



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

FORUM A CURA DI
RAFFAELLA BRIGHI - THOMAS CASADEI - ALBERTO SCERBO

Giustizia e tecnologia: tra potenzialità e nuovi rischi. Introduzione al forum

contributi di

MICHELE FERRAZZANO - EMANUELE ANDREIS - FLOR MARÍA ÁVILA
HERNÁNDEZ - WANDA D'AVANZO - FERNANDA FAINI –
FEDERICO CASA - ARIANNA MACERATINI

2/2023

RAFFAELLA BRIGHI* - THOMAS CASADEI** - ALBERTO SCERBO***

Giustizia e tecnologia: tra potenzialità e nuovi rischi.

Introduzione al forum****

Le sfide poste al diritto dalle profonde trasformazioni che gli sviluppi scientifici e tecnologici, compresa la più recente esplosione della Intelligenza Artificiale (IA), hanno indotto nella società permeano ogni dimensione delle nostre vite e mutano i tratti stessi dell'esperienza giuridica¹.

Gli articoli di questo *focus* affrontano, da angolature diverse, alcuni aspetti rilevanti di siffatte mutazioni.

Le riflessioni condotte dalle autrici e dagli autori si articolano in due direttrici: la prima è quella delle opportunità che l'innovazione tecnologica ha creato per il mondo del diritto, in particolare per il funzionamento della giustizia (ma non solo); la seconda è quella della sua possibile regolazione a fronte dell'impatto che ha su ogni aspetto della vita sociale, istituzionale ed economica, con la determinazione di nuovi rapporti e di inedite configurazioni del potere che possono comportare la creazione di forme di discriminazione digitale e algoritmica².

Seguendo la prima direttrice, a vent'anni dalle prime disposizioni in materia di processo civile telematico e all'alba di una nuova e importante riforma del sistema giudiziario, la cosiddetta "riforma Cartabia" (che ha introdotto, tra l'altro, una disciplina organica e completa dell'Ufficio del processo, struttura organizzativa a supporto del lavoro giudiziario e amministrativo per l'abbattimento dell'arretrato pendente e dei tempi del processo), è indubbio che la digitalizzazione sia un presupposto essenziale

* Professoressa associata di Informatica giuridica nell'Università di Bologna.

** Professore ordinario di Filosofia del diritto nell'Università di Modena e Reggio Emilia.

*** Professore ordinario di Filosofia del diritto presso l'Università degli studi *Magna Græcia* di Catanzaro.

**** *This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU).*

¹ In una letteratura in rapida espansione si possono vedere, S. AMATO, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020; F. PASQUALE, *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale*, LUISS University Press, Roma, 2021; S. SALARDI, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, Giappichelli, Torino, 2023.

² Su questi profili, si possono vedere, a titolo indicativo: S. VANTIN, *Il diritto antidiscriminatorio nell'era digitale: potenzialità e rischi per le persone, la pubblica amministrazione, le imprese*, Wolters Kluwer, Milano, 2021. Cfr., anche, E. FALLETTI, *Discriminazione algoritmica: una prospettiva comparata*, Giappichelli, Torino, 2023.

delle riforme e sia fondamentale per l'efficientamento del sistema giustizia in applicazione del *Piano Nazionale di Ripresa e Resilienza*.

Digitalizzazione completa dei fascicoli, informatizzazione dei flussi, *data lake* condivisi per i dati grezzi del sistema giudiziario, interoperabilità e integrazione di banche dati e sistemi, formalizzazione della semantica del dato e – profilo particolarmente interessante anche in chiave giusfilosofica – sviluppo di “ontologie giuridiche” sono alcuni degli elementi della trasformazione digitale del “sistema giustizia” nel nostro Paese³.

A questi si aggiungono molteplici studi e sperimentazioni sui possibili usi di sistemi di IA nel processo, a supporto per esempio delle fasi di ricognizione della prova, della fase istruttoria, dell'interpretazione, nel fare predizione o nella predisposizione dei testi⁴.

In particolare, le prospettive offerte dall'applicazione di strumenti di IA nell'informatica forense, disciplina che si occupa della individuazione e valutazione di elementi digitali avente valore probatorio nei procedimenti giudiziari⁵, sono esaminate nel contributo di **Michele Ferrazzano**, che ne illustra i vantaggi in termini di maggiore velocità, precisione e accuratezza delle attività investigative. L'IA in questo campo può essere di ausilio sia nell'automazione delle diverse fasi del trattamento della *digital evidence*

³ Un forte impulso alla digitalizzazione della giustizia è avvenuto con il progetto *UNI4Justice* finanziato dal programma PON (Programma Operativo Nazionale Governance e Capacità Istituzionale) 2014-2020, per contribuire alla realizzazione di un obiettivo di importanza strategica primaria del PNRR: un'organizzazione degli uffici giudiziari, civili e penali, più efficiente, più efficace e più vicina a cittadini e cittadine. Su questi profili si può vedere, da ultimo, F. Costantini, *Giustizia elettronica e digitalizzazione giudiziale: contesto europeo ed esperienza italiana*, in Th. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche: questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, seconda edizione aggiornata e ampliata, Wolters Kluwer, Milano, 2023.

⁴ Sulle nuove applicazioni si possono vedere, *ex multis*, K.D. ASHLEY, *Artificial intelligence and legal analytics: new tools for law practice in the digital age*, Cambridge University Press, Cambridge, Regno Unito, 2020; il fascicolo monografico *Artificial Intelligence for Justice* della rivista “*Artificial Intelligence and Law*”, 25 (3), 2017 (a cura di F. BEX, H. PRAKKEN, T. VAN ENGERS, B. VERHEIJ).

Per una analisi delle esperienze italiane i contributi di M. PALMIRANI, S. SAPIENZA, C. BOMBREZZI, *Il ruolo dell'intelligenza artificiale nel sistema giustizia: funzionalità, metodologie, principi* e di S. PELLEGRINI, S. BENEDETTI, *L'utilizzo di strumenti di intelligenza artificiale nel contrasto alla criminalità organizzata di stampo mafioso*, in M. PALMIRANI, S. SAPIENZA (a cura di), *La trasformazione digitale della giustizia nel dialogo tra le discipline. Diritto e intelligenza artificiale*, Prefazione di M. CARTABIA, Giuffrè, Milano, 2022, rispettivamente a pp. 1-36 e a pp. 255-296.

⁵ Per un inquadramento e una ricognizione degli elementi salienti: R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, prefazione di C. Maioli, Aracne, Roma, 2022.

(estrarre informazioni da set di dati complessi, identificare soggetti, estrarre tracce audio da file multimediali, analisi del linguaggio naturale e classificazione dei contenuti crittografati) sia nel guidare l'esperto nella valutazione delle potenziali prove digitali attraverso l'interpretazione di fatti noti con l'integrazione e la correlazione delle diverse tracce trovate.

Tuttavia, l'eventuale mancanza di controllo e trasparenza di tali strumenti comprometterebbe i requisiti di genuinità e verificabilità che devono essere garantiti nel trattamento di ogni prova informatica. Muovendo da tale contesto, il contributo di **Emanuele Andreis** riflette sul mutamento indotto alla figura dell'operatore del diritto dall'impiego delle tecnologie emergenti nelle professioni forensi per verificare se l'affidarsi ai sistemi informatici possa ridimensionare la stessa consapevolezza "giuridica" dei giuristi e, ancor più, la loro profondità culturale con il rischio di rendere il controllo umano *ex post* irrealizzabile⁶.

La giustizia digitale, inoltre, secondo le analisi di **Flor María Ávila Hernández**, che esamina, in particolare, le iniziative condotte dagli Stati dell'America Latina, se da un lato ha il pregio di avvicinare i tribunali alle aree rurali o remote, d'altro canto, per avere una portata veramente universale deve affrontare il problema delle disuguaglianze nell'accesso alla tecnologia che colpiscono in particolare le minoranze, le donne e altri gruppi vulnerabili e pertanto il nodo dei divari digitali⁷.

Il ruolo essenziale delle reti di telecomunicazione e, più in generale, dell'impiego efficiente di tecnologie all'avanguardia, reso evidente dal recente periodo pandemico, è sottolineato anche da **Wanda D'Avanzo** per quanto riguarda la sanità elettronica, campo di interazione tra uomo e macchina che solleva diverse preoccupazioni sulle conseguenze legali ed etiche. *L'eHealth*⁸, oltre a strumenti di base ormai consolidati legati più

⁶ Per un'ampia disamina di questi profili si rinvia a S. SALARDI, M. SAPORITI (a cura di), *Le tecnologie 'moralì' emergenti e le sfide etico-giuridiche delle nuove soggettività*, Torino, Giappichelli, 2020.

⁷ Per un'ampia e sistematica trattazione: J. VAN DIJK, *The digital divide*, Polity press, Cambridge, Medford, 2020. Cfr., anche, M. RAGNEDDA, G. MUSCHERT (eds.), *Theorizing Digital Divides*, Routledge, New York-London, 2017. Getta uno sguardo su alcuni effetti delle tecnologie, a partire dai rischi di ingiustizia (e dalle modalità per prevenirli e contrastarli), B.G. BELLO, *(In)giustizie digitali. Un itinerario su tecnologie e diritti*, Pacini, Pisa, 2022.

⁸ Per un inquadramento delle principali tematiche si rinvia a G. FIORIGLIO, *Informatica medica e diritto. Un'introduzione*, Mucchi, Modena, 2020. Cfr., inoltre, in precedenza: M. MANCARELLA, *eHealth e diritti. L'apporto dell'Informatica giuridica*, Carocci, Roma, 2013; E.H. SHORTLIFFE, J.J. CIMINO (eds.), *Biomedical Informatics. Computer Applications in Health Care and Biomedicine*, Springer, New York, 2014; C. FARALLI, R. BRIGHI, M. MARTONI (a cura di),

specificatamente agli aspetti documentali, quali il fascicolo sanitario elettronico e la cartella clinica, nonché all'informatizzazione di processi amministrativi e organizzativi, ci sta proiettando verso la realizzazione dell'*Internet dei corpi* con la creazione di una nuova generazione di dispositivi in grado di raccogliere ed elaborare dati e informazioni in tempo reale, capaci di integrarsi e interagire costantemente con il corpo di chi li utilizza. Tale convergenza pone nuovi interrogativi non solo dal punto di vista della protezione dei dati personali, ma anche in relazione alla sicurezza delle informazioni, alla sicurezza fisica delle persone e a questioni cruciali sotto il profilo bioetico⁹.

Venendo alla seconda direttrice, **Fernanda Faini** esamina il modello filosofico, etico e giuridico di "*governance della tecnologia*", in grado di tutelare la persona e i suoi diritti, così come emerge alla luce della normativa europea degli ultimi anni, volta a regolare la dimensione digitale nei suoi diversi aspetti, prestando attenzione anche alle mutate articolazioni del potere. La politica dell'Unione, come illustra Faini, promuovendo un approccio basato sul rischio e con esso una tutela preventiva¹⁰, è orientata a raggiungere un equilibrio tra i diversi interessi in gioco, dal momento che è teso alla tutela dei diritti della persona, ma è anche orientato alla crescita economica e al mercato.

Mentre la portata dei fenomeni di *digital divide*, intesi come partecipazione della popolazione ai circuiti di fruizione e creazione della informazione, in alcune aree del pianeta sembra in fase di attenuazione, **Federico Casa** riflette su come la filosofia del diritto debba spostare il suo interesse sulle discriminazioni digitali, quale effetto negativo dell'affermazione dell'intelligenza artificiale, ossia sullo studio delle nuove disuguaglianze generate o aggravate dalla IA¹¹. Sotto questo profilo, si tratta di comprendere se la necessità di regolare l'intelligenza artificiale

Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth, Giappichelli, Torino, 2015; C. BOTRUGNO, *Telemedicina e trasformazione dei sistemi sanitari. Un'indagine di bioetica*, Aracne, Roma, 2018. Per un interessante e controverso caso di studio: F. LAGIOIA, G. CONTISSA, *The strange case of Dr. Watson: liability implications of AI evidence-based decision support systems in health care*, in "*European Journal of Legal Studies*", 2020, 2, pp. 245-289.

⁹ Su questo versante: L. PALAZZANI, *Dalla bio-etica alla tecno-etica: nuove sfide al diritto*, Giappichelli, Torino, 2017; Ead., *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Studium, Roma, 2020.

¹⁰ Per uno sguardo critico si può vedere E. ORRÙ, *Legittimità e digitalizzazione: per una critica realistica delle politiche di sicurezza dell'Unione europea*, Wolters Kluwer, Milano, 2022.

¹¹ Su questo aspetto, in chiave radicalmente critica, K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro dell'IA*, il Mulino, Bologna, 2022.

consenta di poter avere alcune informazioni sul significato stesso del diritto nell'esperienza umana nell'epoca della pervasività della rete e dell'uso delle tecnologie¹². Non ci si può dunque sottrarre ad un "confronto sui cambiamenti antropologici, sugli aspetti etici connessi alle nuove tecnologie, sui profili di responsabilità, ma sempre con la volontà di ripensare 'sul serio' l'identità attuale del giurista e soprattutto di ricercare le origini dei problemi posti dalla realtà. Per non restare ancorati al piano dell'operatività, ma con la velleità di ripensare l'artificiale nell'alveo di quanto appartiene alla natura dell'essere"¹³, individuandone le potenzialità e, a tempo stesso, indagandone i rischi.

Come sottolinea **Anna Maceratini** l'uso improprio dell'informazione digitale porta a una progressiva concentrazione di conoscenze in grado di determinare pericolose asimmetrie cognitive e squilibri di potere, con rischiose implicazioni per la democrazia¹⁴.

Le nuove disparità digitali, accentuate dall'uso di sistemi predittivi e algoritmi¹⁵, richiedono pertanto l'adozione di "politiche d'uso" mirate e di azioni di regolazione consapevoli, unite a un forte impegno di educazione e formazione continua, valorizzando l'inclusione dei più vulnerabili perché possano esercitare, effettivamente, una cittadinanza attiva anche digitale.

Sotto questo profilo, nel considerare il rapporto tra tecnologia, diritto e società sono di riferimento ancora oggi le parole di Vittorio Frosini che nel volume del 1968 *Cibernetica. Diritto e società*¹⁶ osservava "[...] questo mondo artificiale non è un mondo disumano; anzi esso è creazione proprio della coscienza umana, voluto e fatto dagli uomini, ai quali esso è dunque pienamente omogeneo, assai più dello stesso mondo naturale; il mondo

¹² Interrogativi sui quali si cimentano, entro una visione d'insieme, i contributi raccolti nel fascicolo monografico della rivista *"Teoria e critica della regolazione"*, 2/2021, dedicato a *Teoria e prassi dell'informatica giuridica. Per una riflessione filosofica* (a cura di A. Scerbo).

¹³ A. SCERBO, *Introduzione*, in *"Teoria e critica della regolazione"*, 2/2021, pp. 7-10, p. 9.

¹⁴ Sul punto, in un'ampia letteratura, si possono vedere: S. PIETROPAOLI, *Da cittadino a user. Capitalismo, democrazia e rivoluzione digitale*, in A. CAVALIERE, G. PRETEROSSO (a cura di), *Capitalismo senza diritti?*, Quaderni del Laboratorio H. Kelsen, Mimesis, Milano-Udine, 2021, pp. 31-41; M. BETZU, *I baroni del digitale*, Editoriale scientifica, Napoli, 2022.

¹⁵ Su questi profili, entro una letteratura in espansione: A. GARAPON, J. LASSÈGUE, *La giustizia digitale: determinismo tecnologico e libertà* (2019), a cura di M.R. FERRARESE, il Mulino, Bologna, 2021; il fascicolo monografico della rivista *"Ars interpretandi"*, 1/2021, dedicato a *Algoritmi ed esperienza giuridica* (a cura di A. ANDRONICO, TH. CASADEI). Cfr., da ultimo, F. CORONA, *Giustizia predittiva: quando gli algoritmi pervadono il diritto*, Aracne, Roma, 2023.

¹⁶ Il volume è stato di recente ripubblicato, con introduzione di G. Sartor, nella Collana *"La Memoria del Diritto"* (Roma Tre Press, 2023).

della tecnica è infatti il vero mondo degli uomini, il mondo civile, in cui si dispiega la ragione operativa”¹⁷.

Su queste basi, in un tempo in cui le potenzialità delle tecnologie di oggi erano inimmaginabili, Frosini anticipa l’esigenza di trovare una prospettiva unitaria in cui le opportunità offerte dalle tecnologie e i rischi che esse comportano siano considerati alla luce di una ampia visione ‘umanistica’, ossia incentrata sull’uomo e sulla società: “la civiltà cibernetica [...] comporta una modificazione radicale della condizione umana e crea un genere finora sconosciuto di coscienza esterna dell’uomo, in cui si riflette una nuova composizione della società con un marcato carattere tecnologico. Noi riteniamo [...] che la coscienza interna non debba venire soffocata o disgregata per questo: la coscienza operativa consiste nella tensione tra le due forme, per cui il nuovo atteggiamento dell’una impone una reazione dell’altra, ma non la sua scomparsa”¹⁸.

Quella prefigurata è pertanto una prospettiva di integrazione, dunque, e non di sostituzione che permetta di potenziare le capacità dell’essere umano in nuovi spazi di azione e interazione di fronte alle molteplici sfide legate alla trasformazione digitale e, in particolare, a quelle più dirompenti dell’intelligenza artificiale.

Le riflessioni proposte in questo forum si sono sviluppate, parzialmente, nell’ambito del progetto di ricerca ‘EcoCyber’ (****), coordinato dall’Università di Bologna, all’interno del “partenariato esteso” SERICS (SEcurity and RIghts In the CyberSpace) che, raccogliendo una importante linea di investimento del MUR per il PNRR, promuove ricerche di base su *Cybersecurity, nuove tecnologie e tutela dei diritti*.

Il rischio cyber è globale e di primaria importanza¹⁹ e deve essere affrontato sul piano giuridico, politico, sociologico e etico, oltre che tecnico. Attacchi informatici più aggressivi e sofisticati sono motori di altri rischi non strettamente tecnologici: come emerge dai contributi qui raccolti, discriminazione e controllo sociale, concentrazione del potere digitale, campagne di disinformazione.

¹⁷ V. FROSINI, *Cibernetica. Diritto e società*, cit. p. 124.

¹⁸ Ivi, p. 125.

¹⁹ Su veda sul punto la Relazione annuale (2022) al Parlamento della Agenzia per la Cybersicurezza nazionale.

2/2023

Questi fenomeni possono mettere a rischio i diritti e le libertà fondamentali su cui la comunità si poggia, alterare gli equilibri politici di una nazione e, se sono colpite infrastrutture critiche, determinare gravi conseguenze per comunità, istituzioni, cittadinanza e imprese.

Il progetto promuove dunque un approccio giuridico, strategico e operativo alla cybersicurezza che integra per concezione i diritti fondamentali, compresi i diritti alla privacy e alla protezione dei dati personali, che sono necessari per proteggere i cittadini e i dati dell'UE dagli attacchi informatici. Una sua linea di ricerca è quindi dedicata a promuovere una cultura della sicurezza cyber per sviluppare comportamenti corretti a livello individuale e un approccio consapevole alla sfera digitale.

Sotto questo profilo, colmare il divario digitale – specificamente affrontato in alcuni dei contributi qui pubblicati – è cruciale al fine di migliorare la consapevolezza dei rischi e diffondere pratiche di “igiene” informatica.

Garantendo un accesso equo alla tecnologia e alla cultura digitale, gli individui sono abilitati a prendere decisioni informate nel mondo digitale e a proteggersi dalle minacce cibernetiche.

Queste pratiche di cittadinanza digitale, a loro volta, dovrebbero contribuire a un panorama digitale più equo.



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

MICHELE FERRAZZANO

L'intelligenza artificiale a servizio delle attività di informatica forense

ABSTRACT - The article explores the use of artificial intelligence in digital forensics, highlighting how advanced machine learning technologies can support the analysis of digital data in judicial contexts. Through an overview of the discipline and its practical applications, it discusses the potential for improving investigation efficiency, optimizing time and costs through the automation of traditional tasks. The critical role of artificial intelligence in managing cyber incidents and classifying evidence is analyzed, emphasizing the importance of human-machine collaboration in addressing the technical, legal, and ethical challenges posed by technological evolution.

KEYWORDS - Artificial Intelligence - digital forensics - machine learning - cyber incident management - automation of digital investigations

2/2023

MICHELE FERRAZZANO*

L'intelligenza artificiale a servizio delle attività di informatica forense**

SOMMARIO: *Premessa – 1. Definizioni e oggetto dell'informatica forense – 2. Intelligenza artificiale, machine learning e decisioni automatizzate – 3. Il ruolo dell'intelligenza artificiale nell'informatica forense – 4. Sistemi di intelligenza artificiale nella gestione di incidenti informatici e di indagini informatiche – Conclusioni e Prospettive.*

Premessa

Negli ultimi anni si è acceso un intenso dibattito nel mondo giuridico su come regolamentare l'impiego e le possibili applicazioni dell'intelligenza artificiale in vari campi¹, tenendo a mente i risvolti etici correlati all'uso di questi sistemi².

La possibilità di delegare un sistema informatico nell'assunzione di decisioni complesse è un'idea che diversi studiosi accarezzano da tempo³. In particolare, impiegare sistemi informatici per assumere decisioni in

* Professore a contratto di Informatica all'Università di Modena e Reggio Emilia, Professore a contratto di Computer forensics all'Università di Milano Statale, Cultore della materia Informatica giuridica all'Università di Bologna.

** Contributo sottoposto a valutazione anonima.

¹ Per un inquadramento della genesi e degli sviluppi dell'intelligenza artificiale si veda T. CASADEI, S. PIETROPAOLI, *Intelligenza artificiale: fine o confine del diritto?*, in T. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters-Kluwer-Cedam, Milano, 2021, pp. 219-232.

