force or existing at the time at which the repeal takes effect; (ii) affect the previous operation of any enactment so repealed or anything duly done or suffered; (iii) affect any right, privilege, obligation or liability acquired, accrued or incurred under any enactment so repealed; (iv) affect any investigation, legal proceeding or remedy in respect of any such right, privilege, obligation, liability, penalty, forfeiture or punishment; and any such investigation, legal proceeding or remedy may be instituted, continued or enforced, and any such penalty, forfeiture or punishment may be imposed as if the repealing Act had not been passed.

With the repeal of an enactment, all rules made under it are repealed, unless provision is made to the contrary in the repealing Act. The savings clause reserves something which would be otherwise included in the words of the enacting part. The clause only preserves things which were in force at the time of its enactment and therefore cannot affect transactions which were complete on the date of the repealing Statute. It is inserted in the Statute in order to protect or save a person as regards rights which he or she might have acquired under the repealed law.

Explanatory Memorandum. The function of the explanatory memorandum is to explain certain facts in the Bill. It is normally expressed thus: "This Act seeks to establish the National Transport Commission as an effective, impartial, independent regulatory authority in the Transport sector, promote the implementation of the national transport policy and provide for an efficient economic regulation of the transport sector and for matters".

Short Title. It identifies, describes and gives a name to the Bill. It is often called the statutory nickname of the Bill. For example, "National Transport Commission Bill 2015". Every Bill has a short title. It has to be short for it is merely a label or index-heading to the enactment in question and has also to be apposite. It is cited in the first clause of the Bill. An enactment is cited by reference to the short title or by reference to the number and year. Where in any enactment it is necessary to cite or refer to another Act, its short title is cited in the body and reference to the number and year made in the margin.

Citation. It states how the Act should be cited. For example: "The Act may be cited as the Forest Act 1995".

Schedules. Schedules are used in drafting of Bills to supply supplementary details. Therefore, details of information, statistics, figures, tables, codes, maps and other technical matters highlighted or referred to in the body of the Bill or legislation are contained in the Schedule. Some Bills have Schedules appended to them. As a rule, matters of detail are relegated to Schedules, e.g., illustrations of forms, agreements and plans. When the constitution of an organization is declared in the Bill itself, the mode of appointment and rules governing meetings of that organization are placed in a Schedule. It is sometimes convenient to indicate in a Schedule where several Acts or parts of several Acts are being repealed or where a considerable number of minor amendments are made.

Table of contents. A table of contents is required for longer Bills. The table of contents is based on the headings used in the Bill. The detailed reasons are included in the table of contents at the level of chapters. The table of contents are required in long Bills and may be presented at the level of individual sections. Table of contents follows the executive summary.

Test of Practicability of Legislation. The true test of the practicability of legislation is when the legislation is implemented. How, for example the public responds to it, and whether it will secure a satisfactory level of compliance can only be assessed when the law is in operation. Being a medium of communication, the language of a legislative instrument must be simple, concise and comprehensible. Legislative drafters must at all times follow the sequence

of presentation of legislative instruments in term of structure and organization.

8. Using legislative information management software to facilitate the drafting, consolidating and publishing processes: the examples of Canada and other federal, provincial and municipal jurisdictions

The application of Information Communication Technology (ICT) for Legislative Drafting can improve the overall legislative process by introducing tasks automation, by relying on conventions and standards, by eliminating multiple streaming, by saving time and by making content available to all.

Facilitating Drafting

Drafting can be facilitated by implementing conventions and standards. Conventions pertain to style, template layout and structure. To facilitate drafting, it is essential to introduce standardized applications, expressions and terminology as well as ensure the standardization of methods used to effect amendments or draft new legislation. Part of the conventions includes the integration of any particular classification embedded at the document level or the "fragment"[12] level.

Once the office has implemented conventions and standards, it is very important to review the type of tasks a drafter performs on a daily basis. It soon becomes apparent that drafters using a word processor to write legislation will spend a lot of time manually formatting documents and managing document versions. Modern software technology can help by removing non-drafting tasks and by structuring as well as standardising content. The drafter will thus concentrate on analysing the requirements pertaining to the writing of a particular legislation instead of trying to make sections look good!