Per alcuni recenti percorsi d'indagine si vedano: S. SALARDI, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, Giappichelli, Torino, 2023; J. SEARLE, *Intelligenza artificiale e pensiero umano: filosofia per un tempo nuovo*, Castelvechi, Roma, 2023; U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020.

² Sul tema dell'etica dei sistemi di intelligenza artificiale: L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022; F. FOSSA, V. SCHIAFFONATI, G. TAMBURRINI (a cura di), *Automi e persone. Introduzione all'etica dell'intelligenza artificiale e della robotica*, Carocci, Roma, 2021; G. TAMBURRINI, *Etica delle machine. Dilemmi morali per robotica e intelligenza artificiale*, Carocci, Roma, 2020. Per un approfondimento sull'approccio europeo al tema dell'etica e intelligenza artificiale si veda F.H. LLANO-ALONSO, *L'etica dell'intelligenza artificiale nel quadro giuridico dell'Unione europea*, in *Ragion pratica*, 2/2021, pp. 327-348.

³ Si vedano G. SARTOR, *Artificial intelligence in law and legal theory*, in *Current Legal Theory*, 1992, 10, pp. 1-59; G. SARTOR, *Judicial applications of artificial intelligence*, in *Artificial Intelligence and Law*, 7, 1998, pp. 157-372; F. ROSSI, *Il confine del futuro. Possiamo fidarci dell'intelligenza artificiale?*, Feltrinelli, Milano, 2019.

contesti di controversie giuridiche rappresenta uno dei principali campi applicativi, ipotizzando che in tal modo si possa raggiungere un maggiore senso di giustizia – eliminando la componente umana soggettiva – e potendo altresì ottenere un verdetto in tempi più rapidi⁴.

Sono così stati sviluppati numerosi sistemi esperti con l'obiettivo di prendere autonomamente decisioni sfruttando la rappresentazione di conoscenze giuridiche specialistiche in forma simbolica, con regole logiche e inferenze predefinite: i risultati, tuttavia, sono stati meno promettenti del previsto⁵.

La ricerca in tema di intelligenza artificiale è comunque proseguita e si è evoluta con nuovi metodi di apprendimento automatico molto efficaci che sfruttano la conoscenza derivante dall'analisi di grosse moli di dati (i c.d. *big data*⁶). Di conseguenza, i più recenti sviluppi hanno messo in discussione sia l'introduzione delle tecnologie di intelligenza artificiale in diversi sistemi giuridici, sia la sua sostenibilità etico-giuridica.

Una prova del potenziale di questi strumenti si trova dalla recente pubblicazione del sistema di intelligenza artificiale della OpenAI che permette a qualunque utente della rete Internet, previa registrazione, di poter interrogare l'interlocutore informatico con un linguaggio naturale e ottenere risultati che altrimenti richiederebbero tempo e competenze da ricercare sul mercato.

L'applicazione di sistemi basati su intelligenza artificiale coinvolge anche l'informatica forense⁷, la disciplina che si occupa del trattamento di dati digitali proprio a supporto del sistema giudiziario.

I sistemi di intelligenza artificiale possono favorire l'automazione di compiti tradizionali, ottimizzando il consumo di tempo e la qualità del processo di informatica forense, impattando in maniera significativa sui tempi e sui costi⁸.

Sono numerosi gli ambiti nei quali, già da tempo, vari strumenti commerciali supportano l'operatore di informatica forense che ha esigenza di svolgere compiti quali l'individuazione di oggetti di interesse in un file

⁴ G. CONTISSA, G. LASAGNI, G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet*, 4/2019, pp. 619-634.

⁵ G. SARTOR, *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022.

⁶ Per un'ampia disamina si veda F. FAINI, *Data society: governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis & Taylor, Milano, 2019.

⁷ Per una recente e articolata trattazione si rimanda a R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, prefazione di C. Maioli, Aracne, Roma, 2022.

⁸ R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, op. cit.

multimediale, il riconoscimento di volti umani relativi ai soggetti indagati o di interesse, la stima dell'età del minore in file pedopornografici.

Nel presente contributo, previo un inquadramento dell'informatica forense, si offrirà una panoramica di come gli strumenti di intelligenza artificiale – pur con i loro limiti – possono rappresentare uno strumento di supporto alle indagini informatiche, velocizzandone la conclusione e raffinando i risultati, riducendo anche errori e intervenendo quando l'operatore potrebbe non disporre di pari competenze tecniche.

1. *Definizioni e oggetto dell'informatica forense*

La diffusione su scala mondiale di sistemi informatici e telematici ha comportato l'esigenza di trattare dati digitali rilevanti in procedimenti giudiziari. Nacque così in ambienti giuridici anglosassoni la disciplina della *digital forensics*: con questa espressione si intende la scienza che si occupa di rispondere alle esigenze di giustizia relativamente all'analisi dei dati digitali a fini di investigazione e di giustizia per reati informatici, per reati non informatici ma commessi con sistemi informatici e reati per i quali si rinvenivano tracce o indizi nei sistemi informatici.

La prima definizione di informatica forense che troviamo nella dottrina italiana, ad opera di Cesare Maioli⁹, evidenzia che trattasi della «disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova».

Le procedure da seguire per trattare dati digitali a fini processuali sono così state inizialmente definite negli anni Ottanta dalla FBI e successivamente da varie organizzazioni, sino ad arrivare alla più recente definizione di un documento della ISO (International Standard Organization) che fornisce indicazioni relative al trattamento del dato informatico nelle prime fasi, come indicato nello standard ISO/IEC 27037¹⁰.

⁹ C. MAIOLI, *Introduzione all'informatica forense*, in P. Pozzi (a cura), *La sicurezza preventiva dell'informazione e della comunicazione*, FrancoAngeli, Milano, 2004.

¹⁰ Lo standard ISO/IEC 27037, emesso per la prima volta e aggiornato all'ultima versione del 2018, si colloca tra i documenti della serie 27000 relativa alla sicurezza delle informazioni.

In sintesi, il trattamento di dati informatici a fini forensi si propone di dare voce alle prove¹¹ attraverso le fasi di: 1) individuazione dei dati di interesse; 2) raccolta dei dati di interesse attraverso procedure tecniche di acquisizione forense che, rispettando le procedure del caso, si propongono di creare una copia dei dati senza apportare alterazioni; 3) analisi dei dati raccolti; 4) valutazione dei dati analizzati per ricostruire i fatti o smentire le valutazioni delle altre parti; 5) rappresentazione di tutte le fasi precedenti all'interno di un documento che confluisce nel procedimento giudiziario di competenza.

A seconda delle caratteristiche dei dispositivi che contengono i dati da trattare, è possibile identificare diverse aree di specializzazioni che potrebbero essere ripensate nel tempo in base allo sviluppo tecnologico. Ciascuna area presenta caratteristiche tecniche omogenee e analoghe implicazioni anche sotto il profilo della procedura da adottare¹².

La *disk forensics* è la principale e più antica branca dell'informatica forense che infatti nacque sotto il nome di *computer forensics*, occupandosi di supporti di memorizzazione di dati informatici come *hard disk* o chiavette USB che solitamente sono contenuti anche all'interno di *personal computer* e *laptop*.

Dal momento che i sistemi informatici si collegano a reti (siano esse locali o la rete Internet), è intervenuta nel tempo l'esigenza di raccogliere dati in transito durante le comunicazioni: si fa così riferimento alla *network forensics* nei casi in cui il dato non è memorizzato staticamente in una memoria ma va raccolto "a volo" durante il transito da un sistema informatico a un altro. Le procedure di *network forensics* impattano anche in tutti i casi in cui si raccolgono dati da sistemi remoti, come ad esempio le macchine virtuali e in generale i dati disponibili in *cloud*¹³.

Il successivo poderoso sopravvento preso da tablet e, soprattutto, smartphone ha portato poi all'esigenza di definire una nuova classe che risponde al nome di *mobile forensics*.

Oltre all'analisi di dati dei dispositivi mobili, si correlano spesso a queste attività le operazioni relative a: 1) il trattamento delle schede di memoria contenute in essi (che rientra nel novero delle attività di *disk*

¹¹ C. MAIOLI, *op. cit.*

¹² Si pensi ad esempio, in ambito di procedimento penale, l'esigenza di informare le parti in caso di accertamenti tecnici che possono causare modificazioni ai dati (art. 360 c.p.p.) oppure no (art. 359 c.p.p.).

¹³ Si pensi ad esempio al trattamento di dati memorizzati in sistemi di *cloud storage* come, ad esempio, citando i più diffusi, OneDrive, Dropbox, iCloud o GoogleDrive.

forensics); 2) l'esame di tabulati telefonici utili per geolocalizzare con approssimazione la posizione in cui si trovava l'utilizzatore dell'apparecchio in un momento passato, in caso di attività telefonica o telematica tramite abbonamento telefonico e non tramite connessione a reti wireless.

Sono poi presenti diversi casi non collocabili nelle categorie sopra definite in virtù del fatto che a determinare l'associazione sono le caratteristiche di *hardware* e *software* che compongono il sistema di interesse: si fa riferimento, ad esempio, a sistemi di antifurto, impianti di videosorveglianza, impianti industriali. Ognuno di essi porta, solitamente alla definizione di sub-categorie come, ad esempio, nel caso del trattamento di dati di autoveicoli che porta a coniare il termine *vehicle forensics*¹⁴.

Qualsiasi sia la categoria di riferimento, l'informatica forense è una disciplina applicabile a tutti gli ambiti del diritto. Per questo motivo, nel corso degli anni, gli ordinamenti giuridici nazionali e sovranazionali sono intervenuti per recepire le innovazioni tecnologiche sia tra le definizioni di reato sia tra le procedure da seguire.

Ad esempio, in ambito penale, i reati informatici fanno la loro comparsa nell'ordinamento giuridico italiano alla fine del 1993, quando con la Legge 23 dicembre 1993, n. 547¹⁵, vengono introdotti una serie di reati commessi a danno di sistemi informatici o che prevedono l'uso del sistema informatico come arma. Parallelamente, diverse modifiche sono state introdotte al codice di procedura penale per disciplinare le modalità con le quali è possibile raccogliere e trattare i dati nel rispetto delle garanzie per le difese. Tanto i reati quanto le procedure poi sono stati aggiornati negli anni, in particolare a seguito del recepimento della Convenzione di Budapest¹⁶ in tema di cybercrime del 2001 attraverso la Legge n. 48/2008 che ha portato a delineare definizioni comuni di reato tra i vari paesi, definire poteri comuni di indagine e predisporre mezzi di cooperazione internazionale.

¹⁴ M. FERRAZZANO, *L'informatica forense nella ricostruzione di incidenti stradali: dai veicoli a guida umana all'autonomous driving*, Giappichelli, Torino, 2019.

¹⁵ Legge 23 dicembre 1993, n. 547. "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

¹⁶ L. LUPARIA (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)*, Giuffrè, Milano, 2009.

2. Intelligenza artificiale, machine learning e decisioni automatizzate

L'Intelligenza Artificiale è un campo interdisciplinare della scienza e dell'ingegneria che si concentra sulla creazione di sistemi informatici che possono eseguire compiti che richiedono intelligenza umana, come il riconoscimento del linguaggio naturale, la visione artificiale, la pianificazione, il ragionamento, la decisione e l'apprendimento¹⁷. Alla base dell'intelligenza artificiale vi sono sistemi che si basano su metodi di apprendimento automatico avanzati come il *deep learning*¹⁸ e il *reinforcement learning*¹⁹.

L'intelligenza artificiale ha rivoluzionato il modo in cui è possibile assumere decisioni in una vasta gamma di settori, tra cui ormai già da tempo la sanità, la finanza, la gestione delle risorse umane e la produzione. Sono numerosi, da anni, i campi nei quali i sistemi di intelligenza artificiale supportano l'essere umano, grazie alla capacità di elaborare grandi quantità di dati in tempi rapidi, tramite identificazione di pattern (c.d. *pattern recognition*)²⁰ e capacità di estrarre informazioni utili per prendere decisioni.

Il *machine learning* è una branca dell'intelligenza artificiale che si occupa dello sviluppo di algoritmi che consentono ai computer di apprendere dai dati e migliorare le prestazioni nel tempo senza essere esplicitamente programmato, impiegando algoritmi per eseguire attività come la classificazione, la regressione, il clustering, la riduzione della dimensionalità e l'elaborazione del linguaggio naturale per analizzare i dati, identificare pattern e fare previsioni²¹.

Il processo di apprendimento automatico coinvolge: (1) la scelta di un modello di apprendimento, (2) la preparazione dei dati, (3) l'allenamento del modello, (4) la validazione e (5) l'ottimizzazione dei risultati. In tal modo, in molti contesti è possibile imparare – come un essere umano in crescita – a rilevare situazioni note o anche nuove, come identificare potenziali frodi nei pagamenti con carta di credito, identificare pattern di acquisto dei clienti o valutare la capacità creditizia di un cliente. Il machine learning può anche essere utilizzato per ottimizzare i processi di

¹⁷ S.J. RUSSELL, P. NORVIG, *Artificial intelligence: a modern approach*, vol. 25. Prentice hall, 2010.

¹⁸ I. GOODFELLOW, Y. BENGIO, A. COURVILLE, *Deep learning*, MIT press, Cambridge (Mass.) 2016.

¹⁹ R.S. SUTTON, A.G. BARTO, *Reinforcement learning: An introduction*, MIT press, Cambridge (Mass.), 2018.

²⁰ C.M. BISHOP, *Pattern recognition and machine learning*, Springer, Dordrecht, 2006.

²¹ T.M. MITCHELL, *Machine learning*, McGraw Hill, New York, 1997.

produzione, per prevedere le esigenze di manutenzione delle attrezzature o per identificare i rischi ambientali. L'obiettivo del processo di apprendimento automatico è quello di utilizzare questi modelli per fare previsioni su dati di test che non sono stati utilizzati per addestrare il modello.

Altri strumenti a supporto dell'intelligenza artificiale sono: la *programmazione genetica* che utilizza tecniche di evoluzione artificiale per generare soluzioni ottimali ai problemi, proponendosi di individuare le migliori configurazioni di produzione, per progettare nuovi prodotti o per valutare le prestazioni del personale; la *programmazione a vincoli*, che utilizza algoritmi per trovare soluzioni ai problemi tenendo conto, appunto, di un insieme di vincoli ed è impiegabile, ad esempio, nei casi in cui occorre pianificare la produzione, la distribuzione delle risorse o i turni dei dipendenti; i *sistemi esperti*, che utilizzano la conoscenza qualificata e navigata per elaborare le informazioni e formulare raccomandazioni, come ad esempio valutare le richieste di prestito, determinare il dosaggio dei farmaci o identificare i rischi di sicurezza; i *sistemi di supporto alle decisioni*, che aiutano gli utenti a prendere decisioni fornendo informazioni pertinenti e analisi per, ad esempio, analizzare dati finanziari, valutare i rischi di un'attività di investimento o fornire raccomandazioni di marketing personalizzate; infine, i sistemi di raccomandazione, che utilizzano algoritmi per analizzare i dati dei clienti e formulare raccomandazioni personalizzate in contesti come l'*e-commerce* nei quali si intende suggerire prodotti correlati e per personalizzare l'esperienza di acquisto dell'utente.

Tuttavia, è importante notare che l'utilizzo di strumenti di intelligenza artificiale per prendere decisioni può presentare punti critici. Ad esempio, ci possono essere problemi di *bias* algoritmico, in cui i modelli di intelligenza artificiale possono essere influenzati da pregiudizi inconsapevoli incorporati nei dati o, peggio, da insieme di dati di partenza viziati da errori²². Appare, quindi, superfluo notare che i dati utilizzati dagli strumenti di intelligenza artificiale devono essere scrupolosi e affidabili in quanto la loro qualità può influenzare l'accuratezza dei modelli di intelligenza artificiale e le raccomandazioni che vengono formulate.

²² In una letteratura in espansione si possono considerare: F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in "Federalismi.it", n. 11, 2020, pp. 85-110; T. CASADEI, *Istituzioni e algoritmi: tra strategie funzionali ed "effetti collaterali"*, in *Smart. La persona e l'infosfera*, in U. SALINITRO (a cura di), Pacini giuridica, 2022, pp. 245-265; e, da ultimo, F. FALLETTI, *Discriminazione algoritmica. Una prospettiva comparata*, Giappichelli, 2022.

Tenendo conto di questo aspetto, l'intelligenza artificiale può senza alcun dubbio e timore di smentita essere un assai valido strumento di supporto alla decisione, senza che sostituisca completamente ragionamento e intuizione umana e, senza dimenticare che – in taluni casi – non è in grado di dimostrare anche un “briciolo di umanità” nella valutazione.

3. *Il ruolo dell'intelligenza artificiale nell'informatica forense*

Nell'ultimo decennio si è assistito alla generazione di nuove informazioni quasi esclusivamente attraverso l'uso di sistemi informatici e, parallelamente, alla digitalizzazione di ciò che era nato in formato analogico come ad esempio libri o video.

Lo scibile umano è dunque ormai in forma digitale. Qualsiasi attività investigativa oggi non può non tenere conto di questa realtà.

Le attuali procedure e pratiche di indagine digitale prevedono interazioni umane che richiedono tempo, rallentando così l'intero processo. Per questo motivo, molti progetti di ricerca, studi e prodotti professionali hanno iniziato a proporre soluzioni basate sull'intelligenza artificiale per superare gli ostacoli noti²³.

Nella storia dell'intelligenza artificiale sono stati sperimentati diversi approcci che hanno prestato attenzione ai modelli mentali e al ragionamento o al comportamento umano, nel tentativo di sviluppare sistemi che simulino l'esecuzione di compiti umani e di costruire sistemi idealmente intelligenti o sistemi che impieghino comportamenti razionali per agire correttamente.

Ai fini di questo contributo, viene evidenziato come l'intelligenza artificiale può essere uno strumento di grande supporto nell'esecuzione di compiti comunque affidati all'essere umano, consentendo però di completare l'elaborazione in tempi nettamente più rapidi e con una marginalità di errore significativamente ridotta.

²³ Sull'utilizzo dell'intelligenza artificiale nella *digital forensics*, si vedano: F. MITCHELL, *The Use of Artificial Intelligence in Digital Forensics: An Introduction*, in *Digital Evidence & Electronic Signature Law Review*, 35/2010, pp. 35 ss.; A.M. QADIR, A. VAROL, *The Role of Machine Learning in Digital Forensics*, in 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-5; A. JARRETT, K.R. CHOO, *The impact of automation and artificial intelligence on digital forensics*, in *Wires forensic science*, 3, 6/2021, pp. 1-17.

Non ci si focalizzerà su altre casistiche pure di elevato interesse scientifico, come ad esempio la possibilità che sistemi di intelligenza artificiali si rendano rei di comportamenti illeciti e attività dannose, con tutte le conseguenze giuridiche che ciò trascina tra cui, in particolare, le questioni rilevanti sulla responsabilità di tali azioni.

Le abilità sempre più sofisticate che troviamo nei sistemi di intelligenza artificiali non sono da intendere come replica dell'intelligenza umana; in molti casi, anzi, si distaccano dai processi cognitivi umani²⁴, al punto da sfuggire al controllo e alla comprensione dei loro stessi sviluppatori. Infatti, i processi che guidano gli algoritmi sono ormai completamente diversi dai processi della mente umana, e infatti nessuna mente umana o combinazione di menti umane potrebbe riprodurli e spesso nemmeno capirli²⁵.

L'obiettivo non è, quindi, raffrontare tali processi ai processi cognitivi umani, o – peggio – comparare le performance della mente umana con quella del sistema informatico, bensì mantenere viva l'attenzione sul rapporto tra l'intelligenza artificiale e l'essere umano, preservando il confine tra essi al fine di sfruttare quanto di utile essi propongono per l'umanità²⁶.

In tal senso, quindi, non si chiede ai sistemi di intelligenza artificiale di "risolvere" i casi di informatica forense, ma di supportare l'operatore umano nelle molteplici fasi che vanno dalla raccolta di informazioni alla presentazione dei risultati di un accertamento o di una prova in tribunale:

- *analisi dei dati*: l'intelligenza artificiale può essere utilizzata per analizzare grandi quantità di dati, ad esempio registrazioni telefoniche, e-mail e messaggi di testo, per identificare modelli o anomalie che potrebbero essere rilevanti per l'indagine, previa creazione di "modelli di interesse" che possono essere individuati e messi all'attenzione dell'utente;
- *riconoscimento di immagini*: l'intelligenza artificiale può essere utilizzata per identificare i contenuti di file multimediali (immagini o video) in modo da catalogarne i contenuti, come ad esempio armi, sostanze stupefacenti, pedopornografia, piuttosto che situazioni come ad esempio partite di calcio, programmi televisivi, scene di violenza e

²⁴ E. DI MAURO, *La Mente umana e la mente artificiale*, Asterios, 2018.

²⁵ E. ESPOSITO, *Dall'Intelligenza artificiale alla comunicazione artificiale*, in *Aut Aut*, 392/2021, 20-34.

²⁶ M. ZANICHELLI, *L'intelligenza artificiale e la persona: tra dilemmi etici e necessità di regolazione giuridica*, in *Teoria e Critica della Regolazione Sociale*, 2/2021, 141-159.

così via; una più puntuale applicazione prevede il riconoscimento facciale dei soggetti ripresi, come capita nei nostri smartphone consultando la galleria, in modo da poter rilevare con precisione e velocità tutti i file nei quale determinati soggetti sono ripresi; i confronti possono avvenire così sulla base di singoli campioni messi a disposizione o di banche dati;

- *analisi del linguaggio naturale*: l'intelligenza artificiale può essere utilizzata per analizzare il linguaggio naturale – sia esso scritto o parlato – per identificare parole chiave o frasi rilevanti per l'indagine; nel caso del parlato, può essere di supporto per automatizzare processi altrimenti molto lunghi e dispendiosi come la trascrizione di audio;

- *analisi del comportamento*: l'intelligenza artificiale può essere utilizzata per analizzare il comportamento degli individui in modo da identificare schemi o anomalie che potrebbero essere rilevanti per l'indagine, come ad esempio l'analisi di uno stile di guida o di una camminata per distinguere il caso della persona sana da quella della persona sotto effetto di alcool o sostanze stupefacenti;

- *simulazione di scenari*: l'intelligenza artificiale può essere utilizzata per situazioni complesse come, ad esempio, un incidente stradale o la rottura di una fune di un impianto funiviario, per consentire di ricostruire gli eventi e darne una spiegazione più precisa.

Di seguito viene presentata una panoramica delle applicazioni dell'intelligenza artificiale nella *digital forensics*, evidenziando vincoli e vantaggi.

4. Sistemi di intelligenza artificiale nella gestione di incidenti informatici e di indagini informatiche

Ancora oggi, per difendersi dai cyber-attacchi nella quasi totalità dei casi vengono impiegati semplici soluzioni quali ad esempio software antivirus e difese perimetrali come i firewall. Tuttavia, gli attacchi informatici diventano sempre più sofisticati e le misure di sicurezza tradizionali sono ormai molto spesso inefficaci²⁷: ciò è dovuto anche al fatto

²⁷ La Cybersicurezza, considerata per decenni un settore meramente tecnico e per addetti ai lavori, è oggi finalmente al centro delle politiche della Unione europea che con la Strategia per la Cyber Security del 2020 ha intrapreso un percorso di definizione del quadro giuridico, politico e di investimenti unitario e all'altezza delle sfide attuali.

che il tempo necessario per rilevare e investigare le minacce quotidiane è crescente in un contesto nel quale mancano competenze, accuratezza e capacità di riconoscerle.

In questo quadro, sistemi di intelligenza artificiale possono essere in grado di intervenire in maniera efficiente contro le minacce alla sicurezza delle informazioni, rilevando e analizzando rapidamente milioni di registri ed eventi anomali, identificando file dannosi o riconoscendo un comportamento anomalo.

Un esempio pratico è rappresentato dai centri operativi di sicurezza (SOC). Un SOC è una struttura che ospita un gruppo di esperti di sicurezza informatica responsabile del monitoraggio continuo e dell'analisi della postura di sicurezza di un'organizzazione: l'obiettivo è quello di rilevare, analizzare e rispondere agli incidenti di cybersecurity utilizzando una combinazione di soluzioni tecnologiche e un solido insieme di processi. Considerando il numero di fonti di dati rilevanti, l'impossibilità di esaminare manualmente tutti i file di log è evidente e pertanto il supporto di un sistema basato su individuazione di eventi noti e non, dunque attraverso ragionamenti complessi di intelligenza artificiale, diventa indispensabile.

Questo ostacolo viene tradizionalmente superato affidandosi a un sistema che correla gli input di decine di fonti di sicurezza diverse, ciascuna delle quali monitora uno specifico vettore di attacco, in modo da notificare al SOC il verificarsi di un evento insolito.

Poiché il SOC scrive queste regole di correlazione dopo il verificarsi di un incidente, per essere avvisato del suo ripetersi, vi sono due aspetti negativi principali.

In primo luogo, si perdono diversi eventi importanti perché le regole di correlazione si basano su un insieme specifico di input. Se il SOC definisce regole troppo ristrette, il sistema non si attiverà per eventi minimamente diversi. Considerando la variabilità all'interno dell'organizzazione di applicazioni, sistemi e ambienti, è improbabile che due attacchi siano identici.

In secondo luogo, se le regole non sono abbastanza restrittive, si possono riscontrare risultati falsi positivi: ciò comporta il rischio di mascherare gli attacchi reali a causa della generazione di innumerevoli avvisi che non possono essere prontamente filtrati dal SOC per identificare

le minacce reali²⁸.

Ecco, quindi, che i sistemi di intelligenza artificiale diventano fondamentali per sopperire alle intrinseche criticità che la componente umana e la complessità tecnica del fenomeno richiedono. È comunque evidente che un sistema, per quanto intelligente, può essere vittima di errori e pertanto non può allo stato essere delegato in toto questo ruolo, divenendo necessario “l’ultimo clic” in capo a un operatore umano.

Focalizzandosi invece nel più ampio contesto dell’esame di dati digitali, per come è stata già presentata, la *digital forensics* prevede un momento nel quale i dati devono essere soggetti ad analisi forense per ricercare le evidenze di interesse per lo specifico caso al quale si è chiamati a rispondere. Molto spesso l’analisi verte su grandi quantità di dati che richiedono sempre più una forte interazione umana per giungere a comprendere cosa è presente nei file a disposizione. Conseguentemente, l’analisi supportata da sistemi intelligenti è una esigenza che ormai è diventata ineludibile da parte di forze di polizia e consulenti tecnici che si avvicinano a una investigazione digitale.²⁹

Poiché, tuttavia, a valle del processo investigativo di informatica forense vi è esigenza di documentare in dettaglio tutto ciò che è stato fatto, occorre prestare attenzione a quanto necessario per spiegare il processo di ragionamento che è dietro all’attività svolta e ai risultati ottenuti.

Uno dei principali inconvenienti dei sistemi esperti risiede nel fatto che potrebbero non funzionare bene con grandi quantità di dati, specie se non particolarmente noti come categoria in precedenza, circostanza in forte contrapposizione con l’ordinaria disponibilità di tanti dati nelle indagini forensi digitali nelle quali ciò che si incontra è spesso rilevato per la prima volta³⁰.

L’identificazione di tipi o cluster specifici di dati in un’indagine è gestita al meglio da un tipo di intelligenza artificiale che si occupa di “riconoscimento di modelli”. Il tipo di riconoscimento di modelli con cui le persone hanno più familiarità è il riconoscimento di immagini, in cui il

²⁸ R. BRIGHI, M. FERRAZZANO, L. SUMMA, *Legal issues in AI forensics: understanding the importance of humanware*, in “i-Lex”, 1/2020, pp. 19-42.

²⁹ Cfr. A. KRIVCHENKOV, B. MISNEVS, D. PAVLYUK, *Intelligent methods in digital forensics: State of the art*, in *Reliability and Statistics, in Transportation and Communication*, Springer, Cham, 2018, pp. 274-284; F. MITCHELL, *The use of artificial intelligence in digital forensics: An introduction*, in *Digital Evidence and Electronic Signature Law Review*, 7/ 2010, pp. 35-41.

³⁰ S. COSTANTINI, G. DE GASPERIS, R. OLIVIERI, *Digital forensics and investigations meet artificial intelligence*, in *Annals of Mathematics and Artificial Intelligence*, 86/2019, pp. 193-229.

2/2023

software tenta di identificare parti di un'immagine. Esistono molti altri esempi di riconoscimento di pattern, come il rilevamento di un pattern in un'email di spam o di un pattern di una specifica tipologia di file (es. audio, video, eseguibile...) in un'immagine forense di un disco. Molte delle tecniche utilizzate per questi riconoscimenti si basano pesantemente sulla statistica o sul ragionamento probabilistico, o su entrambi.

Le forme più complesse e accurate di riconoscimento delle immagini, che possono essere utilizzate per individuare determinati tipi di contenuti, si basano sulla consapevolezza del funzionamento del sistema percettivo umano. Tuttavia, questi strumenti hanno attualmente un alto tasso di falsi positivi e falsi negativi (a seconda di dove si trovano le soglie), oltre ad essere molto pesanti sotto un profilo computazionale, ma comunque permettono una catalogazione più rapida della consultazione dell'essere umano. Motivo per il quale è premiante delegare al sistema di intelligenza artificiale la prima catalogazione e passare poi il testimone all'operatore umano che può compiere l'approfondimento solo sulle categorie di interesse, ovvero validare i risultati raggiunti dal sistema.

Conclusioni e prospettive

Tenuto conto di quanto è in continua espansione l'archiviazione di dati in forma digitale all'interno di sistemi informatici, il carico di lavoro dell'operatore che si occupa di esaminare dati per finalità di informatica forense è evidentemente aumentato e destinato a crescere ulteriormente: di contro, per una più efficace azione di individuazione delle minacce e di repressione dei fenomeni illeciti, una risposta reattiva con processi attivabili in tempi rapidi è necessaria per preservare le evidenze ed analizzare i dati per poter svolgere le opportune valutazioni.

I sistemi di intelligenza artificiale e le tecniche di *machine learning* consentono di automatizzare compiti tradizionali, ottimizzando il consumo di tempo e la qualità del processo di informatica forense, con un impatto significativo sui tempi e sui costi.

Si possono evidenziare diversi casi in cui l'informatica forense si avvale proficuamente di sistemi di intelligenza artificiale, come ad esempio la classificazione di evidenze tra rilevanti e non rilevanti, l'individuazione di oggetti di interesse in un file multimediale, il riconoscimento di volti umani relativi ai soggetti indagati o di interesse, la stima dell'età della persona coinvolta in attività sessuale che può essere individuata come un

minore e conseguentemente materiale relativo a sfruttamento sessuale dei minori. Senza dimenticare anche la tutela della sfera personale che, per tramite di un sistema di intelligenza artificiale che effettivamente sia progettato per comportarsi con riservatezza, consente di ottimizzare i tempi e la qualità del processo forense con un occhio particolare al mantenimento del segreto di ciò che, pur esaminato, risulti non rilevante.

Per tutto quanto esposto, l'applicazione di soluzioni di intelligenza artificiale all'interno della *digital forensics* non solo appare come una importante opportunità da cogliere ma come una necessità non ulteriormente rinviabile, tenuto conto che comunque spetta all'essere umano validare i risultati del lavoro proposti dal sistema intelligente.

Infatti, per quanto l'attività umana non possa (e non debba, allo stato attuale della tecnologia) essere sostituito da una macchina, le competenze umane devono rimanere fondamentali per affrontare tutte le questioni tecniche, giuridiche ed etiche che l'intelligenza artificiale pone interfacciandosi con l'informatica forense. Ciò anche in virtù di come sono strutturati i procedimenti giudiziari oggi, nei quali il ruolo del consulente tecnico o del testimone sono cruciali per spiegare ciò che il dato informatico propone, con tutte le conseguenze in tema di ammissibilità rispetto alle modalità di trattamento.

Come si potrebbe realizzare un modello del genere?

Come anticipato, l'uso di sistemi di intelligenza artificiale non deve intorpidire ma, al contrario, stimolare gli operatori umani che si interfacciano: se mal programmati, come ogni strumento, possono generare più danni che benefici. Risulta quindi ancor più indispensabile lavorare alla formazione qualificata degli operatori di forze dell'ordine e di professionisti privati che siano in grado di affrontare problematiche tecniche, giuridiche ed etiche causate dall'introduzione di sistemi di intelligenza artificiale nei processi di analisi forense.

Lo sviluppo dei sistemi di intelligenza artificiale, invece, viene avanti da sé in quanto una delle maggiori aree di interesse della ricerca scientifica e, pertanto, appare fuori luogo fornire, in questa sede, linee guida e prospettive. Ci si limita ad evidenziare l'esigenza di tracciare come i processi decisionali vengono assunti al pari di quanto è richiesto al professionista che viene coinvolto come consulente tecnico o come agente di polizia giudiziaria in un procedimento giudiziario³¹.

³¹ R. BRIGHI, *Informatica forense, algoritmi e garanzie processuali*, in "Ars Interpretandi", 26/2021, pp. 153-164.



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

EMANUELE ANDREIS

L'informatica nelle professioni giuridiche e lo spazio dell'intelligenza umana

ABSTRACT - Following an analysis of the evolution of procedural disciplines pursuant the development of telematic and electronic trial, this paper investigates the IT tools that lawyers, prosecutors and judges have to use as well as the newest artificial intelligence (AI) softwares available for their activities. Without stepping into the field of robot-justice system, the study aims to verify how the actual use of IT tools and especially AI can modify the competences of law practitioners. The outcome suggests that it would be difficult to keep deep knowledge of laws and comprehension of the facts to supervise AI.

KEYWORDS - telematic trial - law professionals - legal tech - legal databases
- human oversight

2/2023

EMANUELE ANDREIS*

L'informatica nelle professioni giuridiche e lo spazio dell'intelligenza umana**

SOMMARIO: 1. Introduzione – 2. I processi telematici – 3. Esempi di IA applicata al lavoro del giurista – 4. Dalle innovazioni più semplici alla difficoltà del controllo sull'IA.

1. Introduzione

Da tempo si discute dell'impatto, sempre apparentemente futuribile e quanto mai già concreto, delle tecnologie informatiche e in particolare dell'intelligenza artificiale (IA) su snodi cruciali del diritto sostanziale e processuale¹.

L'attenzione della maggior parte degli studiosi si concentra oggi sugli sviluppi possibili e sui relativi rischi e opportunità, eppure – prima ancora di riflettere sulle applicazioni tecnogiuridiche che si preannunciano come prossime – pare opportuno volgere lo sguardo sull'impatto già oggi riscontrabile di quei “prodotti della tecnica” a disposizione dei professionisti del diritto e il cui utilizzo è ormai diffuso.

* Assegnista di ricerca nell'Università di Parma, Progetto *Uni4Justice*, promosso dal Ministero della Giustizia e cofinanziato dall'Unione Europea, PON Governance e Capacità Istituzionale 2014-2020.

** Contributo sottoposto a valutazione anonima.

¹ Si vedano, tra gli altri, A. PAJNO – F. DONATI – A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Il Mulino, Bologna, 2022; R. GIORDANO – A. PANZAROLA – A. POLICE – S. PREZIOSI – M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè, Milano, 2022; T. CASADEI – S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche*, WKI, Milano, 2021; U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020; G. PASCUZZI, *Il diritto dell'era digitale*, Il Mulino, Bologna, 2020; S. FARO – T. E. FROSINI – G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Il Mulino, Bologna, 2020; A. D'ALOIA (a cura di), *Intelligenza artificiale e diritto*, Franco Angeli, Milano, 2020; CENTRO NAZIONALE DI PREVENZIONE E DIFESA SOCIALE, *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Giuffrè, Milano, 2020; A. SANTOSUOSSO, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, Milano, 2020; Y. MENECEUR, *L'intelligence artificielle en procès. Plaidoyer pour une réglementation internationale et européenne*, Bruxelles, 2020; A. GARAPON – J. LASSÈGUE, *Justice digitale*, Parigi, 2018; D. RUGGIU, *Human Rights and Emerging Technologies*, Pan Stanford Publishing, Singapore, 2017. Nonché i fascicoli monografici di alcune riviste: *Archivio penale*, n. 3/2013; *Rivista di filosofia del diritto*, n. 1/2019; n. 1/2020; ampia sezione di *Ars Interpretandi*, n. 1/2021.

La disamina di questi applicativi induce a pensare che si possa determinare un mutamento della figura dell'operatore del diritto, che riguarda non tanto aspetti esteriori, bensì competenze e conoscenze. I termini della questione non si riducono alla mera estensione delle competenze necessarie a maneggiare le apparecchiature tecnologiche: occorre verificare se tali strumenti – e l'agio che provocano – possano ridimensionare la stessa consapevolezza "giuridica" dei giuristi e, ancor più, la loro profondità culturale.

L'interrogativo, insomma, riguarda la possibilità di ricondurre ancora al canone tradizionale delle professioni giuridiche gli stessi avvocati e giudici umani estensivamente dotati di macchine per fare "tutto", pur muovendo dalla consapevolezza che tale "canone" è in evoluzione da tempo, o forse da sempre². Al fine di affrontare questo interrogativo, procederò con la disamina degli strumenti tecnologici che il giurista è ormai chiamato, anche dalle novità normative, a utilizzare, per poi passare a quelli che, pur senza essere obbligatori, sono a disposizione delle menzionate categorie professionali e possono avere un impatto sul loro statuto.

2. I processi telematici

L'evoluzione informatica da cui si deve partire è il processo telematico, che poi, in concreto, si declina in tante forme quante sono le nostre procedure: vi è la storica e consolidata – da oltre un decennio – versione civile³, la successiva estensione agli ambiti amministrativo⁴ e

² Cfr., rispettivamente su avvocatura e magistratura, F. GIANARIA – A. MITTONE, *L'avvocato del futuro*, Torino 2022, pp. 24 ss., pp. 10 ss., pp. 110 ss. e G. ZAGREBELSKY, *La giustizia come professione*, Einaudi, Torino, 2021, p. 10.

³ Dopo le notifiche telematiche (DD.LL. 112/2008 e 193/2009 e D.M. Giustizia 44/2011), il D.L. 179/2012 promosse una fase sperimentale di processo civile telematico (PCT), in alcune sedi, e la sua successiva graduale diffusione generale tra il 2014 e 2015. Cfr. E.M. FORMER, *Le procedure digitali*, Milano, 2022, pp. 5-6; G. FICHERA, *I dati normativi del PCT. Difficoltà di interpretazione di norme di rango diverso, necessità di sistemazione*, in A. CIRIELLO (a cura di), *Il processo telematico. Civile, penale, amministrativo, tributario, contabile*, Milano, 2019, p. 99.

⁴ L'art. 136 Cod. proc. amm. avviò l'informatizzazione del sistema, ma – come nel settore civile – affinché tale norma divenisse effettiva si è dovuto attendere la disciplina sublegislativa di attuazione: in questo caso, il D.P.C.M. 16 febbraio 2016, n. 40 in base al quale il nuovo modello è stato applicato a tutti i processi instaurati a partire dall'inizio del 2017 e poi, dal 2018, a tutti quelli pendenti (la disciplina ha poi subito modifiche con la

tributario⁵. Mentre l'avvio di tentativi di telematica nel processo penale è solo recente (prima per l'esigenza di operare durante la pandemia da Covid-19⁶ e nonostante le misure di distanziamento adottate in tale contesto, quindi in virtù della Riforma c.d. Cartabia⁷) e conserva significativi limiti. Il "processo penale telematico" (P.P.T.) infatti si ferma all'interlocuzione tra Uffici e difensori nel momento della conclusione delle indagini preliminari, consentendo l'acquisizione degli atti delle indagini (come il precedente TIAP⁸) e il deposito di atti e memorie indirizzati alla

normativa emergenziale in virtù, prima dell'abrogazione a opera dell'art. 4, co. 3, D.L. 28/2020, quindi dei Decreti del Presidente del Consiglio di Stato 22 maggio 2020, 28 dicembre 2020 e – infine – 28 luglio 2021): cfr. E.M. FORMER, op. cit., 6-7, pp. 382 ss.

⁵ Il quale è stato tra i primi coinvolti nell'informatizzazione ai sensi dell'art. 39, co. 8, D.L. 98/2011 (attuato con i Dd.M. Economia 23 dicembre 2013, n. 163, 4 agosto 2015 e – da ultimo – 6 novembre 2020), con una telematizzazione vera e propria dei processi dal 1° dicembre 2015, con un anno e mezzo di rodaggio su parte del territorio, raggiunto capillarmente solo dal luglio 2017 e del tutto obbligatorio a partire dal luglio 2019: cfr., ancora, E.M. FORMER, op. cit., pp. 7 e 409 ss.

⁶ Le stesse notifiche telematiche, previste per il settore penale dagli stessi decreti legge menzionati per il civile (D.L. 112/2008, art. 51, e D.L. 193/2009, art. 4, co. 3, lett. a), avevano riguardo a limitati casi e destinatari (non l'imputato) e l'attuazione è stata rinviata (L. 228/2012) sino alla fine del 2014: cfr. I. FEDELE, *Le notifiche telematiche penali in Cassazione*, in A. CIRIELLO (a cura di), *Il processo telematico*, cit., 163-7 e G. FICHERA, *I dati normativi*, cit., 115. Il deposito telematico, a lungo mera facoltà per gli Uffici giudiziari (art. 35 D.M. 44/2011), è stato autorizzato in maniera ubiquitaria (ma non sostitutiva del cartaceo) esclusivamente nel 2020, a causa della chiusura degli Uffici giudiziari a causa della pandemia. L'art. 24, co. 1, D.L. 137/2020 obbligò al passaggio tramite il portale del PPT (processo penale telematico) per una serie ristretta di atti del procedimento, poi estesa con D.M. 13 gennaio 2021, ma che rimane tuttora limitata a soli atti della fase delle indagini preliminari. Cfr. F. PORCU, *Il "portale del processo penale telematico": un passo in avanti (e qualche inciampo) verso la digitalizzazione*, in *Dir. pen. proc.*, 2021, fasc. 10, pp. 1399 ss. Per gli altri atti del processo penale, l'art. 24, co. 4 (e poi co. 6-bis ss.) D.L. 137/2020 ha ammesso solo una facoltà di deposito tramite posta elettronica certificata esclusivamente agli indirizzi attivati e indicati dal Direttore Generale Sistemi Informativi Automatizzati (DGSIA) del Ministero della Giustizia.

⁷ Vd., tra gli altri, artt. 5-6, D. Lgs. 10 ottobre 2022, n. 150. Sulla riforma cfr. L. GIORDANO, *L'istituzione del processo penale telematico*, in A. BASSI – C. PARODI (a cura di), *La riforma del sistema penale*, Milano, 2022, 19 ss. e, prima del decreto delegato, P. TONINI, *Le nuove tecnologie e la riforma Cartabia*, in *Dir. pen. proc.*, 2022, fasc. 3, pp. 293 ss.

⁸ Trattamento Informatico Atti Penali: quest'ultimo applicativo era stato istituito dalla circolare DGSIA 26 gennaio 2016 come gestore unico nazionale in grado di *seguire* il materiale acquisito anche nelle fasi *processuali*, consentendo «l'interfaccia tra il SICP [sistema informativo della cognizione penale, consultabile solo dagli Uffici Giudiziari] e l'utente finale»: cfr. E. FORMER, op. cit., p. 259. Scansione e inserimento degli atti di indagine sulla piattaforma erano stati però ostacolati dalle carenze organiche delle Procure che si rivelavano in estremo ritardo nella digitalizzazione dei documenti cartacei.