By accessing a unique content source repository coupled with automated versions management, the drafter will also save time and worry less about making errors, duplications or inconsistencies.

Technology will help by introducing international norms to help structure the content (e.g., XML). Then, with appropriate software tools, this structured content can be applied thereby properly formatting to the content (e.g., XSLT, XSL-FO etc.). The rendering of the content is thus removed from the drafter's main activities.

Furthermore, when the content's single source is well defined, it can automatically be published online to provide legislative content research capabilities. Legislative content will thus be at the drafters' fingertips.

Finally, implementing a unique, structured content source will also provide advantages for the consolidating and publishing processes.

Facilitating Consolidating

Once a bill is passed, the new Act is available for consolidation[13]. When it comes to updating legislation with a new Act that modifies an existing Act, often, another department independent from the drafting office — oftentimes called the Law Revision Office — will perform the tasks related to the consolidating process.

Generally, without a modern ICT solution, the Law Revision Office will take the new Act and manually update the legislation with legislative commands found in the new Act. This office will either copy/paste these, using word processor or a specialised publishing tool, or the process will be entirely manual. This means photocopying the pages of the Act (copy), cutting the appropriate words included in the legislative command (cut), and then literally gluing the paper (paste) in order to create a paper blue print.

If the Drafting Office uses structured content and applies all the appropriate conventions, including the standardisation of methods used to effect amendments to legislation, then modern ICT technology can help by introducing a tool that will recognise which part of the legislative commands need to be applied, thus saving hours of copying and pasting.

A modern ICT solution will also recognise the origin of the modification and automatically create a historical repository of legislation.

Furthermore, quality assurance becomes a much faster process since computerised tools can provide a before-and-after comparison following the application of any legislative command.

Facilitating Publishing of legislation

Once the content is structured and centralised in a unique content source (repository), then the publishing process enables the legislation to be generated in a large selection of formats, depending on the purpose of the copy.

In order to make this large selection available, the prior legislative processes — drafting and consolidating — will include metadata related to the content. During the publishing process, the metadata can then provide links between documents (e.g., Act and its related statutory instruments), between a section and all its historical versions as well as between statutory books.

From the same content source, legislation can almost instantly be made available on paper, on the Internet or on mobile devices.

Notes

[1]G. Thornton, *Legislative Drafting*, 4th Ed., Butterworths, 1996, p. 128.

[2]See K.W. Patchett, *Nigerian Legislative Drafting Course*, Course Notes, RIPA, Regent's College, 1992, p. 337.

[3]Finland Ministry of Justice, *Bill Drafting Instructions*, 2006, p. 8.

[4]«A checklist is a list of items you need to verify, check or inspect... Using a checklist allows you to ensure you don't forget any important steps»; see J. Brun, *What is a Check List?*, in "Nimonik - Articles about quality, environmental and safety compliance issues", October 2011.

[5]Clerk, National Assembly of Nigeria, *The Nation newspaper*, September 2, 2014.

[6]It now recognised that legislative drafting is a "new sub-discipline of law" or the legal profession, see generally H. Xanthaki, *Legislative Drafting: A New Sub-Discipline of the Law is Born*, in "IALS Student Law Review", Vol. 1, 2013, n. 1, pp. 57-70.

[7]H. Xanthaki, *Drafting Legislation. A Modern Approach*, Ashgate Publishing, 2008, pp. 1-18 at p. 6.

[8]S.S. Shikyil, *Practical Guide on Legislative Drafting*, 2006, p. 23.

[9]See section 36 of the 1999 *Constitution of the Federal Republic of Nigeria* (as amended).

[10]For example, see the *Petroleum Industry Bill*, 2009 version.

[11]For example the *Offshore Production Sharing Contracts Act*, 2000 had a lifespan of fifteen (15) years which expired in the year 2015. The purpose of this legislation was to grant tax holiday or exemption to oil companies that were involved in exploitation of oil and gas resources in offshore oil fields; considering the huge financial expenses involved in undertaking such offshore oil exploitation activities, the Federal Government of Nigeria granted them an exemption from payment of taxes for the first fifteen years of production.

[12]The term fragment refers to any part of a bill, an Act or a statutory instrument.