Procura, senza che la piattaforma sia destinata, allo stato attuale, a ospitare le interlocuzioni (di PM e difese) con lo stesso Ufficio giudiziario preposto a questa fase, il G.I.P., neppure per gli (eventuali) momenti processuali delle indagini preliminari (incidenti probatori, udienze per l'archiviazione o la proroga delle indagini)⁹. Addirittura sono estranei alla telematica gli stessi atti di indagine se curati dalle Procure presso i Tribunali per i Minori.

Al di fuori dell'interfaccia del processo penale telematico, sono state dematerializzate molte comunicazioni tra Uffici giudiziari e parti: sia le notifiche da parte degli Uffici, sia i depositi, inizialmente facoltativi, tramite posta elettronica certificata¹⁰, sia la trasmissione garantita da molti Uffici anche tramite posta elettronica ordinaria degli atti con originali digitali (per esempio i verbali stenotipati delle udienze).

Il sistema resta molto frammentato¹¹, anche nello stesso processo civile, in cui la telematizzazione è consolidata: solo la recente riforma Cartabia ha superato le resistenze dei giudici di Cassazione e innanzi al Giudice di Pace, oltre che per il settore della Volontaria Giurisdizione¹²; ma per questi ultimi (GdP e VG), siccome le parti possano stare in giudizio personalmente, la telematica non sarà obbligatoria¹³.

⁹ Cfr. L. GIORDANO, op. cit., pp. 19 ss.

¹⁰ Art. 24 D.L. 137/2020 (vd. nota 6). La facoltà all'epoca prevista è stata superata e resa obbligatoria ai sensi dell'art. 6, co. 1, lett. c, del D.Lgs. 151/2022.

¹¹ Sono molti i sistemi informativi adottati nei diversi settori dell'amministrazione della giustizia e per lo più non sono comunicanti e integrati fra loro: cfr. E. FORMER, op. cit., 226 ss. Per dettagli sulle criticità del portale penalistico, cfr., tra gli altri, F. PORCU, op. cit., 1405-8 e P. TONINI, *Le nuove tecnologie*, cit., 294, 296-7. In un recente studio a oggi inedito sono stati contati almeno trenta sistemi in ambito penale (M. PALMIRANI – A. TONIOLO, *Glossario Sistemi Informativi della Giustizia*, 2022, p. 30).

¹² Art. 196-*quater* Disp. Att. Cod. proc. civ. (introdotto dal D.Lgs. 149/2022). I depositi telematici in Cassazione erano stati ammessi, come facoltà, dall'art. 83, co. 11-*bis*, D.L. 17 marzo 2020, n. 18 (conv. in L. 24 aprile 2020, n. 27 e poi confermato dalla successiva normativa emergenziale e successivo provvedimento DGSIA del 27 gennaio 2021). Cfr. A. PANZAROLA, *Il processo civile e la rivoluzione tecnologica all'alba dell'era dell'Intelligenza Artificiale (considerazioni generali)*, in *Il diritto nell'era digitale*, cit., 800-1. Inoltre, si consideri come M. PALMIRANI – A. TONIOLO, op. cit., p. 10, continuo anche per il settore civile oltre venti diversi sistemi informativi, malgrado in questo ambito siano maggiori le occasioni di automazione e interoperabilità (stimolate e propiziate, a ben vedere, dal decennio di processo civile telematico).

¹³ Circostanza che già veniva denunciata da numerose relazioni annuali degli Uffici giudiziari come giustificativa della difficoltà di integrazione: i cittadini, nel partecipare personalmente alle menzionate procedure, oltre a non aver dimestichezza con il diritto, spesso non ne hanno con l'informatica e men che meno con la procedimentalizzazione informatica delle attività.

Minimo comun denominatore, tra le svariate procedure informatizzate, la possibilità (quando non l'obbligo) per i professionisti – magistrato o avvocato – di accedere ai fascicoli digitali e depositare telematicamente almeno alcuni atti¹⁴.

Una prima riflessione muove dal ruolo di questi adempimenti, presupposto per la fruizione di un diritto fondamentale quale l'accesso alla giustizia (e, correlativamente, per l'esercizio da un lato della giurisdizione e dall'altro dell'assistenza in giudizio): per il loro compimento è indispensabile - sia in seno all'Ufficio giudiziario, sia per il professionista - il ricorso a strumenti quali computer, collegamenti di rete, applicativi, identità digitali e servizi di posta elettronica certificata¹⁵: cioè tecnologie "abilitanti" fornite esclusivamente da operatori privati.

In secondo luogo, il processo telematico, pur con le diverse velocità evidenziate, contribuisce alla segmentazione tra i professionisti. Si sono notevolmente ridotte le occasioni di incontro tra magistrati e avvocati, ancor più tra avvocati e cancellieri, ma anche tra esponenti della medesima categoria se coinvolti in tipologie di attività diverse. Una declinazione dell'iperspecializzazione delle professioni tipica nel nostro tempo, ma anche dell'isolamento e dell'individualismo indotti e progressivamente enfatizzati dalla digitalizzazione degli scambi e delle interazioni¹⁶.

3. Esempi di IA applicata al lavoro del giurista

¹⁴ Singolarmente, nell'amministrativo, l'accesso non è tutelato da un'identità digitale rigidamente verificata (firme digitali e SPID), ma basta la PEC: cfr. E. FORMER, op. cit., 385.

¹⁵ Le definizioni normative di questi concetti si rinvencono nell'art. 1, co. 1, del CAD: «(lett. s) firma digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici; ... (lett. u-quater) identità digitale: la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale; ... (lett. v-bis) posta elettronica certificata: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi». Sulle medesime, cfr., per esempio, F. FAINI, *E-Government and Open Government Initiatives*, in G. ZICCARDI (a cura di), *Cyber Law in Italy*, Wolters Kluwer International Law, UK, 2020, 96 s.; F. MURINO, *Dalla firma elettronica agli smart contract*, in T. CASADEI – S. PIETROPAOLI (a cura di), op. cit., 74 ss.

¹⁶ In proposito, a livello generale, tra gli altri A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in ID. (a cura di), *Intelligenza artificiale e diritto*, cit., 51.

Oltre alla strumentazione necessaria per adempiere ai processi telematici, a disposizione dei professionisti vi sono ormai anche ulteriori *software*, che possono agevolare determinate attività con l'impiego – anche – dell'intelligenza artificiale, pur non sostitutiva della funzione umana coinvolta. Anzitutto, ricordo tre applicativi esaminati in un recente studio di Della Morte¹⁷:

- *Watson Debater* individua le argomentazioni maggiormente usate con riferimento a un determinato argomento;
- *Ross Intelligence* suggerisce correlazioni tra argomentazioni giuridiche e percentuali di successo in giudizio;
- *Alibi software* propone argomenti difensivi appositamente riferiti a specifiche accuse.

Esistono inoltre strumenti che possono «automatizzare la ricerca in campo legale, [...] la redazione o il controllo di contratti o documenti, [...] valutazioni tecniche (ad esempio per il calcolo di indennità [...] di assegni di mantenimento, [...] dei danni [...]) e anche determinare il possibile esito di una controversia, attuale o potenziale», come ricordato da Donati¹⁸, il quale cita il *software Luminance* in uso negli studi legali anglosassoni per le *due diligence* in ambito di "M&A"¹⁹; nonché l'algoritmo sviluppato nel 2016 presso l'*University college of London* per predire l'esito di controversie *CEDU* con un'attendibilità prossima all'80%²⁰.

Come si vede, il fenomeno è molto ampio e si possono ancora considerare ulteriori sistemi intelligenti a disposizione dei professionisti:

- a) gli strumenti di *e-discovery*, che agevolano la ricerca di elementi rilevanti nell'ambito di reperti probatori informatici, in un fascicolo processuale o nella documentazione di una pratica²¹. Al riguardo,

¹⁷ ID., *Judgements without Judges. The Algorithm's Rule of Law*, in A. MARCHETTI – G. RIVA (a cura di), *Humane Robotics: A Multidisciplinary Approach Towards the Development of Humane-Centered Technologies*, Milano, 2022, p. 387.

¹⁸ ID., *Intelligenza artificiale e giustizia*, in A. D'ALOIA (a cura di), op. cit., p. 181.

¹⁹ *Ibid.*, nt. 6.

²⁰ *Ivi*, p. 197.

²¹ Su questi applicativi, cfr.: F. SANTAGADA, *Intelligenza artificiale e processo civile*, in *Il diritto nell'era digitale*, cit., pp. 827 ss. Per un'esemplificazione, inoltre si veda il sito: <https://www.clio.com/blog/lawyer-ai/>. La pratica dell'*e-discovery* è ormai un dato acquisito, anzi si ritiene che consenta di eseguire indagini informatiche più mirate e l'estrazione di copie forensi meno invasive, in ossequio anche ad alcune pronunce della Suprema Corte (si possono citare Cass. pen., sez. un., 20 luglio 2017, n. 40963, in *Ced Cass.*, rv. 270497, e, come recente esempio di un filone piuttosto consolidato ma non privo di antagonisti, Cass. pen., sez. 6, 28 settembre 2021, n. 38460). In argomento, cfr.: M. FERRAZZANO – L. SUMMA,

2/2023

non manca chi azzarda un'ipotesi di negligenza professionale per l'avvocato il quale non abbia garantito la miglior tutela del proprio assistito trascurando un documento che avrebbe potuto individuare se si fosse dotato di tutti gli strumenti utili e disponibili²²;

- b) le banche dati più innovative, che dopo l'implementazione della ricerca semantica parrebbero in grado di restituire i risultati giuridici rispondendo a quesiti formulati in linguaggio naturale e non attraverso l'introduzione di "parole chiave"²³;
- c) applicativi descritti come capaci di sviluppare ricerche giurisprudenziali automaticamente, riconoscendo i dettagli del caso e proponendo esiti immediatamente fruibili e allegabili²⁴;
- d) sistemi di IA capaci di analizzare bozze di atti giudiziari (o pareri) al fine di individuare ulteriori spunti di approfondimento o di segnalare i precedenti giurisprudenziali coerenti con il caso, ma non citati, o quelli riportati sebbene superati, anche solo "indirettamente"²⁵ (è evidente l'utilità di strumenti di questo tipo negli ordinamenti di *common law*: non a caso, è in quel contesto che si è iniziato a svilupparli; d'altro canto la direzione che ha assunto il nostro diritto vivente, con la crescente importanza della

La selezione dei dati informatici in ambito giudiziario, in AA.VV., *Nuove questioni di informatica forense*, a cura di A. Brighi, Bologna, 2022, 76-7.

²² Ipotesi rinvenibile non solo su siti commerciali (<https://www.clio.com/blog/need-to-know-ediscovery/>), ma anche in pubblicazioni di settore (<https://www.americanbar.org/news/abanews/publications/youraba/2017/september-2017/7-ways-artificial-intelligence-can-benefit-your-law-firm/>). Con una formulazione ragionevolmente più cauta è stato affermato – per la diligenza contrattuale e per mantenere competitività – un onere di «costante aggiornamento e assunzione di competenze basilari riguardanti gli strumenti tecnologici a disposizione» (G.A. PARINI, *Utilizzo dell'intelligenza artificiale in sostituzione o a supporto dell'avvocato: prospettive future e dovere di competenza tecnologica*, in *Teoria e critica della regolazione sociale*, 2021, fasc. 2, p. 161, p. 168).

²³ <https://www.lisia.it/>. Con riferimento alla ricerca semantica, M. STEPKA, *Law Bots: How AI is reshaping the legal profession*, 21 febbraio 2022, in *businesslawtoday.org*: «The keyword or boolean search approach that was the hallmark of the service for decades has been augmented by semantic search. This means the machine learning algorithms are trying to understand the meaning of the words, not just match them to keywords».

²⁴ Sempre esaminando il più "avanzato" scenario nordamericano, *Casetext* e *Fastcase*. Cfr. <https://www.clio.com/blog/lawyer-ai/>

²⁵ Sistema denominato *Quick Check*: cfr. M. STEPKA, op. cit.; in tema, si veda anche G. RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen.*, 2019, fasc. 3-web, 1.

giurisprudenza e dei relativi precedenti²⁶, renderebbe molto utile questa funzione anche nel nostro ordinamento²⁷;

- e) strumenti volti a soppiantare l'esperienza diretta acquisita dai professionisti, che si prefiggono di fornire dettagli sui giudici (sulla loro storia e sulle loro decisioni), come sugli avvocati (e le relative percentuali di successo nelle diverse iniziative assunte) in relazione agli argomenti dei giudizi, al fine di prevederne i possibili esiti²⁸;
- f) applicativi che automatizzerebbero tutta la consulenza legale, interiorizzando nell'algoritmo i diversi percorsi argomentativi e le nozioni giuridiche, per poi assemblarle e fornire la risposta di fronte alle richieste di assistenza ²⁹ (espressamente, lascerebbero telefono o email per rispondere all'esigenza di "contatto umano", o forse di personalizzazione: insomma, un *call center* – con rispetto parlando – dotato di sofisticata *legal tech*)³⁰.

²⁶ Per effetto di queste dinamiche, muta lo stesso concetto di "legalità" e il suo ruolo viene in parte attribuito a quello – diverso – di "prevedibilità": cfr., tra gli altri, G. GORLA, *Precedente giudiziale*, in *Enc. giur. Treccani*, vol. XXIII, Roma, 1990; N. IRTI, *Un diritto incalcolabile*, in *Riv. dir. civ.*, 2015, pp. 11 ss.; C.E. PALIERO – S. MOCCIA – G. DE FRANCESCO – G. INSOLERA – M. PELISSERO – R. RAMPIONI – L. RISICATO (a cura di), *La crisi della legalità. Il «sistema vivente» delle fonti penali*, ESI, Napoli, 2016; A. CADOPPI, voce *Giurisprudenza e diritto penale*, in *Dig. disc. pen.*, Agg. 2017, pp. 411 ss.; L. EUSEBI, *L'insostenibile leggerezza del testo: la responsabilità perduta della progettazione politico-criminale*, in *Riv. it. dir. proc. pen.*, 2016, pp. 1668 ss.; L. FERRAJOLI, *Contro il creazionismo giurisprudenziale. Una proposta di revisione dell'approccio ermeneutico alla legalità penale*, in *Ars interpr.*, 2016, fasc. 1, pp. 23 ss.; R. PALAVERA, *Il penalista e il suo partito*, Pisa, 2018, pp. 32 ss.; M. TARUFFO, *Verso la decisione giusta*, Torino, 2020, pp. 422 ss.

²⁷ Proprio sulla relazione tra l'impiego della tecnologia e il rilievo attribuito ai precedenti, cfr., di recente R. GIORDANO, *Il precedente nell'era digitale*, in ID. – A. PANZAROLA – A. POLICE – S. PREZIOSI – M. PROTO (a cura di), op. cit., pp. 1021 ss.; A. PAJNO, *Intelligenza artificiale e autonomia del giudice. Il ruolo del fatto e il valore del precedente*, in ID. – F. DONATI – A. PERRUCCI (a cura di), op. cit., Vol. II, *Amministrazione, responsabilità, giurisdizione*, Bologna, 2022, pp. 394 ss.

²⁸ Così descrive *Lex Machina* M. STEPKA, op. cit.; riflessioni in proposito anche in A. D'ALOIA, *Il diritto verso "il mondo nuovo"*, cit., p. 43.

²⁹ Per esempio, *VisiRule*, presentato nel relativo sito: https://www.visirule.co.uk/visirule-for-law-firms?gclid=EAIaIQobChMI0aLL1Ozm-AIV8f3VCh3hnAQ1EAAYASAAEgJHd_fD_BwE

³⁰ Sulle ipotesi di «sostituzione in toto» del professionista si sofferma G. A. PARINI, op. cit., p. 169, la quale esamina anche la proliferazione di applicativi utili ad agevolarne le incombenze *non giuridiche* (la gestione dello studio e del personale, la fatturazione). Quanto alla "sostituzione", l'Autrice sottolinea come le previsioni di legge riservano determinate attività agli iscritti agli albi e dunque impediscono il conferimento di incarichi alle

In questo vasto campionario di tecnologie capaci di agevolare o sostituire alcune delle attività dei professionisti del diritto (elenco precario, sempre aperto, in ragione della rapidità dell'evoluzione tecnologica) rientrano anche gli applicativi di IA che assistono i giudici nella definizione delle pene da comminare (e, in particolare, del rischio di recidiva): molto noto negli anni scorsi il *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS)³¹, che peraltro non è l'unico esempio di tale funzione³².

4. Dalle innovazioni più semplici alla difficoltà del controllo sull'IA

Si è visto come il processo telematico contribuisca a isolare gli operatori del diritto, i quali, anche in virtù delle straordinarie banche dati e dell'agio con cui le possono consultare, possono divenire molto colti: sono maggiori le letture raggiungibili e – salvo la distrazione causata dalla persistente reperibilità garantita dai moderni sistemi di telecomunicazione – è maggiore il tempo a disposizione, recuperato grazie agli applicativi che subentrano nelle “altre” attività. C'è però il rischio che gli stessi giuristi perdano l'interesse per tali letture, se possono lasciare che sia l'IA a consultarle ed estrarne le citazioni utili. Quand'anche scegliessero di documentarsi, quell'isolamento già segnalato rischierebbe di rendere quella cultura alquanto autoreferenziale, priva di un solido e diretto contatto con

macchine. Proprio queste discipline hanno impedito all'applicazione (dal nome evocativo) *DoNotPay* di intervenire quale difensore in giudizio: cfr. l'aggiornamento del 27 gennaio 2023 in M. FOTI, *Avvocati vs Intelligenza Artificiale (IA): il primo avvocato robot al mondo*, in *Altalex*, 25 gennaio 2023, e T. ROSELLI, *Dalla difesa al banco degli imputati: l'avvocato robot già finisce nei guai*, in *Il Dubbio*, 15 marzo 2023, entrambi reperibili sui relativi siti.

³¹ La notorietà deriva dal *leading case* “*Loomis*” (Wisconsin Supreme Court – *State vs. Loomis*, case 2015AP157-CR, *Judgement July 13th 2016*, in *Harvard Law Review*, 130-2017, pp. 1530 ss.), cognome dell'imputato che sollevò eccezioni nei confronti dell'uso di COMPAS nel giudizio come supporto nella determinazione della durata della pena, sulla base – tra l'altro – delle previsioni di recidiva, rispetto alle quali si è scoperto che l'algoritmo non era stato sterilizzato da dati che esprimevano schemi discriminatori: cfr., oltre alla pronuncia, tra gli altri, F. DONATI, op. cit., pp. 186 ss.; L. D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena*, in *Dir. pen. cont. – trim.*, 2019, fasc. 2, pp. 362 ss.; J. NIEVA FENOLL, *Intelligenza artificiale e processo*, Torino, 2019, 59; L. MALDONADO, *Risk and need assessment tools e riforma del sistema sanzionatorio*, in G. DI PAOLO – L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Trento, 2022, pp. 151 ss. (<https://iris.unitn.it/handle/11572/361122>).

³² In proposito, cfr. ancora L. MALDONADO, op. cit., pp. 153 ss.

la realtà, con le esigenze e le sensibilità dei propri interlocutori (sempre più occasionali).

Ciascuna delle applicazioni esaminate, senza arrivare a quelle sostitutive *tout court*, può contribuire a questo percorso di straniamento del professionista. Certo, le diverse applicazioni di intelligenza artificiale meritano un giudizio modulato esaminando la singola innovazione, anche in considerazione del soggetto che la intenda usare e del contesto di impiego. Ciononostante, ai fini del presente lavoro ritengo di poter trarre, a partire dall'attenzione dedicata ai sistemi meno complessi (ricerche in banche dati giuridiche e documentali), alcune riflessioni che ipotizzo possano valere anche per le ulteriori innovazioni.

È pacifico che nel lessico giuridico l'affinità terminologica non comporta l'equivalenza dei relativi concetti. Pertanto, un ricorso indiscriminato e poco sorvegliato a strumenti di ricerca automatizzata rischia di determinare confusioni, o quantomeno esiti inadeguati di ricerca. In secondo luogo, vi è la possibilità che i criteri adottati dall'IA a bordo della banca dati non siano pertinenti rispetto alla ricerca da svolgere (talvolta documenti disponibili non emergono, talaltra risultano repertoriati solo da alcune banche dati): finora molte indagini si sono preoccupate dei pregiudizi dell'IA, in quanto elemento con vistose conseguenze contraddittorie per il nostro ordinamento. Ciò non significa che la progettazione dell'algoritmo non possa avere altri *bias* e altri errori. Specialmente se si considera come le competenze per realizzarlo siano precipuamente matematico-informatiche, campi che – al di là dell'esercizio della logica, comune ai giuristi – restano distanti dalla formazione giuridica e dalla stessa consapevolezza dei principi e della sistematica dell'ordinamento. Inoltre, ancora con riguardo al funzionamento degli applicativi, occorre ricordare che il meccanismo algoritmico è fondato su ricorrenze ripetute tali da indurre "l'approvazione" di un risultato³³: il discernimento giuridico, viceversa, si muove (o quantomeno può muoversi) su piani diversi, paralleli, sia tramite l'analogia, sia tramite l'interpretazione sistematica e l'applicazione di principi provenienti da istituti e ambiti diversificati³⁴.

³³ Su questi meccanismi, tra i tanti: D. AMOROSO – G. TAMBURRINI, *La questione del controllo umano significativo sui sistemi robotici ad autonomia crescente*, in A. D'ALOIA (a cura di), op. cit., pp. 89 ss.

³⁴ Sulla diversità dei metodi, si veda l'approfondito studio di P. MORO, *Intelligenza artificiale e professioni legali. La questione del metodo*, in *Journal of Ethics and Legal Technologies*, 2019, vol. 1, pp. 28 ss.

2/2023

Peraltro, l'elaborazione artificiale di dati giudiziari (evidentemente personali e spesso sensibili) determina la forte perplessità derivante dalla natura privata dei *software* (salvo che ne siano sviluppati di libera accessibilità, magari in seno a centri di ricerca universitari o a qualche agenzia pubblica), con l'ennesima sovrapposizione tra Stato e mercato³⁵ e rischi inerenti alla sicurezza dei dati (aggredire fisicamente un Ufficio giudiziario – ma anche uno studio legale –, accedere alle carte ivi conservate e riuscire a movimentarle è cosa ben diversa da raggiungere le infrastrutture informatiche e penetrare in archivi potenzialmente illimitati). Certamente, è anche per affrontare questi rischi che l'ordinamento ha predisposto le discipline in materia di tutela della riservatezza dei dati e della sicurezza cibernetica, questo però non significa che i pericoli siano per ciò solo esclusi (né ridotti³⁶) e che pertanto possano essere dimenticati.

D'altronde, passando così all'impatto sul professionista che impiega gli applicativi esaminati, ricorrere a "ricerca semantica" e formulazioni dei quesiti "in linguaggio comune" riduce l'esercizio di focalizzazione del problema e del proprio pensiero, dal momento che le scienze educative insegnano che, per ciò, è essenziale saperlo formulare³⁷. Da quest'ultima considerazione ne discende un'altra: malgrado il giurista possa beneficiare di tutti questi dispositivi, considerato che potrà concentrare le proprie energie nelle attività di maggiore creatività e sforzo intellettuale (o in quelle di relazione), pare allo stesso tempo non inverosimile che *in ciascuna* di esse si ritroverà in qualche modo privato della maggior consapevolezza che avrebbe acquisito proprio continuando a dedicarsi in prima persona alle diverse incombenze, incluse quelle secondarie e meno stimolanti.

Tramite lo studio e la selezione di documenti si riesce a tenere traccia di eventuali materiali estranei all'oggetto della ricerca, ma che – anche solo per qualche aspetto inizialmente ignorato nell'impostazione dell'analisi – possono acquisire rilievo successivamente o ri-orientare la stessa attività di selezione. Inoltre, se si tratta di documenti giuridici, la loro consultazione offre un arricchimento su discipline e tecniche espositive diverse da quelle quotidianamente frequentate. Si tratta di competenze determinanti in una

³⁵ Così S. AMATO, op. cit., 148. Lo stesso Autore (ivi, 147), tuttavia, rammenta un software statale (nel caso, atto a contrastare frodi commerciali) oggetto di censure da parte della magistratura olandese per violazione della riservatezza dei cittadini.

³⁶ La ricorrenza di c.d. *data breach* e *cyber attack* aumenta ogni anno: cfr., per esempio, M. DE NICOLA, *Difendere e creare valore con la cybersecurity*, in *Controllo di gestione*, 2023, fasc. 1, 39.

³⁷ Sull'impatto dei prodotti della tecnica sulla formazione ha riflettuto, com'è noto, già M. HEIDEGGER; cfr. sul punto P. MALAVASI, *Educare robot? Pedagogia dell'intelligenza artificiale*, Vita e pensiero, Milano, 2019, p. 47.

materia che vive di collegamenti intertestuali e competenze interdisciplinari. Certo, perde queste opportunità anche il professionista il quale si avvalga, invece che di tecnologie, di collaboratori meno esperti per lo svolgimento di tali attività: anch'essi potrebbero non individuare alcuni elementi considerati marginali per inesperienza ma in realtà rilevanti, anch'essi potrebbero non trasmettere a chi li ha incaricati nulla di più delle informazioni richieste, così come potrebbero omettere di tener conto delle eventuali informazioni e consapevolezze circa discipline e argomenti reperiti (o reperibili) tra le pieghe della documentazione. Lo stesso vale per la consultazione della giurisprudenza e della dottrina, attività dispendiosa in termini di tempo, quanto arricchente per la miniera di nozioni spesso ben più estese di quelle originariamente oggetto di ricerca. Nel rivolgersi all'IA in modo pervasivo, però, oltre a perdere opportunità di conoscenza (e risparmiare tempo), rischiano di affidarsi ciecamente al supporto: questo è invero un esito diffuso nel ricorso alla tecnologia in quanto si traspone sulla medesima la moderna fiducia in scienza e tecnica³⁸, dimenticando che l'informatica non è una scienza pura, bensì un campo di probabilità (implicante una mera tensione verso il limite della certezza)³⁹.

Questa circostanza non è secondaria. Infatti, sebbene oggi si insista da più parti sulla necessità di un *controllo umano* sull'IA⁴⁰, tale controllo - oltre

³⁸ Cfr., tra gli altri, G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in CNDPS, op. cit., p. 12; L. LUPARIA DONATI, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, ivi, 116; S. MASON, *The presumption that computers are "reliable"*, in ID. – D. SENG (a cura di), *Electronic evidence and Electronic Signatures*, Londra, 2021, 127 ss. (nell'ordinamento inglese vige la presunzione legale relativa di affidabilità degli strumenti elettronici).

³⁹ U.E. MOSCATO, *Calculemus? Da Leibniz all'intelligenza artificiale*, in CNDPS, op. cit., pp. 27 ss. Segnala quanto sia inappropriato attribuire una fiducia esasperata all'informatica, con riferimento agli esiti di prove informatiche, R. BRIGHI, *Informatica forense, algoritmi e garanzie processuali*, in *Ars Interpretandi*, 2021, 1, p. 154: «Le sorgenti digitali possono contenere informazioni parziali, incomplete o ambigue rispetto all'ambiente che, solo combinate con altri dati, diventano elementi di prova in dibattimento».

⁴⁰ Così, oltre a UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, Parigi, 2021, §§ 35-6 (reperibile sul relativo sito), gli interventi dell'Unione Europea riepilogati da M. ZANICHELLI, *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in A. D'ALOIA (a cura di), op. cit., Milano, 2020, pp. 67 ss. Sul tema, cfr. ancora EAD., *L'intelligenza artificiale e la persona: tra dilemmi etici e necessità di regolazione giuridica*, in *Teoria e Critica della Regolazione Sociale*, 2021, fasc. 1, 149, 152; D. AMOROSO – G. TAMBURRINI, op. cit., pp. 89 ss.; G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in CNDPS, op. cit., pp. 22 ss.; G. ZACCARIA, *Mutazioni del diritto: innovazione tecnologica e applicazioni predittive*, in *Ars interpretandi*, 2021, fasc. 1, p.

2/2023

a non essere spesso esercitato - rischia di perdere consistenza a fronte sia delle qualità perdute o non acquisite dai giuristi⁴¹, sia della dimensione dei dati: per esaminare un fatto, per difendere e per giudicare potrà esser indispensabile maneggiare quantità di dati sempre più ingenti, il cui governo in assenza di supporto sarà pressoché impossibile⁴². Il conseguentemente necessario aiuto algoritmico, però, non potrà essere più di tanto controllato *umanamente*: se l'elaborazione algoritmica fosse appunto così necessaria, una verifica a posteriori del suo funzionamento riproporrebbe il medesimo problema dello sforzo *sovraumano* di gestione della mole di dati.

Come ho anticipato, le riflessioni proposte prendono le mosse dal ricorso a banche dati (specie se evolute) e ad applicativi di *e-discovery*, a cui ritengo di poter attribuire un ruolo emblematico di quanto può derivare dalla diffusione delle ulteriori tecnologie. Da un lato, la combinazione di svariati applicativi, a partire dalla telematizzazione del processo, enfatizza gli effetti di alienazione del professionista. Dall'altro, se la disomogeneità tra informatica e diritto nei metodi e nelle impostazioni non limita la fiducia in strumenti così "semplici", non è irragionevole ipotizzare un ancora maggiore affidamento in sistemi più evoluti. Si pensi a quelli menzionati, in grado di redigere contratti, introdurre autonomamente i precedenti rilevanti negli atti o di individuare gli argomenti più efficaci nel caso specifico: è evidente che il giurista, man mano che vi si affida, perde dimestichezza e consapevolezza, mentre – parimenti – sarà tentato di affidarsi, per le ragioni già esposte. Eppure, è proprio rispetto all'IA più "forte", con maggiori, più decisive, funzioni, che è necessario il controllo dell'uomo.

Di fronte al rischio che il controllo *ex post* diventi irrealizzabile, diventa essenziale governare *umanamente* – con consapevolezza giuridica – *ex ante*

30. Anche la giurisprudenza rimarca la necessità di un'ultima parola del decisore umano (si vedano le pronunce statunitensi sul caso *Loomis*, di cui *supra*, e quelle del "nostro" TAR del Lazio, sez. III-bis, nn. 9224/2018, 6606/2019, 10964/2019).

⁴¹ Cfr. F. GIANARIA – A. MITTONE, op. cit., p. 69 e A. PUNZI, *Difettività e giustizia aumentata. L'esperienza giuridica e la sfida dell'umanesimo digitale*, in *Ars Interpretandi*, 2021, fasc. 1, p. 115.

⁴² I fascicoli, negli anni, sono divenuti sempre più estesi, in particolare grazie a quanto in essi riversato dalla tecnologia. Sulla complessità generata dall'estensione dei dati disponibili, cfr. S. AMATO, op. cit., p. 138: «più crescono i dati e più il sistema diviene complesso; più il sistema diviene complesso e più la gestione del sistema si complessifica; più si complessifica la gestione del sistema e più l'intelligenza artificiale tende a divenire generale... a passare dalla singola applicazione che reagisce ai nostri impulsi a una ridefinizione complessiva che si sviluppa attraverso e oltre i nostri impulsi».

la programmazione, la manutenzione e l'aggiornamento delle tecnologie algoritmiche. Parimenti, proprio nella temperie digitale, i giuristi sono chiamati a conservare e curare la propria consapevolezza culturale.



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

FLOR MARÍA ÁVILA HERNÁNDEZ

La justicia digital y la desigualdad latinoamericana

ABSTRACT - The Covid-19 pandemic has accelerated the process of incorporating digital technologies into many aspects of daily life. One of those aspects was digital justice, the use of ICTs within judicial bodies. Many countries in the region have created virtual systems for the publication of public files, electronic notifications, hearings through videoconferences, among others. However, Latin America is seriously affected by the problem of inequality, being the most unequal region in the world. In this sense, it is necessary that public policies related to ICTs recognize this problem and are configured to have a truly universal scope. Digital justice can bring the courts closer to rural or remote sectors, but first it is necessary to address the problem of inequality in access to technology.

KEYWORDS - Technology - digital justice - inequality - ICTs

FLOR MARÍA ÁVILA HERNÁNDEZ*

La justicia digital y la desigualdad latinoamericana**

SOMMARIO: 1. *Introducción* – 2. *Las tecnologías digitales en el ámbito jurídico en Latinoamérica* – 3. *Desigualdad y derechos emergentes* – 4. *Conclusión*

1. Introducción

La llegada de la pandemia del Covid-19 provocó cambios drásticos a nivel global en nuestra forma de convivir, trabajar, adquirir bienes y servicios, comunicarnos, entre otros aspectos. Las tecnologías digitales cumplieron un rol central en este proceso, convirtiéndose en herramientas indispensables para la vida cotidiana. No obstante, las desigualdades sociales estructurales existentes en Latinoamérica afectan el acceso y uso de estas tecnologías por diversos sectores de la población, quienes en muchos casos se han visto impedidos de acudir a estas, en un momento donde su uso es fundamental.

Esta situación conlleva el riesgo de que la brecha digital se convierta en el principal determinante de la desigualdad en la región durante los próximos años. En consecuencia la importancia de incrementar el acceso a las nuevas tecnologías se ha convertido en un tema de importancia estratégica para el futuro de la región, lo que puede observarse tanto en la literatura como en los comunicados de organizaciones internacionales como la CEPAL¹.

Las tecnologías virtuales han transformado los sistemas económicos, la forma de hacer negocios, los modelos productivos, los hábitos de consumo y los patrones de desarrollo de Latinoamérica y el mundo. La desigualdad en el acceso a la tecnología supone dejar a sectores vulnerables al margen de estos nuevos sistemas económicos, lo que sólo aumenta su alienación y transmite el problema a las futuras generaciones.

Según datos de la CEPAL, existen en Latinoamérica más de 40 millones

* Professoressa di Teoria dello Stato, Teoria dei diritti umani e Metodologia giuridica presso l'Università Cattolica di Colombia, Bogotá.

** Contributo sottoposto a valutazione anonima.

¹ CEPAL. Es urgente universalizar el acceso a las nuevas tecnologías para reconstruir mejor con igualdad y sostenibilidad: CEPAL, <https://www.cepal.org/es/noticias/es-urgente-universalizar-acceso-nuevas-tecnologias-reconstruir-mejor-igualdad#:~:text=Existe%20el%20riesgo%20de%20que,y%20el%20Caribe%20> (CEPAL).

de hogares que no cuentan con conexión a internet, de los cuales la mitad se ubica en los dos quintiles más pobres de la sociedad. Igualmente casi la mitad de los niños entre las edades de 5 y 12 años no cuentan con acceso a internet y durante la pandemia se calcula que más de 32 millones de niños no pudieron acceder a la educación virtual.

Por otro lado, las desigualdades estructurales que históricamente han afectado a la región han tenido como consecuencia que millones de personas dependan de la economía informal, de esquemas de producción poco diversificados y en base a modelos poco eficientes, además de contar con limitadas oportunidades para adquirir nuevas habilidades que puedan mejorar sus opciones laborales. Estos factores contribuyen a la brecha digital y disminuyen el impacto que la revolución digital pueda tener en sus vidas.

Pese a que la pandemia sirve como el principal punto de referencia para el uso de las tecnologías digitales, desde hace un par de décadas los gobiernos de la región reconocieron el potencial de estas tecnologías en diversos ámbitos, más allá de la economía y la educación. El derecho y la administración de justicia son sectores de vital importancia para cualquier Estado. No sorprende entonces que los gobiernos hayan incorporado paulatinamente las tecnologías digitales en los ámbitos jurídicos, ya sea con fines netamente administrativos (transformación de archivos físicos en archivos digitales a los que los usuarios pueden acceder de forma remota, así como bases de datos interactivas sobre ley y jurisprudencia) o con fines decididamente más ambiciosos (audiencias virtuales, por dar un ejemplo).

Sin embargo, estos desarrollos tecnológicos en el ámbito del derecho enfrentan los mismos problemas del uso de la tecnología en otros ámbitos, específicamente la falta de acceso por parte de millones de personas. En la presente investigación se repasarán algunas de las principales iniciativas gubernamentales que mezclan el derecho y las nuevas tecnologías, para luego analizar el problema de la desigualdad en el acceso a las nuevas tecnologías.

2. Las tecnologías digitales en el ámbito jurídico en Latinoamérica

Como hemos señalado, las tecnológicas de la información y las comunicaciones (o Tics) han traído consigo una serie de transformaciones transcendentales, ya sea en el ámbito privado o el público. En este último

sector, las Tics han llevado al desarrollo de lo que se denomina el “gobierno electrónico”, el uso de la tecnología para aumentar la eficiencia de las actuaciones de la administración pública, mejorando la prestación de servicios a las comunidades. Dentro de las muchas facetas del gobierno electrónico destaca la justicia digital, es decir, la incorporación de la tecnología en el funcionamiento de los órganos de justicia.

Dentro del ámbito judicial, las Tics suelen usarse de dos maneras: en primer lugar y la más común, es como un soporte digital para las actuaciones procesales, que una vez realizadas de forma tradicional se suben a un archivo o base de datos digital, que sirve de apoyo para los usuarios, permitiendo el seguimiento a distancia de las actuaciones. El segundo es la creación de sistemas que permiten realizar actuaciones legalmente validas directamente a través de los medios digitales, sin necesidad de presentarse físicamente en el tribunal o utilizar soportes físicos².

El uso de sistemas digitales facilita la función de los tribunales, tanto al momento de la gestión de las causas, como al momento de decidir. Según Londoño Sepúlveda:

De esta forma, si el Juzgado, Tribunal o Corte, cuenta con un sistema que le permita gestionar de manera automatizada las etapas del proceso, minimizar la realización de tareas repetitivas, determinar su agenda claramente, entonces se puede concentrar en su función más importante, la toma de decisiones. Es allí donde en la actualidad igualmente ocurren importantes demoras, pues mucho del esfuerzo de la justicia se pierde en la gestión de los procedimientos cuya automatización se propone. Igualmente un sistema de gestión de los procesos va a evitar que una determinada causa se olvide o simplemente no se gestione debido al gran cúmulo de trabajo con el que tienen que lidiar los despachos judiciales.³

El uso de archivos, soportes y expedientes digitales también facilita la gestión de información sensible. Dependiendo de la competencia del tribunal, los expedientes pueden contener información confidencial relativa a los hechos del caso, la información de las personas naturales y jurídicas involucradas (incluyendo información sobre sujetos vulnerables como menores de edad,

² M.E. GARCÍA BARRERA, *Juzgado sin papel, un paso más en la justicia electrónica*, in *Rev. IUS. Rev. del Inst. Ciencias Puebla*, vol. 12, no. 41, 2018, pp. 133-154.

³ N.R. LONDOÑO SEPÚLVEDA, *El uso de las TIC en el proceso judicial: una propuesta de justicia en línea*, in *Revista Facultad de Derecho y Ciencias Políticas*, 40, 112, 2010, pp. 123-142, p. 137.

víctimas de violencia doméstica, sexual o de género), secretos corporativos, propiedad intelectual, números telefónicos, información bancaria, resultados de evaluaciones médicas o psicológicas, así como información propia de los tribunales y jueces, que pueda afectar el funcionamiento de los órganos de justicia o la seguridad de los funcionarios.

El uso de la TIC permite agilizar el procesamiento de la información, reduciendo los procesos burocráticos involucrados, en muchos casos responsables de gran parte de la carga de trabajo de los juzgados tanto en América como en Europa. En este sentido, la justicia digital es un aspecto clave en la búsqueda de modernizar el funcionamiento de los órganos de justicia, lo que justifica el interés que en las últimas décadas se ha dedicado al crecimiento de la justicia digital, el desarrollo de la cual permite igualmente expandir el alcance de los órganos de justicia a zonas rurales y poco accesibles, al limitar la necesidad de acudir personalmente a las sedes de los órganos de justicia.

En los últimos años uso de la justicia digital se ha extendido en Latinoamérica a distinto nivel. Al menos 18 estados de la región publican datos relativos a la estructura de los órganos de justicia, calendarios judiciales, diarios oficiales y mantienen una base de datos para la consulta y publicación de jurisprudencia. Más de la mitad de estos Estados también ofrecen información acerca de los requisitos para los trámites y procedimientos y sus respectivos plazos, así como otros servicios disponibles. La justicia digital también facilita el intercambio de información entre los funcionarios del poder judicial, ya sean jueces, secretarios, entre otros, lo que agiliza la gestión de las causas y los casos de colaboración entre distintas sedes.

Dentro de la justicia digital y los derechos al uso de las nuevas tecnologías, se comprende:

- Derecho al uso de la tecnología, y sub derechos/obligación de uso de Tic.
- Derecho al debido proceso digital.
- Derecho a presentar documentos electrónicos.
- Derecho a presentar pruebas por medios digitales.
- Derecho a radicar digitalmente.
- Derecho a la seguridad digital.
- Derecho a la protección de datos.
- Derecho a acceder al expediente por medios digitales.
- Derecho a la autenticación digital.
- Derecho a tener las decisiones de forma electrónicas (autenticidad,

integridad y disponibilidad).

- Derecho a la notificación electrónica.
- Derecho a la impugnación electrónica.

Analicemos algunos ejemplos del uso de las TIC y la justicia digital en América Latina. En Argentina, los primeros ejemplos de uso de las tecnologías digitales por parte del Estado en ámbitos relacionados al derecho tienen lugar en la década de los noventa y han continuado desarrollándose desde entonces. Estos primeros usos incluyen la digitalización de documentos, las notificaciones por medios electrónicos, las firmas electrónicas y el poder hacer pagos de servicios públicos a través del internet. No obstante, no sería hasta la aprobación de la Ley Nro. 26685, de Expediente Electrónico, que se inicia la justicia digital, con un sistema que permite la realización de actos procesales a través de los medios digitales⁴.

El caso de Costa Rica es similar, la introducción de las TIC en el ámbito judicial tiene lugar a inicios de los noventa, como parte de los esfuerzos gubernamentales por modernizar el sistema de justicia del país. Con la llegada del nuevo milenio, estos esfuerzos se incrementaron, lo que ha llevado a que se ofrezcan una gama de servicios y herramientas digitales al público para la gestión y el seguimiento de los procedimientos judiciales, además de transformar la manera en la que los órganos de justicia operan⁵.

En Venezuela, el momento clave para el nacimiento de la justicia digital se produjo en el año 2000, con una sentencia de la Sala Constitucional del Tribunal Supremo de Justicia (específicamente la sentencia 656 de ese año), que reconoció como necesario el actualizar el ordenamiento jurídico nacional para adaptarlo a la realidad de las nuevas tecnologías y las oportunidades que estas ofrecen. Para la Sala, esto debía traducirse en cambios técnicos y jurídicos que permitiesen establecer un sistema virtual mediante el cual los usuarios puedan realizar actuaciones judiciales, introducir documentos, firmarlos, enviarlos a los tribunales y que estos puedan archivarse digitalmente. En 2001 se dicta el Decreto ley sobre mensajes de datos y firmas electrónicas, ante la falta de

⁴ G.A. AMONI REVERÓN, *El uso de la videoconferencia en cumplimiento del principio de inmediación procesal*, in *Rev. Ius*, vol. 7, no. 31, 2013, pp. 67-85, doi: 10.35487/rius.v7i31.2013.2.