[13]Consolidation is a term that can represent at least two concepts in Commonwealth Legislative Processes: the first concept refers to updating legislation with the content of a modifying Act; the second concept refers to classifying the new Act under a certain subject of law in order to create compendium of Acts related to the same subject.

* * *

L'applicazione delle ICT al drafting legislativo: note dall'esperienza nigeriana e canadese

Riassunto: Questo contributo riguarda l'applicazione delle tecnologie dell'informazione e della comunicazione (ICT) all'attività di drafting degli atti normativi, facendo riferimento alle esperienze della Nigeria e del Canada. L'esperienza nigeriana ha inizio nel 1992, quando un gruppo di giuristi provenienti da quel paese prese parte al corso in materia di tecniche di redazione degli atti normativi tenuto a Londra da K. Patchett, riportando poi in patria le competenze acquisite e formando altri giuristi sugli stessi temi; T.C. Jaja presenta qui le idee che hanno guidato la progettazione di un software di aiuto alla redazione degli atti normativi nigeriani. Considerando l'esperienza canadese, C. Lamarre spiega come l'applicazione delle ICT al drafting possa migliorare l'intero processo legislativo.

Parole chiave: Tecnologie dell'informazione e della comunicazione – Drafting legislativo

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

ISSN 2704-7318
Fascicolo 2-2020
DOI: 10.32091/RIID0019

Maria Romana Allegri, *Oltre la par condicio. Comunicazione politico-elettorale nei social media, fra diritto e autodisciplina*, Milano, Franco Angeli, 2020

Autorecensione

Questo libro nasce dalla constatazione che, a fronte del massiccio utilizzo dei social media nelle campagne elettorali degli ultimi anni e, più in generale, nella comunicazione politica, si assiste a una certa ritrosia – a livello sia nazionale che europeo – a regolare questo fenomeno con gli strumenti propri del diritto. Ciò è tanto più singolare quanto più si riflette sul fatto che il legislatore del passato si è affannato, nel corso del tempo, a produrre norme idonee a regolare la diffusione di contenuti di tipo politico-elettorale attraverso i mezzi di comunicazione tradizionali (stampa e radiotelevisione), nel tentativo – forse non ben riuscito – di garantire a tutti i soggetti politici pari opportunità di accesso ai media e, quindi, pari opportunità di contribuire alla formazione dell'opinione pubblica e della volontà politica degli elettori. Lo sforzo normativo compiuto negli scorsi decenni è stato volto a dare concreta attuazione ai principi che la Corte costituzionale ha affermato e ribadito in numerose sentenze, cioè che il diritto dei cittadini a ricevere informazioni il più possibile complete e attendibili, provenienti da una molteplicità di fonti, è un elemento essenziale e indefettibile della democrazia, che in un contesto politico-elettorale i cittadini devono essere messi nella condizione di potersi formare la propria opinione liberamente, senza essere sottoposti a pressioni e condizionamenti occulti, infine che a tutti i soggetti politici deve essere garantita pari possibilità di diffondere le proprie idee e istanze e che questo, in un sistema mediatico dominato dalle esigenze di mercato, non è possibile se non attraverso la previsione di regole idonee.

Tutte le esigenze che la Corte costituzionale ha espresso e che il legislatore ha cercato di cogliere nel passato rimangono immutate anche oggi. Dunque, quali sono le ragioni per cui la comunicazione politico-elettorale attraverso i social media continua ad essere caratterizzata da una sostanziale anomia?

A questo interrogativo si tenta di rispondere nel libro attraverso un ragionamento che muove inevitabilmente da una descrizione del fenomeno oggetto di studio, delineata nel primo capitolo attingendo alla cospicua letteratura sociologia e politologica su questo argomento. In particolare, vengono evidenziate le analogie fra le strategie di marketing commerciale e quelle usate in politica (in particolare, le tecniche di profilazione dei cittadini-elettori, di segmentazione dei pubblici e di microtargeting) e ne vengono delineate le conseguenze in termini di formazione dell'opinione pubblica: polarizzazione ideologica, costruzione di "bolle" informative, mancanza di trasparenza e frammentazione dei messaggi politici (dark ads). Vengono poi esaminate le modalità di manipolazione del consenso politico attraverso il subdolo utilizzo dei social bots e l'analisi dei big data con finalità non solo predittive, ma anche orientative e