⁵ K. MORALES-NAVARRO, *La inclusión de las tecnologías en la gestión judicial Poder Judicial de República de Costa Rica*, in C. RIEGO, A. BINDER (eds.), *El rol de las Nuevas Tecnologías en el Sistema de Justicia*, Eds. Publicación semestral del Centro de Estudios de Justicia de las Américas - CEJA, Año 9, N° 162011, pp. 48-55.

regulación sobre esta materia en el país, un avance influenciado por la sentencia ya mencionada.

Lamentablemente los desarrollos en la materia han sido irregulares. Por ejemplo, aún no existe una normativa que autorice o regule la celebración de audiencias virtuales mediante videoconferencias dentro de los procedimientos judiciales. La única mención del uso de este método se encuentra en la Ley Orgánica contra la Delincuencia Organizada y el Financiamiento del Terrorismo, aprobada por la Asamblea Nacional en el año 2012, que establece la posibilidad de hacer uso de videoconferencias en aquellos casos donde la comparecencia de un testigo residente en una ciudad diferente a aquella donde se celebra el proceso se estime como no conveniente o sea imposible por causas de fuerza mayor. Otros ejemplos incluyen el Código Orgánico Procesal Penal de 2012 que permite la realización de notificaciones por medios digitales, incluyendo el uso de correos electrónicos e incluso videoconferencias, o la Ley Orgánica del Tribunal Supremo de Justicia de 2010, que autoriza el uso las tecnologías digitales en los procesos que se celebren en esa instancia, sin hacer más referencias, dejando un amplio margen a los magistrados para decidir que tecnologías pueden emplearse y las regulaciones al uso de las mismas⁶.

En cuanto a Colombia y al igual que en los Estados ya mencionados, el empleo de las Tics en el ámbito judicial inicia a mediados de la década de los noventa, específicamente en el año 1995, cuando se elabora la “estrategia de sistematización del ejercicio de la función judicial y la administración de justicia”, mediante la cual se destinaban fondos a nivel nacional para la adquisición de equipos, la construcción de infraestructura y el desarrollo de sistemas informáticos para gestionar las causas en el sistema de justicia colombiano, así como para capacitar al personal del poder judicial para hacer uso de la tecnología y los nuevos sistemas que serían implementados.⁷

No obstante no sería hasta la década pasada cuando muchos de estos planes se materializarían en medidas concretas a nivel administrativo y legislativo que realmente puede hablarse de justicia digital en Colombia. Un momento clave es la aprobación de la Ley 1394 de 2010, por la cual se determina un arancel judicial y mediante la cual se destinaron recursos para

⁶ G.A. AMONI REVERÓN, *El uso de la videoconferencia en cumplimiento del principio de inmediación procesal*, in *Rev. Ius*, vol. 7, no. 31, 2013, pp. 67-85, doi: 10.35487/rius.v7i31.2013.21

⁷ Consejo Superior de la Judicatura, *Plan de desarrollo de la Justicia 1995-1998*, Bogotá, Colombia, 1994.

atender el problema de la congestión de los tribunales. A través de esta ley se encomendó a la Sala Administrativa del Consejo Superior de la Judicatura el elaborar un programa para invertir los fondos recibidos en el desarrollo e implementación de la justicia digital en Colombia. Gracias a esto el poder judicial pudo desarrollar software para la administración de las causas judiciales y la atención a los usuarios. El primer sistema implementado tenía como nombre “Justicia XXI”, un sistema cliente-servidor, mientras que el segundo se denomina “Justicia Web”, que permite el seguimiento de los procesos judiciales ordenadas cronológicamente, además de servir de respaldo para los jueces al momento de alcanzar una decisión para las controversias⁸.

Otra innovación importante fue la creación del programa “Pretoria”, un sistema de inteligencia artificial diseñado para gestionar los procedimientos de acción de tutela constitucional, que permite recibir, clasificar y analizar los diferentes procedimientos que con excesiva frecuencia reciben los tribunales en Colombia. Es importante aclarar que el procedimiento de acción de tutela constitucional, acción para buscar la garantía y protección de los derechos fundamentales ante amenaza o violación proveniente de una autoridad o funcionario público, donde el solicitante espera la restitución de sus derechos y el fin de las conductas que los amenazan o violan, constituye una de las principales causas de la saturación de los órganos de justicia en Colombia. Se estima que entre los años 2015 y 2019 se recibieron más de 720 mil acciones de tutela al año. Pese al éxito de este sistema automatizado, no se han establecido sistemas similares para el resto de los procedimientos, ni se utilizan herramientas de análisis digital de datos en las demás sedes judiciales, lo que a todas luces parece una oportunidad perdida para solucionar el problema de la congestión de los órganos de justicia y brindar una mejor experiencia a los usuarios⁹.

Por su parte, a nivel administrativo, en los documentos del Consejo Nacional de Política Económica y Social CONPES-3854 de 2016 y CONPES 3995 de 2020, desarrollaron el concepto de la justicia digital. Estos documentos hicieron énfasis en temas como la ciberseguridad y las obligaciones del Estado

⁸ G.S. LÓPEZ-JARAMILLO, *Nuevo modelo de justicia en línea colombiano*, in *Tecnologías al servicio de la Justicia y el Derecho*, Pontificia Universidad Javeriana, Colombia, Bogotá, 2019, pp. 37-58.

⁹ E. ESTEVEZ, P. FILLOTRANI, S. LINARES LEJARRAGA PROMETEA, *Transformando la administración de justicia con herramientas de inteligencia artificial*, Banco Interamericano de Desarrollo, Washington, DC, USA, 2020, doi: 10.18235/0002378

de proteger a los usuarios y reducir los riesgos a los que estos puedan verse expuestos en el uso de las Tics, la protección de los datos personales y la identidad, el resguardo de la confidencialidad, entre otros aspectos¹⁰.

Por último es importante hacer mención a los esfuerzos gubernamentales que tuvieron lugar en el marco de la pandemia del Covid-19. Estos pueden observarse de forma clara en el Decreto 806 de 2020, Por el cual se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia, en el marco del Estado de Emergencia Económica, Social y Ecológica. Mediante este decreto se implementaron medidas para el funcionamiento de la administración de justicia durante la pandemia en cumplimiento con las recomendaciones de bioseguridad y distanciamiento social, dando prioridad al uso de las Tics en los procesos judiciales, especialmente el uso de actuaciones virtuales y videoconferencias como sustituto de las audiencias presenciales. Sin embargo, se trató de medidas de emergencia y tras el fin de la pandemia se han retomado las audiencias y procesos tradicionales¹¹.

En el caso de Brasil, las iniciativas comienzan a mediados de la década de los dos mil, específicamente con la Ley 11419 de 2006 donde se crea el expediente electrónico para todos los procesos judiciales, ya sean civiles, mercantiles, laborales, administrativos, entre otros. Por su parte la Ley 11900 aprobada en 2009 estableció el uso de videoconferencias para la declaración de personas privadas de libertad, pero solo en casos excepcionales¹².

En años recientes el Estado ha adelantado otras iniciativas vinculadas a las nuevas tecnologías y a la justicia digital, como Plan Decenal del sistema de justicia 2017-2027 y Plan Sectorial de Desarrollo Rama judicial 2019-2022. Además el gobierno ha destinado más de la cuarta parte del presupuesto anual del poder judicial al desarrollo de la justicia digital y a la inversión tecnológica¹³.

¹⁰ Departamento Nacional de Planeación, Política Nacional de Confianza y Seguridad Digital, Bogotá, Colombia, DNP, 2020, p. 51.

¹¹ Presidencia de la República de Colombia, *Decreto 806 de 2020*, Bogotá, 2020, pp. 21.

¹² A. FREIRE PIMENTEL, C.P. MATEUS, Y.P. MENDES SALDANHA, *El proceso judicial electrónico, la seguridad jurídica y violaciones de los derechos fundamentales desde el punto de vista del sistema jurídico brasileño*, in *Rev. Derecho, Comun. y Nuevas Tecnol.*, no. 17, 2017, pp. 119.

¹³ E. GIL BOTERO, *Las TIC como logro para una justicia moderna*, in *Tecnologías al servicio de la Justicia y el Derecho*, Pontificia Universidad Javeriana, Colombia, Bogotá, 2019, pp. 59-69.

México llevó a cabo la reforma de la Ley Federal de Procedimiento Contencioso Administrativo para incluir la justicia digital. Esta reforma, que tuvo lugar en 2009, ha permitido la celebración de audiencias virtuales, el expediente electrónico y la sustanciación de los procesos judiciales a través del internet, y ha estado en plena vigencia desde 2011¹⁴.

En el caso de El Salvador, los desarrollos de la justicia digital se han dado únicamente en los últimos años. En 2015 el órgano legislativo del país aprobó la celebración de audiencias virtuales pero exclusivamente en los juicios criminales. El objeto de la medida fue el agilizar las audiencias para aquellas personas privadas de libertad, evitando así los problemas asociados al traslado de los prisioneros a las sedes de los tribunales¹⁵.

Comparando el desarrollo y evolución de la justicia digital en diferentes países de América Latina, es posible apreciar ciertos patrones emerger. En casi todos los casos, el interés en el uso de las tecnologías digitales en los sistemas de justicia comenzó en la década de los noventa, pero sin que se realizaran avances significativos, para luego reaparecer en los 2000's, donde finalmente se habían establecido sistemas digitales para apoyar el funcionamiento de los órganos de justicia.

Estos sistemas han variado de forma considerable en su complejidad y en la cantidad de servicios que ofrecían al público. Algunos solo tienen una función complementaria, permitiendo consultar los actos procesales y la jurisprudencia, mientras otros han ido más allá, aprovechando las oportunidades de la tecnología para la gestión de los casos y autorizando actuaciones directamente en los expedientes digitales. No obstante, aún no se ha producido una transformación digital plena en los sistemas jurídicos, siendo muy común que estos sean una excepción para casos específicos.

Como señala Rodríguez Márquez:

Como se ha podido observar, los tribunales latinoamericanos han invertido tiempo y fondos nacionales en su automatización. Por lo anterior, la incorporación de las TIC para los países de la región ha constituido una oportunidad para consolidar la eficacia y eficiencia en los procesos judiciales, para estrechar un vínculo permanente

¹⁴ R.J.Á. CHÁVEZ, *El Modelo del Sistema de Justicia en Línea y su expansión a otros ámbitos de la jurisdicción*, in D.C. Salgado, J. B. Quinto (eds.), *El derecho mexicano contemporáneo: Retos y dilemas*, Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, 2011, pp. 197-212.

¹⁵ Asamblea Legislativa El Salvador, *Decreto 146 de 2015*, El Salvador, 2015.

del Estado con los ciudadanos, asimismo, para fomentar la participación ciudadana en los procesos judiciales y hacer transparente la información pública como arma contra la corrupción. Sin embargo, pese a estos esfuerzos, Beauchard y Hammergren coinciden en que dicha automatización no se ha utilizado para crear bases de datos mejoradas, sino para el procesamiento de textos de documentos ordinarios (documentos tradicionales escaneados), razón por la cual existe ausencia del flujo de datos sobre los casos, lo cual imposibilita evaluar los impactos¹⁶.

La justicia digital es una herramienta que ofrece muchas posibles ventajas, no solo para mejorar la gestión de los casos a nivel administrativo, sino para extender el alcance de los órganos de justicia, permitir atender a poblaciones rurales y remotas, mejorar la calidad del servicio, entre otros beneficios. En ese sentido, es necesaria aumentar la inversión en la justicia digital en Latinoamérica como mecanismo para llevar la justicia a las comunidades y grupos más vulnerables.

Pero este objetivo solo podrá ser alcanzado si la inversión en tecnología también está dirigida a las comunidades a las que se pretende apoyar, no solo para darles los dispositivos y la infraestructura para acceder a los sistemas informáticos, sino para capacitarlos en el manejo de esos mecanismos. De lo contrario, los miembros de estas poblaciones dependerán de terceros para poder acceder a la justicia digital y no podrán hacer un seguimiento personal de los procesos que los involucren a ellos y a sus comunidades.

3. Desigualdad y derechos emergentes

El tema de la justicia digital surge en el marco de una serie de derechos relacionados al acceso y aprovechamiento de las nuevas tecnologías por parte de la población. Estos derechos incluyen la accesibilidad por parte de toda la población a la tecnología, a la infraestructura tecnológica, a los servicios necesarios para el funcionamiento de estos recursos, como la electricidad y la conectividad a internet; pero también incluye otros temas relacionados, como la neutralidad del internet (es decir, permitir un acceso igualitario a las distintas páginas y servidores de internet); los derechos a la privacidad, a la

¹⁶ M.P. RODRÍGUEZ-MÁRQUEZ, *Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano*, in *Revista UIS ingenierías*, Universidad Industrial de Santander, vol. 20, núm. 3, 2021, pp. 19-46.

identidad y a la confidencialidad; la libertad de expresión, de crear contenido y compartirlo, de estar informado; el derecho a la educación con respecto a las nuevas tecnologías y que estas sean accesibles y comprensibles para el público. Todo lo anterior implica que para que las nuevas tecnologías tengan el impacto deseado en la sociedad, es decir, se conviertan en factores de la transformación social que puedan alcanzar todos los sectores de la población, debemos acercarnos a ella con una perspectiva que tenga como eje la integración y aquellos factores que juegan un rol en las dinámicas de poder de la sociedad, como la raza, el género, la clase, la cultura y la identidad¹⁷.

No obstante la perspectiva tradicional al abordar el problema de la tecnología y la desigualdad, pone todo su énfasis en el tema de la accesibilidad, universalidad y en la apropiación de las tecnologías, sin involucrar las perspectivas de género o de raza. Así, los enfoques tradicionales por un lado asumen la neutralidad de las nuevas tecnologías, encontrando en la implementación de las mismas el origen de las desigualdades¹⁸.

Por otro lado, el énfasis en el tema de la brecha digital desde una postura netamente socioeconómica ignora otras dinámicas de poder involucradas en la forma como ciertos individuos o grupos se relacionan con las tecnologías. Por ejemplo Yansen y Zukerfeld señalan que en el caso de las mujeres, estas suelen tener un contacto y un aprendizaje tardío en el ámbito de las tecnologías digitales, generalmente en el contexto de la capacitación laboral o la educación superior, no suelen acercarse a estas a más temprana edad o de una forma más didáctica y experimental, en gran medida por las actitudes sociales que desincentivan su aproximación a este campo y disminuyen su interés, en comparación con sus pares masculinos¹⁹.

En cualquier caso, los elevados niveles de desigualdad en la región (y América Latina es la región más desigual del mundo) afectan los esfuerzos gubernamentales dirigidos a alcanzar la integración social de la población, ya que coexisten en el seno de la sociedad experiencias vitales con diferencias dramáticas, lo que lleva a que los ciudadanos desarrollen expectativas muy diferentes con respecto a sus vidas. Estos problemas además afectan la propia

¹⁷ L. BENÍTEZ-EZYAGUIRRE, *Ciberfeminismo y apropiación tecnológica en América Latina*, in *Virtualis*, Fri, 04 Jan 2019.

¹⁸ J. WAJCMAN, *Technofeminism*, Polity, Cambridge, Reino Unido, 2004.

¹⁹ G. YANSEN, M. ZUKERFELD, *Códigos generizados: La exclusión de las mujeres del mundo del software, obra en cinco actos*, in *Universitas Humanística*, 76, 2013, pp. 207-233.

geografía interna de nuestros países, tanto a nivel regional (por ejemplo, que exista una mayor concentración de recursos y un mejor nivel de vida en las capitales, mientras que las zonas periféricas suelen ser áreas rurales con mayores índices de pobreza y menor acceso a los servicios públicos esenciales) como dentro de las mismas ciudades, por lo que situaciones como la segregación residencial y la estratificación social son predominantes en América Latina²⁰.

Barcena y Prado señalan como un factor importante en la desigualdad la percepción de que las oportunidades que ofrece la sociedad a las personas para mejorar sus condiciones de vida (sean laborales, educativas o de otro tipo) se ofrecen de forma asimétrica, favoreciendo a aquellos que ya se encuentran en una posición ventajosa dentro de la sociedad, aquellos con mayores ingresos y con una mayor proporción de los recursos, posición a la que han llegado gracias a los prejuicios sociales heredados de generación en generación dentro de una “cultura del privilegio”. De esta forma, todos los procesos sociales entran en esta dinámica preexistente y solo ayudan a mantener el status quo, beneficiando de forma desproporcionada a quienes ya gozan de la mayoría del poder económico y social, lo que a su vez solo extiende el problema hacia las futuras generaciones, como parte de un círculo vicioso²¹.

Como ha señalado la CEPAL:

Los análisis de la CEPAL sobre el desarrollo económico y social han señalado que las economías latinoamericanas y caribeñas históricamente se han caracterizado por la presencia de una marcada heterogeneidad estructural³, que está, en gran medida, en la base de los altos niveles de desigualdad social que caracterizan a la región. La estructura productiva, poco diversificada y altamente heterogénea, en la cual los sectores de baja productividad generan aproximadamente el 50% del empleo, constituye un determinante importante de la desigualdad social. El mercado laboral es el eslabón fundamental que vincula esa estructura productiva con una elevada desigualdad del ingreso en los hogares, relacionada con una distribución muy diferenciada de las ganancias de la productividad y con un acceso altamente

²⁰ Organización de las Naciones Unidas (2013), *Report on the World Social Situation*, 2013, Inequality Matters (ST/ESA/345), Nueva York, Departamento de Asuntos Económicos y Sociales.

²¹ A. BÁRCENA, A. PRADO (2016), *El imperativo de la igualdad: por un desarrollo sostenible en América Latina y el Caribe*, Buenos Aires, Comisión Económica para América Latina y el Caribe (CEPAL)/Siglo XXI.

estratificado al empleo de calidad y a la protección social²².

La desigualdad afecta a su vez la libertad de la población al limitar por un lado la autonomía de las personas, su capacidad para tomar decisiones acerca de su futuro y de desarrollar su propio proyecto de vida; y por otro lado al cercenar el poder político de los individuos o grupos más desfavorecidos, esto es, su capacidad de influenciar la toma de decisiones a nivel colectivo en aspectos como la seguridad por ejemplo. Ambas capacidades se encuentran distribuidas de forma desigual en lo que De Ferranti denomina las “desigualdades de agencia”, que impiden a las personas y comunidades escapar de los esquemas de explotación y subvertir los patrones históricos de marginación social, que en la mayoría de los casos son el resultado de dinámicas complejas donde la dimensión del poder político juega un rol protagonista²³.

Citando nuevamente a Barcena y Prado:

...las brechas productivas no operan solo en el plano socioeconómico, en el que generan desigualdad de ingresos, sino que atraviesan la cultura y las capacidades, y vulneran la propia autonomía de las personas, afectando el ejercicio de sus derechos y el desarrollo de sus capacidades [...].²⁴

En consecuencia el enfoque de las políticas públicas en América Latina debe apuntar más allá de la universalidad como se ha entendido tradicionalmente, y dirigirse específicamente a brindar ayuda a las poblaciones y grupos históricamente marginados y vulnerables, como las mujeres, los grupos indígenas, las poblaciones afrodescendientes, la comunidad LGBT, las personas discapacitadas, los inmigrantes y las personas con menores ingresos. De acuerdo con la CEPAL:

Las políticas públicas de desarrollo social basadas en un enfoque de derechos están

²² CEPAL, *La matriz de la desigualdad social en América Latina*, 2016. Reunión de la Mesa Directiva de la Conferencia Regional sobre Desarrollo Social. Santo Domingo, República Dominicana.

²³ P. DE FERRANTI, Y OTROS, *Desigualdad en América Latina: ¿Romper con la historia?*, Banco Mundial, Washington, D.C., 2004.

²⁴ A. BÁRCENA, A. PRADO (2016), *El imperativo de la igualdad: por un desarrollo sostenible en América Latina y el Caribe*, Buenos Aires, Comisión Económica para América Latina y el Caribe (CEPAL)/Siglo XXI.

orientadas hacia la universalidad, lo que permite fomentar la inclusión social, pero de manera complementaria pueden utilizarse políticas focalizadas, selectivas o de acción positiva para romper las barreras de acceso a los servicios sociales y al bienestar que enfrentan las personas que se encuentran en condiciones de pobreza o vulnerabilidad, las mujeres, los afrodescendientes, los pueblos indígenas, las personas que residen en áreas rezagadas, las personas con discapacidad y los migrantes, así como los niños, los jóvenes y los ancianos...²⁵.

Esto aplica especialmente a las políticas vinculadas a las Tics, donde las desigualdades estructurales que históricamente han afectado a la región se traducen en barreras para el acceso, uso y apropiación de las nuevas tecnologías por parte de los grupos menos favorecidos. En consecuencia, las políticas en materia de Tics deben considerar esta realidad y buscar incorporar al mundo digital a aquellos que aún no gozan de sus beneficios.

4. *Conclusión*

Durante las últimas décadas ha habido un esfuerzo notable de parte de los diferentes Estados de América Latina por elaborar políticas públicas relacionadas con las tecnologías digitales para modernizar muchos aspectos de la función de gobierno. Uno de los aspectos a los que se les ha dado mayor importancia es a la justicia digital, el uso de las Tics dentro del poder judicial.

La justicia digital en la región se ha traducido principalmente en la creación de sistemas virtuales para la digitalización de los documentos y actos procesales, para el seguimiento y la revisión de los mismos a través del internet. Sin embargo, pocos Estados han permitido la realización de actos procesales directamente en los expedientes virtuales, y otros usos de la tecnología, como las videoconferencias para celebrar audiencias virtuales, o el uso de sistemas para la gestión y el procesamiento de las causas, solo han sido implementados de forma excepcional.

Sin embargo, el uso generalizado de las Tics en la región se ve impedido por las circunstancias históricas de desigualdad en nuestro continente y que afectan de forma particular a las minorías, a las mujeres y a otros grupos vulnerables. En consecuencia, las políticas públicas relacionadas con las

²⁵ CEPAL, *La matriz de la desigualdad social en América Latina*, 2016. Reunión de la Mesa Directiva de la Conferencia Regional sobre Desarrollo Social. Santo Domingo, República Dominicana.