M.R. Allegri, ricercatrice di Istituzioni di diritto pubblico, è Professoressa aggregata di Diritto pubblico, dell'informazione e della comunicazione presso Sapienza Università di Roma, Dipartimento di Comunicazione e Ricerca Sociale.

persuasorie (nudging). Emerge da questo quadro che la capacità che i social media possiedono di orientare l'opinione pubblica è enormemente superiore a quella propria dei mezzi di comunicazione tradizionali e si presta in modo assai maggiore a sviluppare meccanismi di pressione non trasparenti. Da ciò dovrebbe derivare l'esigenza di una più accorta e accurata regolamentazione di questo fenomeno, non certo quella della sua de-regulation.

E allora perché il diritto stenta ad affermarsi in questo campo? Una prima difficoltà può essere rappresentata – come indicato nel secondo capitolo del libro – dal fatto che le piattaforme digitali attraverso cui i contenuti politico-elettorali vengono diffusi sono un'infrastruttura tecnologica, che si avvale degli strumenti offerti dallo sviluppo delle tecnologie digitali (i software algoritmici). La "decifrabilità" del messaggio politico – in altre parole, la trasparenza riguardo ai committenti, ai finanziatori, alla selezione dei destinatari, alle finalità del messaggio, alle strategie utilizzate per la sua più efficace diffusione – che sarebbe necessaria affinché i cittadini acquisiscano consapevolezza di "ciò che sta dietro" ai contenuti cui vengono esposti, non può essere ottenuta solo attraverso regole giuridiche, ma impone che in certa misura tali regole vengano tradotte in norme tecniche immanenti al mezzo prescelto. Il giurista, però, agisce su un piano diverso – e in un momento diverso – rispetto al progettista software e quindi, laddove la norma giuridica riesce ad intervenire all'origine dei processi di creazione algoritmica, che rimangono di esclusivo appannaggio dei tecnici, il diritto si condanna al ruolo di "inseguitore permanente" degli strumenti tecnologici che si evolvono in continuazione. Poiché non è affatto scontato che chi produce norme giuridiche sia in grado di comprendere pienamente i meccanismi di funzionamento degli algoritmi, onde poterne predisporre una regolamentazione efficace, la produzione normativa sconta l'oggettiva difficoltà di tradurre il linguaggio tecnico in linguaggio giuridico: per questo, concetti quali la trasparenza algoritmica o la spiegabilità degli algoritmi, che si tenta talvolta di introdurre per via legislativa o regolamentare o giurisprudenziale, sono caratterizzati da una inevitabile e ineliminabile approssimazione. Non va dimenticato, infine, che gli algoritmi sono "beni" protetti dai diritti di proprietà intellettuale e dal segreto industriale, per cui la loro integrale rivelazione, comprensiva del codice-sorgente, sarebbe comunque irrealizzabile.

Una seconda difficoltà deriva dalla natura dei social media, che sono gestiti da società private, operanti sul mercato con finalità di lucro, che svolgono oggi una funzione essenziale per la diffusione di idee e opinioni e che però, a differenza delle testate giornalistiche e delle emittenti radiotelevisive, non hanno una responsabilità editoriale per i contenuti che veicolano. Anche per questo non è affatto agevole estendere ad essi la disciplina sulla comunicazione politico-elettorale costruita negli anni per i mezzi di comunicazione tradizionali. In ogni caso, il terzo e il quarto capitolo del libro sono dedicati all'analisi della disciplina vigente, per verificarne l'applicabilità ai social media ed evidenziare eventuali lacune normative che sarebbe necessario colmare. L'analisi si concentra inizialmente (terzo capitolo) sul fondamento costituzionale della comunicazione politico-elettorale, esaminando la differenza fra l'approccio statunitense, basato sulla libera competizione nel free marketplace of ideas, e quello europeo, fondato sul concetto di limitazione ex lege dei diritti individuali, purché proporzionata e necessaria nel contesto di una società democratica, come sancito dall'art. 10 della Cedu. Si confrontano inoltre i due diversi orientamenti espressi dalla dottrina costituzionalistica italiana, secondo i quali la propaganda politica è da considerarsi, per l'uno, un diritto individuale compreso nell'ambito della libera manifestazione del pensiero e, per l'altro, una funzione strumentale alla realizzazione del diritto collettivo ad essere informati, a sua volta principio cardine della democrazia. La consistente giurisprudenza della Corte costituzionale sembra condividere questo secondo orientamento. Quindi, se si aderisce all'idea per cui la libera manifestazione del pensiero non vada intesa solo in termini di diritto individuale, ma anche di funzione essenziale allo svolgimento della vita democratica, si evidenzia l'opportunità di regolare per legge l'esercizio di tale libertà mediante i mezzi di comunicazione e di estendere tale regolamentazione anche ai social media, essendo questi ultimi i mezzi che oggi, nei contesti politico-elettorali, appaiono dotati di maggiori possibilità di influenzare l'opinione pubblica.

Il quarto capitolo, che analizza l'evoluzione della disciplina della comunicazione politica nel corso degli anni (in particolare le leggi n. 212/1956, n. 515/1993 e n. 28/2000, nonché la rilevante giurisprudenza costituzionale), giunge alla conclusione che in tema di propaganda politica via Internet l'attenzione – anche del legislatore – non deve diminuire, ma spostarsi dal problema della par condicio radiotelevisiva a quello del bilanciamento fra la preservazione della libertà di espressione e la tutela dei diritti individuali, nonostante i condizionamenti derivanti dagli interessi economici dei grandi operatori del web. Le piattaforme digitali, infatti, hanno acquisito di fatto una notevole forza politica, poiché sono in grado di influenzare ciò che la gente vede o sente, tanto da poter

essere considerate alla stregua di attori primari della competizione politica. Sebbene l'Agcom, nelle linee-guida pubblicate a febbraio 2018, abbia suggerito di applicare anche ai social media alcuni aspetti della normativa vigente per le campagne elettorali attraverso i mezzi tradizionali, questa estensione analogica – peraltro semplicemente suggerita e non imposta con atti normativi vincolanti – non è così semplice. Infatti, la disciplina del "silenzio elettorale" nel giorno destinato alle votazioni e in quello precedente, così come il divieto di propaganda elettorale nei pressi delle sezioni elettorali, mal si adattano alla natura e alle modalità di diffusione dei messaggi mediante i social media, cui non è possibile imporre limiti di tempo e di luogo. Lo stesso può dirsi del divieto di diffusione dei sondaggi demoscopici nei quindici giorni antecedenti alla data delle votazioni, nonché del divieto di comunicazione istituzionale delle pubbliche amministrazioni nel periodo della campagna elettorale: tali divieti potrebbero riferirsi al limite solo alla produzione di nuova pubblicità istituzionale e alla diffusione di nuovi risultati di sondaggi nei giorni precedenti il voto, ma non potrebbero riguardare la riproposizione e la continua circolazione in Internet di contenuti già prodotti in precedenza. Invece, senza difficoltà potrebbero – e dovrebbero – essere estesi alla propaganda politica online gli obblighi di indicare il committente responsabile della pubblicità politica (anche per impedire la diffusione di messaggi provenienti da profili fake) e l'ammontare delle somme spese. Proprio per eliminare le incongruenze, quindi, sarebbe necessario dettare per i social media una disciplina specifica.