2/2023

nuevas tecnologías deben estar enfocadas en incorporar a estas poblaciones en el uso de las Tics.



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

WANDA D'AVANZO

L'evoluzione della *e-Health*. Aspetti bioetici dell'*Internet of Bodies*.

ABSTRACT - The health emergency linked to the Covid-19 pandemic has increased public interest in e-health, the so-called e-Health, which involves the use of increasingly cutting-edge technologies based on artificial intelligence, blockchains and the Internet of things to open up new forms of interaction between man and machine. In the medical field, the world of information technology is now projected towards the creation of a new generation of devices capable of collecting and processing data and information in real time, capable of integrating and interacting constantly with the body of those who use them. This vast area of experimentation takes the name of the Internet of Bodies, or Internet of bodies, which describes a wide range of Internet-connected devices that monitor the human body, collect physiological, biometric or behavioral data, and exchange information through a wireless network. But the convergence between health care and technology raises several concerns about the legal and ethical consequences of the use of tools that connect humans to the Internet, not only from the point of view of the protection of personal data, but also in relation to information security and bioethical issues.

KEYWORDS - e-Health - internet of things - internet of bodies - RFID - privacy - security

2/2023

WANDA D'AVANZO*

L'evoluzione della e-Health. Aspetti bioetici dell'Internet of Bodies**

SOMMARIO: 1. Introduzione – 2. Le tecnologie a supporto della sanità elettronica L'Internet of Bodies – 3. I dispositivi dell'Internet dei corpi – 4. La tecnologia RFID – 5. Risvolti bioetici dell'Internet dei corpi. Tutela dei dati e consenso – 6. Il problema della sicurezza informatica nella gestione dei dati sanitari – 7. Conclusioni.

1. Introduzione

L'emergenza legata alla pandemia da Covid-19 ha aumentato l'interesse pubblico per la sanità elettronica, c.d. *e-Health*, e ne ha determinato una rapida ascesa in funzione della necessità di garantire la continuità nell'erogazione delle cure ambulatoriali in concomitanza con la drastica riduzione degli spostamenti e dei contatti tra le persone.

La pandemia ha, di fatto, imposto e accelerato l'adozione di soluzioni digitali e strumenti avanzati in ambito sanitario, al fine di offrire una sorveglianza clinica integrata e completa, semplificando e assicurando la stabilità dell'assistenza.

E l'ampia diffusione di tecnologie di ultima generazione mostra come, allo stato attuale, i sistemi sanitari stiano attraversando una fase di revisione completa in cui diventa fondamentale puntare ad un miglioramento generale del servizio offerto. Infatti, in una prospettiva di *smart governance* dei servizi pubblici essenziali assume fondamentale importanza la creazione di servizi sanitari più efficienti, sfruttando ciò che di meglio possono offrire le tecnologie ICT al fine di ridurre o rimuovere le barriere sociali.

La digitalizzazione in sanità va intesa sia dal punto di vista aziendale che dal lato dell'utente e coinvolge tutte le strutture, pubbliche e private, preposte alla tutela della salute e l'intera gamma delle funzioni proprie del settore cui si applicano le tecnologie ICT.

L'elemento di base della trasformazione è costituito dalla digitalizzazione delle informazioni sanitarie, che vengono raccolte e gestite attraverso strumenti tecnologici, consentendo così compiti, mansioni ed atti di assistenza sanitaria, ma anche atti amministrativi e organizzativi. L'assetto generale del sistema sanitario nel suo insieme è, quindi,

* Professore aggregato di "E-Governance e società digitali", Università degli studi "Magna Græcia" di Catanzaro.

** Contributo sottoposto a valutazione anonima.

rappresentato da flussi informativi: clinici, epidemiologici, statistici, economico-finanziari e formativi che oggi vengono sempre più gestiti in modalità digitale.

Questo nuovo modo di raccogliere e far circolare i dati ha l'obiettivo, da un lato, di migliorare la qualità del servizio sanitario nazionale, con conseguente miglioramento dell'efficienza ed economicità amministrativa, in una prospettiva di amministrazione digitale, e, dall'altro, mira a favorire una migliore comunicazione tra medico e paziente in un'ottica di teleassistenza.

La dematerializzazione della documentazione medica favorisce la condivisione delle informazioni tra gli attori del sistema attraverso la c.d. cartella clinica elettronica e il c.d. fascicolo sanitario elettronico, che rappresentano le azioni di base per la transizione digitale del settore sanitario¹.

A livello comunitario, la *e-Health* rappresenta uno dei più importanti obiettivi dell'agenda digitale europea, non solo per quel che riguarda i rapporti tra pazienti e strutture mediche, in cui rileva l'interoperabilità dei servizi di sanità elettronica, ma anche, come si vedrà più in dettaglio nel prosieguo, per ciò che concerne le nuove possibilità di comunicazione *peer-to-peer* tra medici e pazienti e quelle innovazioni tecnologiche che possono avere un impatto considerevole sullo stile di vita degli individui, come i dispositivi indossabili, le applicazioni per *smartphone* o gli strumenti di teleassistenza².

La sanità digitale richiede, quindi, la concreta attuazione da parte delle aziende sanitarie degli Stati membri della riorganizzazione dei processi interni e di erogazione dei servizi ai cittadini, nonché l'implementazione della digitalizzazione dell'intera relazione tra medico e paziente nella prospettiva di favorire la continuità delle cure, la maggiore disponibilità di informazioni sul paziente, la più agevole gestione dei

¹ La riflessione informatico giuridica in materia di *e-health* ha analizzato il tema da molti punti di vista: non solo la digitalizzazione delle procedure, ma anche gli aspetti bioetici e i rischi connessi all'abuso delle tecnologie. Fra gli altri si citano: C. FARALLI, R. BRIGHI, M. MARTONI (a cura di), *Strumenti, diritto, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'e-Health*, Giappichelli, Torino, 2015; L. PALAZZANI, *Dalla bio-etica alla tecnologia: nuove sfide al diritto*, Giappichelli, Torino, 2017; U. PAGALLO, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, Mimesis, Milano, 2022.

² Sul tema si veda T. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche*, Ipsoa, Milano, 2021, *amplius*.

processi sanitari³.

Adeguare la sanità alla trasformazione digitale significa per questo uniformare il sistema sanitario nazionale alla *governance* partecipata e responsabile dei vari ambiti e dei vari livelli di intervento della pubblica amministrazione.

In tal senso, la Commissione europea ha fornito una serie di raccomandazioni agli Stati membri per la creazione di un sistema sicuro che permetta ai cittadini europei l'accesso transfrontaliero ai documenti sanitari, un progetto importante che pone le basi per la realizzazione di un ambiente digitale delle cartelle cliniche condivisibili, avviato da tempo e alimentato da ulteriori *input* sulla diagnostica per immagini e referti.

I Paesi Ue dovrebbero, quindi, riuscire a scambiarsi i profili sanitari sintetici e le prescrizioni elettroniche attraverso l'utilizzo dell'*eHealth Digital Service Infrastructure* (eHDSI), l'infrastruttura unica europea di servizi digitali per l'assistenza sanitaria in un ambiente digitale.

La Commissione ha anche stabilito una tabella di marcia per consentire a pazienti e operatori sanitari di collegare i dispositivi e le tecnologie ed investire nella ricerca verso la medicina personalizzata del futuro, che si sostanzia in servizi sanitari più intelligenti, più sicuri e centrati sul paziente, con particolare attenzione alla c.d. *Mobile Health*, grazie alla rapida crescita di utilizzo di *tablet* e di *smartphone*⁴.

La grande attenzione verso la sanità digitale a livello comunitario trova fondamento nella previsione secondo la quale le spese di carattere sanitario e assistenziale determineranno un incremento del 9% del prodotto interno lordo dell'Ue entro il 2050 ed è verosimile che le tecnologie dell'informazione e della comunicazione possano contribuire in modo sostanziale a ingenti risparmi di spesa e a recuperi di produttività in termini indiretti come *Return on Investment* (ROI).

A livello nazionale, la sesta missione del PNRR assegna al potenziamento del digitale un ruolo di fondamentale importanza per lo sviluppo della telemedicina, la valorizzazione del patrimonio informativo sanitario e il potenziamento del fascicolo sanitario elettronico⁵.

³ M. PAPARELLA, S. SOLVI, *Che cos'è il Fascicolo Sanitario Elettronico e come utilizzarlo*, in *Forum PA*, 2016.

⁴ P. L. DI VIGGIANO, *Sanità digitale e Welfare elettronico*, in *Rivista elettronica di diritto, economia, management*, 3, 2014, pp. 77-78.

⁵ M.T. DELLA MURA, *La nuova Sanità con il PNRR: digitale e dati sono i pilastri del futuro*, in *Agenda Digitale* (www.agendadigitale.eu), 2021.

2. Le tecnologie a supporto della sanità elettronica. L'Internet of Bodies

La sanità elettronica si attua, quindi, attraverso l'utilizzo di tecnologie all'avanguardia che stanno facendo il loro ingresso in ogni settore della pubblica amministrazione. Alla base di questo processo si pongono la raccolta, la gestione e l'analisi, anche predittiva, dei dati che rappresentano gli elementi chiave per la creazione di ambienti pubblici *smart*.

Le tecnologie che trovano un sempre maggior impiego sfruttano le potenzialità dell'intelligenza artificiale, delle *blockchains* e dell'Internet delle cose per aprire a nuove forme d'interazione tra uomo e macchina, quasi a voler creare una sorta di fusione tra i due elementi.

Nel campo medico, in particolare, il mondo dell'informatica è ormai proiettato verso la creazione di una nuova generazione di apparecchi in grado di raccogliere ed elaborare in tempo reale dati e informazioni, rendendoli di uso comune e diffuso, in grado di integrarsi e di interagire costantemente con il corpo di chi li utilizza.

In un mondo altamente connesso, gli individui sono sempre più consapevoli del controllo che possono esercitare sul proprio benessere fisico e questo favorisce l'introduzione di tecnologie in grado di offrire nuove possibilità di comunicazione tra medici e pazienti.

Questa vasta area di sperimentazione prende il nome di *Internet of Bodies*, o Internet dei corpi, espressione coniata nel 2016 per descrivere l'ampia gamma di dispositivi connessi ad Internet che monitorano il corpo umano, raccolgono dati fisiologici, biometrici o comportamentali, e scambiano informazioni attraverso una rete *wireless*. In sostanza, l'Internet dei corpi si avvale di una serie di strumenti tecnologici che collegano l'essere umano a dei dispositivi artificiali connessi alla rete. Essi monitorano il corpo umano, raccolgono parametri sanitari e altre informazioni personali e trasmettono tali dati grazie alle tecnologie di connettività⁶.

Come per l'Internet delle cose, l'Internet dei corpi opera su quattro livelli. Funziona attraverso un *hardware* di elaborazione dati e una serie di applicazioni di configurazione gestibili direttamente dagli utenti che, tramite la rete, scambiano informazioni in modo sicuro tra loro e con un *hub*

⁶ A.M. MATWYSHYN, *The internet of bodies*, in *Wm & Mary Law Review*, 61, 2019, p. 77. Sul punto si veda anche C. AMATO, *Internet of Bodies: Digital content directive, and beyond*, in *Jipitec*, 12, 2021, pp. 181 ss.; G. BODDINGTON, *The Internet of Bodies—alive, connected and collective: the virtual physical future of our bodies and our senses*, in *AI & society*, 2021, pp. 1-17.

centrale a intervalli prestabiliti o in tempo reale, permettendone al contempo l'archiviazione, l'analisi e la visualizzazione⁷.

E gli strumenti di cui si avvale per funzionare possono essere di due tipologie: non invasivi ed indossabili, oppure invasivi, cioè impiantabili, iniettabili o ingeribili.

Esistono, poi, anche una serie di applicazioni dell'Internet medico che creano delle soluzioni ospedaliere intelligenti come ad esempio i letti connessi con funzionalità di monitoraggio dei segni vitali.

Con riguardo specifico al campo della salute, queste tecnologie sono progettate per apportare una serie di benefici sia per la gestione del sistema sanitario che per il supporto alle decisioni cliniche e nella medicina preventiva.

La tecnologia dell'Internet dei corpi è pensata per consentire agli operatori sanitari di intervenire tempestivamente grazie al monitoraggio da remoto delle condizioni di salute del paziente, prevenendo ed evitando situazioni critiche di emergenza. Inoltre, la raccolta su larga scala di dati sanitari tramite dispositivi medici intelligenti potrebbe supportare l'analisi delle tendenze sanitarie di vaste aree demografiche e geografiche, offrendo soluzioni per migliorare il sistema sanitario pubblico.

3. I dispositivi dell'Internet dei corpi

I dispositivi dell'Internet dei corpi indossabili sono ormai una categoria diffusissima. Questi strumenti sono una diretta espressione del c.d. *ubiquitous computing*, perché non si limitano ad introdurre la tecnologia informatica in oggetti di uso quotidiano e diffuso, ma sono in grado di interagire tra loro e con l'ambiente circostante in modo automatico e, spesso, anche senza che l'utente ne sia pienamente consapevole. Essi, inoltre, garantiscono la continua accessibilità alle informazioni, essendo sempre a contatto ed operando in simbiosi con il fruitore e, quindi, costantemente disponibili all'uso.

La caratteristica più rilevante dei dispositivi indossabili è la connettività: pur non costituendo un tratto di differenziazione specifico rispetto ad altri dispositivi, risulta tuttavia essere un elemento funzionale

⁷ S.B. BAKER, W. XIANG, I. ATKINSON, *Internet of things for smart healthcare. Technologies, challenges, and opportunities*, in *IEEE Access*, 5, 2017, pp. 26521-26544; J. CALVILLO-ARBIZU, I. ROMÁN-MARTÍNEZ, J. REINA-TOSINA, *Internet of things in health: Requirements, issues, and gaps*, in *Computer Methods and Programs in Biomedicine*, 208, 2021, 106231.

imprescindibile, se non in alcuni casi il principale elemento caratterizzante le tecnologie indossabili, specificatamente concepite per aumentare le possibilità di interazione del fruitore con l'ambiente sia reale che virtuale.

Questi supporti indossabili hanno trovato fin da subito largo impiego nel settore biomedicale e sono utilizzati per il monitoraggio continuo a distanza delle condizioni fisiche di pazienti a rischio o affetti da particolari patologie⁸.

Ma a seguito del crescente interesse del mercato nei confronti di supporti mobili sempre più versatili, grazie all'abbassamento dei costi, sono stati perfezionati anche dispositivi con una vocazione più spiccatamente commerciale, utilizzabili dagli utenti nella normale vita quotidiana, nel tempo libero oppure come supporto ad attività pratiche di vario genere.

I *fitness tracker*, ad esempio, sono tecnologie esterne al corpo che raccolgono informazioni che vengono analizzate da *software* proprietari di aziende private. I braccialetti, gli orologi, e le varie applicazioni per *smartphone* possono tenere traccia dei movimenti del corpo, della frequenza cardiaca, degli schemi di sonno e altri dati fisici utili per il monitoraggio.

Molti dispositivi effettuano ulteriori analisi intuitive, offrendo agli individui un quadro completo della propria salute ed incoraggiando così migliori misure sanitarie preventive, come una dieta sana e l'esercizio fisico. Questi dispositivi funzionano utilizzando accelerometri avanzati e altri sensori in grado di tradurre il movimento in misurazioni digitali.

Accanto ai dispositivi indossabili, gli strumenti dell'Internet dei corpi comprendono, come visto in precedenza, tecnologie più invasive che, al momento, sono solo in sperimentazione e/o in via di prima applicazione.

Per citare qualche esempio possiamo menzionare i pancreas artificiali che potrebbero automatizzare il dosaggio dell'insulina per i soggetti affetti da diabete.

I nuovi *pacemaker* cardiaci e defibrillatori impiantabili potrebbero consentire il controllo continuo ed in tempo reale delle fluttuazioni cardiache di un paziente, regolando la frequenza dei battiti.

La possibilità di impiantare delle interfacce di comunicazione tra cervello umano e computer potrebbe consentire ai soggetti che hanno subito l'amputazione di un arto di controllare le protesi con la mente.

Una ulteriore tecnologia, approvata già dal 2017 dalla *Food and Drug Administration* americana per la diffusione su larga scala per particolari categorie di malati, è la pillola digitale.

⁸ E. GERMANI, L. FEROLA, *Il wearable computing e gli orizzonti futuri della privacy*, in *Dir. Inform.*, 1, 2014, p. 76.

Le pillole digitali contengono sensori che registrano l'assunzione del farmaco. Questa tecnologia è stata introdotta nel trattamento della schizofrenia e di alcune forme di disturbo bipolare e depressione. Gli operatori sanitari e i medici accedono alle informazioni trasmesse dalla pillola digitale attraverso un portale web⁹.

Da ultimo, le società di *software* di intelligenza artificiale, stanno sviluppando dei sistemi in grado di rilevare e raccogliere dati sulle emozioni umane analizzando le espressioni facciali, le intonazioni della voce e altri segnali audiovisivi, aprendo la strada ad una nuova branca dell'Internet dei corpi che prende il nome di *Internet of Behaviours* o Internet dei comportamenti¹⁰.

4. La tecnologia RFID

È prevedibile che nel prossimo futuro le funzionalità dei dispositivi dell'Internet dei corpi saranno ampliate e perfezionate.

Una delle possibilità più prossime, già prospettate dalla scienza, di evoluzione di queste tecnologie sarà quella di inserire nel corpo umano dei *microchip* in grado di connettere l'uomo alla rete tramite la c.d. RFID.

La sigla "RFID" è l'acronimo dell'espressione "*Radio Frequency Identification*" e assolve una funzione di identificazione di beni, individui o animali per effetto di una trasmissione di segnali a radiofrequenza. L'identificazione comporta l'attribuzione di un'identità univoca finalizzata alla raccolta di informazioni riguardanti gli interessati mediante l'ausilio di apparati radio, associati agli stessi. Le informazioni vengono assunte tramite operazioni di ricerca, selezione, localizzazione spaziale, tracciamento.¹¹

La tecnologia RFID, nasce fondamentalmente per l'identificazione e il monitoraggio delle merci, nei vari comparti delle catene di produzione aziendale. Ma negli ultimi anni ha trovato ampia diffusione per la grande varietà di applicazioni cui si presta.

⁹ E. FLEISCH, C. FRANZ, A. HERRMANN, *The digital pill. What everyone should know about the future of our healthcare system*, Emerald Publishing, Bingley 2021, pp. 25 ss.; ed anche, C. RIJCKEN, *Reinforests of wearable and insideables*, in ID. (a cura di), *Pharmaceutical care in digital devolution*, Elsevier, London 2021, p. 110.

¹⁰ L.A. MARSCH, S.E. LORD, J. DALLERY, *Behavioral healthcare and technology*, Oxford University Press, Oxford 2015, p. 83.

¹¹ R. MARANI, A.G. PERRI, *Principali Applicazioni Biomedicali della Tecnologia RFID*, in *La Comunicazione. Note, Recensioni e Notizie*, 63, 2020, pp. 2 ss.

A differenza dei più comuni codici a barre, le etichette RFID possono gestire contemporaneamente diverse identità, memorizzano molte più informazioni e sono in grado di misurare anche fattori esterni all'elemento monitorato.

Le etichette RFID altro non sono che microchip dotati di un'antenna integrata per comunicazioni *wireless* che comunicano a distanza con i lettori che acquisiscono i dati e li trasmettono ad un server in modo che siano processati e analizzati. Il sistema RFID non prevede nessun impiego di batterie o fonti fisiche di alimentazione per funzionare¹².

Questa tecnologia si presta alla creazione di applicazioni orientate all'identificazione delle persone, al monitoraggio, mediante sensori appositi, dei parametri vitali ed, in generale, viene presentata come uno strumento in grado di migliorare la qualità della vita, specie in settori come quello sanitario, in cui sono necessarie attività di controllo costante.

Essa ha raggiunto oggi un livello di maturità tale da poter essere utilizzata per l'impianto di etichette intelligenti biocompatibili all'interno del corpo che porteranno, in futuro, allo sviluppo di applicazioni sempre più avanzate¹³.

5. I risvolti bioetici l'Internet dei corpi. Tutela dei dati e consenso.

Ebbene, la convergenza tra assistenza sanitaria e tecnologia solleva diverse preoccupazioni circa le conseguenze legali ed etiche dell'uso di strumenti che collegano l'uomo ad Internet.

L'Internet dei corpi, inteso come evoluzione dell'Internet delle cose, rappresenta una rete aperta di oggetti intelligenti che funzionano in totale autonomia, condividono informazioni, e sono in grado di reagire di fronte a cambiamenti dell'ambiente circostante¹⁴.

L'uso di queste tecnologie prevede la creazione e la manipolazione di grandi quantità di dati, noti come *Big data*, che possono riguardare ogni aspetto della vita umana. E la gestione di questi *big data* può avere impatti

¹² L. BATTEZZATI, J.L. HYGOUNET, *RFID. Identificazione automatica a radiofrequenza*, Hoepli, Milano, 2006; ed anche A. BUSCEMI, *Nuove tecnologie per la prevenzione di errori nelle aziende sanitarie RFID (Radio Frequency Identifier)*, in *Rivista elettronica di diritto, economia, management*, 1, 2010, pp. 213-242.

¹³ S. AMATO, *Biodiritto 4.0: intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020, pp. 89-100.

¹⁴ S. MADAKAM, R. RAMASWAMY, S. TRIPATHI, *Internet of things (IoT): A Literature review*, in *Journal of Computer and Communications*, 3, 2015, pp. 164-173.

considerevoli sulla *privacy*, sulla sicurezza e sul benessere dei consumatori¹⁵.