Come termine di confronto, nel quinto capitolo è stata analizzata la normativa recentemente introdotta in Germania e in Francia – unici Paesi europei ad aver disciplinato in qualche modo l'informazione attraverso i social network – nonché le proposte legislative avanzate nel Regno Unito: si tratta di soluzioni non sempre condivisibili e certamente non esaustive, ma che almeno denotano la volontà politica di fronteggiare le sfide poste dalla modernità attraverso il diritto. Mentre la normativa francese si pone come lex specialis applicabile proprio ai periodi di campagne elettorali, quella tedesca si riferisce a molteplici categorie di contenuti illeciti veicolati attraverso i social network, senza specifico riferimento ai contesti politico-elettorali, anche se alcuni di questi contenuti (ad esempio odio o disinformazione) si prestano a circolare più massicciamente in tali occasioni. La legge tedesca sembra contare troppo sull'effettiva idoneità degli intermediari digitali a vagliare le segnalazioni e ad assumere conseguenti decisioni equilibrate e non lesive dei diritti individuali; inoltre, essa non prevede l'intervento di una autorità giurisdizionale nella gestione del contraddittorio fra gestori della piattaforma e utenti. La legge francese, invece, sottopone le piattaforme digitali al controllo di un'autorità amministrativa indipendente e dispone significative sanzioni amministrative e pecuniarie per i casi di violazione degli obblighi di trasparenza della pubblicità politica a pagamento e delle modalità di utilizzo dei dati personali degli utenti; tuttavia, per alcuni social media adeguarsi a tali prescrizioni può risultare oneroso, senza contare che il sistema sanzionatorio può incoraggiare la tendenza alla rimozione indiscriminata di contenuti che possono apparire "rischiosi". Le esperienze straniere evidenziano, dunque, un'ulteriore (terza) difficoltà con cui deve confrontarsi il legislatore: quella cioè di individuare il punto di equilibrio fra la preservazione della libertà di espressione attraverso i social media, la libertà di iniziativa economica delle piattaforme digitali e le esigenze di controllo e correzione di talune distorsioni che possono verificarsi nella comunicazione politico-elettorale, a beneficio della garanzia della libertà dell'elettore e della preservazione dei processi democratici.

Nel sesto capitolo, dopo aver esaminato il fondamento giuridico del "dogma" dell'irresponsabilità degli intermediari digitali per i contenuti user-generated derivante dalla direttiva europea 2000/31/Ce, viene delineato l'approccio adottato dall'Unione europea, che – rinunciando del tutto al ricorso allo hard law – è piuttosto basato sulla promozione della volontaria adesione, da parte dei gestori delle piattaforme digitali, a codici di condotta e buone pratiche, al fine di contrastare il proliferare dello hate speech e della disinformazione via Internet, soprattutto nei contesti elettorali. In questa scelta si annida la quarta difficoltà che incontra il diritto nell'intervenire nel campo della comunicazione politico-elettorale. Infatti, il principio di irresponsabilità degli intermediari digitali si giustifica oggi solo in base a una finzione giuridica assolutamente anacronistica: quella, cioè, che i gestori delle piattaforme mantengano una posizione di neutralità rispetto alle condotte dei loro utenti. Se ciò poteva essere vero in passato, non lo è più certamente oggi, visto che tutte le grandi piattaforme digitali esercitano un controllo capillare sui comportamenti dei loro utenti a fini di profilazione e contribuiscono attivamente all'organizzazione, presentazione, diffusione e valorizzazione dei contenuti. Sta di fatto che la normativa vigente rende impossibile imporre ai provider obblighi cogenti di monitoraggio e controllo, come sempre ribadito dalla giurisprudenza della Corte di Giustizia dell'Unione europea. Del resto, se gli intermediari digitali fossero considerati per legge responsabili per le conseguenze

derivanti, sul piano civile e penale, dalla circolazione dei contenuti user-generated, bisognerebbe anche accettare che essi procedano sistematicamente a filtraggio preventivo e rimozione selettiva dei contenuti: in altre parole, bisognerebbe rassegnarsi ad accettare l'instaurazione di un sistema di "censura privata" affidato alle piattaforme digitali, del tutto incompatibile con il principio della libera manifestazione del pensiero, tanto più che le piattaforme potrebbero agire non solo in base ad interessi economico-imprenditoriali, ma anche direttamente politici.

E proprio in questo risiede l'ambiguità della situazione attuale, che occorrerebbe in qualche modo sanare: le piattaforme digitali non sono gravate di alcun obbligo "censorio" né sono ufficialmente legittimate a procedere in tal senso, ma di fatto – ciascuna a modo suo, con criteri e intensità variabili e soprattutto senza che gli utenti ne siano adeguatamente informati – tutte quante svolgono spontaneamente un'intensa attività di content moderation. Il problema è che le azioni concretamente intraprese dai principali social media per ottemperare ai codici di autodisciplina promossi dall'Unione europea appaiono caratterizzate da notevole discrezionalità e disomogeneità, che confonde gli utilizzatori delle piattaforme. Inoltre, non sono previste efficaci forme di contraddittorio a tutela dell'utente che voglia reagire alla decisione del gestore della piattaforma in ordine alla cancellazione di taluni contenuti o account. Infine, non tutte le piattaforme hanno sottoscritto i codici di autodisciplina e, anche fra quelle che li hanno sottoscritti, si registra una ampia varietà di forme e di intensità con cui i diversi impegni vengono adempiuti. Non vi è quindi alcuna garanzia che la trasparenza e il controllo pubblico sulla propaganda politico-elettorale online possano essere assicurati allo stesso livello da tutte le piattaforme.

L'ultimo capitolo del libro tratta la questione della particolare protezione di cui devono godere i dati relativi alle opinioni politiche dei cittadini ai sensi dell'art. 9 del regolamento Ue n. 2016/679. La conoscenza di questo tipo di informazioni può essere estremamente rilevante per soggetti pubblici e privati che, per le più varie finalità, hanno interesse a profilare tanto singole persone quanto i diversi segmenti di elettorato, a condizionare le scelte tanto individuali quanto collettive e a predire le tendenze dell'opinione pubblica. Proprio per questo, se davvero si vuole far sì che i cittadini possano concorrere democraticamente (e quindi liberamente) a determinare la politica nazionale, è necessario che il processo generativo di idee e opinioni – in altre parole, la nostra intellectual privacy – venga protetto da indebite interferenze o sorveglianza intrusiva. Grazie all'analisi dei big data, i soggetti che hanno interesse ad influenzare il dibattito politico, servendosi di sofisticati algoritmi dal funzionamento poco trasparente, possono mettere in relazione fra loro le informazioni (in origine non necessariamente consistenti in dati personali) che ciascun individuo rilascia in Rete, analizzandole ed elaborandole, anche in combinazione con ulteriori dati pubblici di tipo statistico o demografico, in modo da ricavarne ulteriori informazioni personali, intime e riservate, come ad esempio l'orientamento politico-ideologico o religioso dei singoli individui. Le informazioni così desunte vengono trattate a fini di profilazione, di predizione e di persuasione, senza però che gli interessati abbiano prestato il proprio consenso a tali tipi di trattamenti, anche perché nessuno può prevedere ab origine a quali risultati condurranno i processi di elaborazione, che tipo di dati potranno esserne derivati o inferiti e conseguentemente quale utilizzo ne verrà fatto. Queste dinamiche evidenziano l'insufficienza dell'approccio basato unicamente sul consenso dell'interessato al trattamento dei propri dati, problema di cui il legislatore europeo si sta occupando nella proposta di regolamento sulla e-privacy, che dovrebbe sostituire l'attuale direttiva 2002/58/Ce. Anche il Garante per il trattamento dei dati personali, nei due provvedimenti emanati nel 2014 e nel 2019 sul trattamento dei dati personali per la propaganda politica, entrambi fondati sulla necessità di acquisire il consenso dell'interessato per l'utilizzo dei suoi dati, non ha comunque risolto il problema dell'asimmetria nel rapporto fra cittadini e gestori delle piattaforme digitali.

Il problema di fondo è sempre quello, ricorrente nella progressiva disciplina di tutti i mezzi di comunicazione, della manipolazione dell'opinione pubblica e del consenso elettorale, che inficia il principio della sovranità popolare. Le questioni prospettate nel libro non sono certo di facile soluzione. Tuttavia, il diritto non può e non deve rinunciare alla sua funzione regolatoria, una volta dimostrata l'insufficienza di un approccio che fa affidamento quasi esclusivo sull'attitudine e la capacità dei social media di autodisciplinarsi. Nonostante le difficoltà, occorre definire almeno un corpus normativo minimo, di livello auspicabilmente europeo, finalizzato a correggere alcune fra le più evidenti distorsioni, affinché il delicato compito della formazione dell'opinione pubblica, soprattutto nei contesti elettorali, non risenta dei condizionamenti derivanti dalle logiche del mercato cui le piattaforme digitali inevitabilmente ubbidiscono.