L'Internet dei corpi mira a stabilire un flusso di comunicazioni dall'uomo alla macchina, sostanzialmente incontrollato, in cui i dati vengono scambiati tra ambienti, persone e oggetti attraverso la connettività di rete. Queste attività di monitoraggio sono registrate e processate, molto spesso nella totale inconsapevolezza dei soggetti interessati.

Un'applicazione generalizzata di questi strumenti potrebbe, dunque, avere profonde ricadute nell'individuazione e nella valutazione delle problematiche bioetiche di queste tecnologie. Dal punto di vista normativo, inoltre, l'attuale sistema di classificazione dei prodotti e dei rischi ad essi correlati appare insufficiente a garantire una reale protezione giuridica.

Una delle questioni più problematiche di utilizzo dell'Internet dei corpi è quella legata al diritto alla protezione dei propri dati personali.

In linea di principio, per utilizzare dispositivi medici intelligenti che siano rispettosi dei principi giuridici occorre fare riferimento alle disposizioni contenute nel Regolamento generale per la protezione dei dati (GDPR) n. 679/2016 in combinato disposto con la normativa nazionale sul consenso informato del paziente, contenuta nella l. 219 del 22 dicembre 2017. Queste norme stabiliscono il principio secondo il quale lo sviluppo della sanità digitale presuppone l'obbligo, normativo e deontologico, del rispetto dei dati personali¹⁶.

Secondo le disposizioni di legge, i dati devono essere trattati in modo lecito, equo e trasparente nei confronti degli interessati; raccolti per finalità determinate, esplicite e legittime; adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità del servizio che li gestisce. Inoltre, è necessario che i titolari del trattamento predispongano tutte le misure necessarie a garantire che la sicurezza dei dati trattati, l'anonimizzazione delle informazioni che non siano più utili allo scopo per cui sono stati raccolti, nonché la possibilità per l'interessato di revocare il consenso in qualsiasi momento.

Il consenso dell'interessato al trattamento, in questo contesto, si pone come un atto autorizzativo di per sé in grado di bilanciare i diversi interessi in gioco sulla base del principio per cui in una società come quella

¹⁵ N KSHETRI, *Big data's impact on privacy, security and consumer welfare*, in *Telecommunications Policy* 38, 2014, pp.1134–1145.

¹⁶ F. CARCHIDI, *Profili di diritto civile della sanità e dell'assistenza: consenso informato e autonomia negoziale etico-algoritmica*, in *BioLaw Journal*, 4, 2022, pp. 443-444; P.B. HELZEL, A. SERGIO (a cura di), *La bioetica come ponte tra società e innovazione*, Aracne, Roma, 2016.

dell'informazione, che ha portato la nascita di nuovi diritti che ridefiniscono l'integrità stessa della persona, l'antico principio dell'*habeas corpus* legato alla libertà personale, in termini di autodeterminazione fisica, diviene oggi anche autodeterminazione digitale.

Il consenso rappresenta il diritto del paziente di scegliere, accettare o anche rifiutare consapevolmente i trattamenti (diagnostici-terapeutici) che gli vengono proposti, dopo essere stato pienamente informato sulla diagnosi e il decorso previsto della malattia, sulle alternative terapeutiche (incluso il loro rifiuto), sulle loro conseguenze.

Tuttavia, la questione diviene più complessa quando si affronta il tema della telemedicina.

L'uso diffuso dei dati sanitari permesso dalle nuove tecnologie sta sviluppando nuovi fenomeni sociali legati agli inediti processi di condivisione e fruizione delle informazioni mediche, o comunque inerenti la salute, concessi dal web. E l'aggregazione e la standardizzazione delle informazioni sanitarie personali offerta dalla tecnologia digitale conferisce a queste informazioni un valore non solo scientifico, ma anche economico di grande rilievo, dando luogo alla necessità di garantire effettività ad un regime giuridico, che non dovrebbe fermare lo sfruttamento di queste informazioni a fini scientifici e terapeutici, ma che comunque deve reprimerne ogni altro impiego che non rispetti il doppio livello di controllo cui è subordinata la circolazione dei dati sensibili.

Il volume di dati che possono essere generati, elaborati e conservati nella fornitura dei servizi di Internet dei corpi porta, dunque, ad interrogarsi sulla effettiva efficacia delle leggi vigenti sulla protezione dei dati e sulla urgenza di provvedere ad una revisione del sistema di tutela prima che la crescita incontrollata di queste tecnologie diventi ingestibile¹⁷.

La protezione dei dati dei pazienti come tutela dello stesso diritto alla libertà della cura dovrebbe divenire un obiettivo primario per gli operatori sanitari ed innescare un processo culturale di cambiamento nell'organizzazione e nella gestione stessa dell'erogazione dei servizi¹⁸.

Per cui la sperimentazione di applicazioni dell'Internet dei corpi non dovrebbe basarsi solo sul consenso del paziente, ma dovrebbe porre delle garanzie certe e delle sanzioni effettive per le chi le viola, di modo che possano essere adottati degli standard tecnologici trasparenti e sicuri fin

¹⁷ B. PUHAN, S. GUPTA, *Ethical Challenges in the Internet of bodies*, in *India Business Law Journal* (<https://law.asia>), 2022.

¹⁸ C. CIAMPI, *La sicurezza dei dati personali sanitari*, in *Rivista elettronica di diritto, economia, management*, 3, 2014, pp. 26 ss.

dalla loro progettazione.

Ma gli elementi problematici di queste tecnologie sono ancora molti: bisognerebbe interrogarsi, infatti, su chi possiede i dati, con quale frequenza li raccoglie, come li utilizza, in considerazione anche del fatto che la digitalizzazione delle informazioni si proietta ontologicamente ben al di là dei singoli contesti nazionali¹⁹.

In relazione a tale ultimo aspetto suscita notevoli incognite la possibilità di utilizzare la rete per favorire la circolazione su scala mondiale dei dati sanitari legati all'esigenza di cura del soggetto che ne è titolare.

Permangono, ulteriormente, diversi dubbi sulla possibilità di revocare il consenso fornito al trattamento dei dati, specie nel caso dei dispositivi impiantabili, o sulla possibilità di vietare alle aziende proprietarie di vendere i dati trattati²⁰.

6. Il problema della sicurezza informatica nella gestione dei dati e delle tecnologie.

Il tema del trattamento dei dati in sanità è strettamente connesso, poi, al problema della cybersicurezza.

Le applicazioni dell'Internet dei corpi, infatti, sono esposte agli stessi difetti di sicurezza di qualsiasi altra tecnologia che memorizza le informazioni su *cloud*. Ma, data la particolare natura di questi dispositivi e dei dati che raccolgono, il rischio diventa particolarmente elevato e rilevante.

La vulnerabilità dei sistemi potrebbe consentire a parti non autorizzate di divulgare informazioni private, manomettere i dati o bloccare l'accesso degli utenti ai propri *account*. E, nel caso di alcuni dispositivi medici impiantati, eventuali attacchi informatici potrebbero potenzialmente manomettere tali sistemi fino a causare lesioni fisiche o addirittura la morte di una persona.

Per tale ragione, la gestione di tecnologie all'avanguardia in sanità dovrebbe essere sempre preceduta da una valutazione d'impatto preventiva supportata da un'attenta analisi dei rischi a fronte di presidi di

¹⁹ G. PREITE, *L'habeas data sanitario come diritto all'autodeterminazione digitale del paziente*, in *Rivista elettronica di diritto, economia, management*, 3, 2014, pp. 105 ss.

²⁰ T. SAHAMA, L. SIMPSON, B. LANE, *Security and Privacy in eHealth: is it possible? A sociotechnical analysis*, in AA.VV., *Proceedings of the 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services*, Helathcom, New York, 2013, pp. 249-253.

sicurezza tecnici e organizzativi che consentono lo svolgimento sicuro dell'erogazione del servizio.

In tal senso, una valida riflessione bioetica non può prescindere, quindi, da considerazioni che attengono alla implementazione di un nuovo modello organizzativo pubblico che sia maggiormente in linea con i principali standard di sicurezza internazionali e che garantisca lo svolgimento di analisi dei rischi con cadenze temporali ben determinate.

Ebbene, in Italia, allo stato attuale, l'utilizzo delle ICT in ambito sanitario presenta ancora diversi problemi che incidono in maniera negativa su una valida gestione della sicurezza.

Dal punto di vista strutturale, il modello di *e-Health* che è stato implementato fino ad oggi non ha comportato un vero cambiamento organizzativo funzionale alla digitalizzazione, ma rispecchia ancora il modello organizzativo tradizionale, con una rigida separazione di ruoli, di banche dati e di processi assistenziali.

La c.d. cartella clinica elettronica, che rappresenta l'elemento cardine alla base della sanità digitale, non è presente in tutte le realtà ospedaliere e, laddove presente, viene applicata soltanto in modo parziale; i *software* e gli applicativi informatici utilizzati dalle strutture sanitarie sono estremamente eterogenei, per cui non favoriscono l'interoperabilità e un controllo univoco dei sistemi informativi; i dati sanitari raccolti nelle cartelle cliniche elettroniche e nei fascicoli sanitari elettronici non sono allineati, per cui diventa molto difficile per il medico ricostruire la storia clinica del paziente.

Questa mancanza di condivisione dei dati limita fortemente la possibilità di creare una rete di collaborazione tra i medici delle varie branche specialistiche, annullando così la funzione che dovrebbe avere la sanità moderna di mettere i pazienti al centro dei percorsi di cura integrati²¹.

Inoltre, dal punto di vista giuridico, la normativa nazionale non ha definito i parametri di standardizzazione tecnica necessari affinché la documentazione digitale sanitaria sia uniformemente condivisibile su tutto il territorio nazionale, con un conseguente mancato coordinamento delle regioni e delle provincie autonome chiamate ad implementare, sul piano gestionale, le innovazioni informatiche.

Comprendere pienamente il valore della digitalizzazione in sanità per garantirne la sicurezza è, dunque, un problema di carattere organizzativo, prima che legale o tecnologico.

Gestire la sicurezza in organizzazioni molto complesse, come quelle

²¹ E. CHILELLI, *Sanità 4.0. Le sfide per un sistema sanitario sostenibile e inclusivo*, in *Rivista elettronica di diritto, economia, management*, 3, 2019, pp. 61-64.

2/2023

operanti nel settore sanitario, è certamente un'attività che richiede una particolare attenzione ed un approccio multidisciplinare e consapevole, basato sugli standard internazionali di riferimento e che, quindi, in tal senso tenga conto non solo degli aspetti normativi e tecnologici, ma anche degli aspetti metodologici, di processo e del fattore umano. Reagire prontamente per ridurre i rischi è un obiettivo imprescindibile, e non più una opzione di scelta, in un contesto nel quale le minacce cibernetiche alle reti, ai sistemi e ai dati sanitari evolvono sempre più rapidamente.

Parlando di sicurezza, fra l'altro, non può non menzionarsi il problema della compatibilità dei materiali tecnologici con il corpo umano.

Nel caso di tecnologie impiantabili, i nanomateriali e i nanoprodotto di cui questi strumenti sono composti presentano un grado di rischio di biocompatibilità che ad oggi non è compiutamente determinabile.

Gli studi fino ad oggi condotti sulla tossicità delle nanotecnologie hanno dimostrato che molte delle proprietà dei nanomateriali esaminate possono tradursi in rischi importanti per la salute umana. Non sono prevedibili quindi, al momento, le conseguenze a lungo termine di una interazione costante di questi strumenti con il corpo umano.

A questo occorre aggiungere i rischi derivanti dalla somministrazione di farmaci che contengono particelle ingegnerizzate i cui effetti oggi sono ancora poco conosciuti²².

7. Conclusioni

In questa prospettiva, l'introduzione e l'implementazione delle applicazioni dell'Internet dei corpi su larga scala non può prescindere da un'attenta valutazione che implica un giudizio importante con riguardo sia al rispetto della vita e dell'integrità fisica e psichica umana sia alle minacce alla libertà e alla autodeterminazione di ogni individuo.

Perdere la proprietà dei dati sulla propria salute potrebbe significare perdere la proprietà del proprio corpo, specie in un contesto tecnologico come quello attuale in cui ha preso il sopravvento l'appropriazione e la monetizzazione delle informazioni personali da parte delle piattaforme digitali, creando delle gravi asimmetrie di potere²³.

²² A.G. SPAGNOLO, V. DALOISO, *Aspetti critici delle nanotecnologie nella sperimentazione clinica e ruolo del Comitato di Etica*, in *Pratica Medica & Aspetti Legali*, 2, 2011, pp. 53-56.

²³ C.C. GOULD, *How democracy can inform consent: Cases of the Internet and Bioethics*, in *Journal of Applied Philosophy*, 2, 2019, pp. 173-191.

Il corpo sta diventando l'oggetto privilegiato di una biopolitica che nella globalizzazione, caratterizzata dall'importanza fondamentale dell'economia di libero mercato e del capitalismo, trova la sua massima espressione²⁴.

Per cui le pratiche innovative legate alla digitalizzazione in medicina richiedono una revisione dei concetti bioetici centrali di autonomia personale e consenso informato, esteso all'idea di responsabilità morale nel campo delle tecnologie mediche a eventi di futuro incerto²⁵.

La biopolitica non dovrebbe poter sottomettere le potenze vitali dell'individuo al solo fine di intensificare la produzione di ricchezza e di potere delle classi dominanti; le persone dovrebbero essere in grado di acconsentire a qualsiasi azione che possa incidere sulla propria libertà, in modo che l'azione stessa obbedisca all'equilibrio di proporzionalità tra le parti coinvolte e quindi essere considerata etica.

Questo perché se l'Internet dei corpi dovesse diventare la nuova normalità l'integrità del corpo umano potrebbe diventare sempre più dipendente da Internet, con una conseguente grave compromissione dei diritti e delle libertà fondamentali degli individui²⁶.

Come giustamente osservato dalla dottrina, si presenta come quanto mai opportuna ed urgente la necessità di favorire delle attività di mediazione finalizzate a conciliare le esigenze e le opinioni di tutte le parti sociali coinvolte nell'innovazione tecnologica che propone scenari dagli impatti imponderabili. L'applicazione di regole comportamentali ampiamente condivise appare indispensabile per affrontare i cambiamenti sociali portati dalle innovazioni tecnologiche mantenendo una visione del futuro saldamente incardinata sui valori del rispetto e della salvaguardia della dignità umana²⁷.

²⁴ Sul tema della biopolitica si veda F. ROSA, *La biopolitica nell'era di Internet*, in *Nòema*, 6-2, 2015, pp. 160-198; M. FOUCAULT, *La volontà di sapere*, Feltrinelli, Milano, 1988, p. 127; ed anche F. GROS, *Y-a-t-il un subject biopolitique?*, in *Nòema*, 4-1, 2013, pp. 31-42.

²⁵ E.G. GREBENSHCHIKOVA, P.D. TISHCHENKO, *Digitized Future of Medicine: Challenges for Bioethics*, in *Russian Journal of Philosophical Sciences* 2, 2020, pp. 83-103.

²⁶ M. EL-KHOURY, C.L. ARIKAN, *From the Internet of things toward the Internet of bodies. Ethical and legal considerations*, in *Strategic Change*, 3, 2021, pp. 307-314.

²⁷ Così, R. VONA, *Libertà ed etica delle biotecnologie*, in *Frontiere mobili*, 2014, pp. 347-359; E. SGRECCIA, *Manuale di bioetica. Fondamenti ed etica biomedica*, Vol. I, Vita e pensiero, Milano, 1999.



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

FERNANDA FAINI

Governare la tecnologia: società digitale, geometrie di potere e regolazione giuridica

ABSTRACT - The paper aims to reflect on the relationship between law and technology, examining the face of contemporary digital society, in order to analyze the current configuration of European legal regulation in this area, the peculiarities that characterize it and the directions that emerge for the future. In particular, the contribution examines the philosophical, ethical and legal model of governance of technology, capable of protecting the person and his rights, as it emerges in the light of the European regulation that has been taking shape in recent years, aimed at regulating the digital dimension in its various aspects (*Data Governance Act, Data Act, Digital Services Act, Digital Markets Act, Artificial Intelligence Act, etc.*), also paying attention to the changing geometries of power. European regulation denotes an evolution of law both in terms of the form of legal regulation and in terms of the substance of instruments provided by the legislature, which innovate traditional paradigms.

KEYWORDS - legal regulation - digital society - technology - data governance - algorithmic transparency

2/2023

FERNANDA FAINI*

Governare la tecnologia: società digitale, geometrie di potere e regolazione giuridica**

SOMMARIO: 1. *Le regole giuridiche nella società digitale* – 2. *Il nuovo volto del diritto: i mutamenti nella forma della regolazione giuridica* – 3. *Il contenuto innovativo del diritto: paradigmi, strumenti e soluzioni* – 3.1. *L'evoluzione del rapporto tra diritto e tecnologia: governance umanocentrica, incorporazione del diritto nella tecnica, supervisione e sorveglianza umana* – 3.2. *Trasparenza algoritmica: comprensibilità, explainability e contestabilità della tecnologia* – 3.3. *Data governance tra protezione e circolazione* – 3.4. *Revisione delle forme di tutela della persona* – 4. *Conclusioni: prospettive e scenari filosofico-giuridici della futura dimensione digitale*

1. Le regole giuridiche nella società digitale

Le tecnologie informatiche, che nel loro avvento hanno assunto il ruolo di strumento nelle mani dell'uomo, nel corso del tempo sono riuscite a superare la loro essenza ontologica di mero strumento e a divenire un mezzo poliedrico capace di determinare una profonda trasformazione nella stessa esistenza umana, accompagnata dall'emersione di nuove esigenze e dall'impatto sulle attività, sulle relazioni e sulle modalità di partecipazione alla vita pubblica, influenzando il progresso ed espandendo le possibilità dell'essere umano.

Il diritto, lo strumento con cui l'uomo da sempre regola la vita, è chiamato ad occuparsi di tali fenomeni, a disciplinare le tecnologie informatiche e a governare la dimensione digitale, al fine di tutelare i diritti e bilanciare interessi diversi e talvolta contrapposti, sanando i conflitti¹.

Nello svolgere la sua funzione il diritto è esposto a mutamenti e sconta le peculiarità dell'oggetto che mira a regolare, costituito dalla dimensione digitale; di conseguenza la regolazione è portata a mutare in conseguenza di una serie di aspetti.

Un primo aspetto deriva dall'oggetto della regolazione, dalla tecnologia stessa, cui si accompagna la presenza di un ecosistema di regole diverso da quello giuridico, ossia le regole applicate dal codice informatico

* *Research Fellow* e docente di informatica giuridica e diritto delle nuove tecnologie presso l'Università di Pisa, l'Università Cattolica del Sacro Cuore e l'Università Telematica Internazionale Uninettuno.

** Contributo sottoposto a valutazione anonima.

¹ Cfr. V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2003, pp. 89 ss.: «se il diritto si attegga alla società come un guanto alla mano, è inevitabile che la diffusione delle tecnologie informatiche influenzi il diritto».

(si parla di *lex informatica* o *digitalis*)². Le tecnologie sono dominate da codici, istruzioni e regole informatiche, capaci di condizionare il comportamento dell'uomo, dal momento che rendono possibili o meno azioni e interazioni, abilitandole o disabilitandole, definendone modi e vincoli, collegando effetti, determinando quali informazioni fornire all'utente e, di conseguenza, il grado di trasparenza e la conoscibilità per chi le utilizza. Al riguardo Lessig usa l'incisiva locuzione "*code is law*" per evidenziare l'aspetto regolatorio insito nel codice informatico³.

Pertanto la *lex informatica*, nel determinare ciò che è possibile tecnologicamente, ha la capacità di condizionare ogni altra forma di regolazione, compresa quella giuridica, e l'uomo, per mezzo dello strumento del diritto, deve essere capace di governarla. Le regole informatiche, infatti, sono prodotte dall'essere umano e, di conseguenza, l'uomo può intervenire sulle stesse per mezzo delle regole giuridiche: pertanto, al fine di non rendere tutto ciò che è tecnologicamente possibile, solo per questo, giuridicamente legittimo, ciò che è giuridicamente lecito costituirà un sottoinsieme del tecnologicamente possibile⁴. Nello svolgere la funzione regolatrice nei confronti della dimensione digitale, l'uomo, per mezzo del diritto, deve essere capace di governare la tecnologia, raggiungendo un difficile equilibrio basato sulla flessibilità e sull'adattabilità, idonee a garantire efficacia alle regole giuridiche e capaci di non limitare le potenzialità dell'evoluzione tecnologica, ma, allo stesso tempo, solidamente fondato sulla prevedibilità e sulla certezza del diritto, senza determinare il dominio della tecnologia sulla regolazione⁵.

² Al riguardo cfr. L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, 1999, pp. 501-546, che nel governo del ciberspazio delinea quattro fattori fondamentali: regole giuridiche, regole sociali, mercato e "il codice" (*lex informatica*). Sul rapporto tra diritto e *lex informatica* cfr., *inter alia*, G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, II ed., Giappichelli, Torino, 2010, pp. 37 ss.; G. SARTOR, *Internet e il diritto*, in C. DI COCCO–G. SARTOR (a cura di), *Temi di diritto dell'informatica*, IV ed., Giappichelli, Torino, 2020, 1 ss.; E. MAESTRI, *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars Interpretandi*, fasc. 1, 2017, pp. 15-28.

³ L. LESSIG, *Code and Other Law of Cyberspace*, Basic Books, New York, 1999. Al riguardo cfr. E. MAESTRI, *Lex informatica e soft law. Le architetture normative del cyberspazio*, in P. MORO – C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, FrancoAngeli, Milano, 2017, p. 172: «La fonte normativa, nel caso della regolamentazione giuridica, è il legislatore; nel caso della *Lex informatica*, invece, a costituire la fonte del codice è il programmatore informatico».

⁴ S. RODOTÀ, *Intervista su privacy e libertà*, a cura di P. CONTI, Laterza, Roma-Bari, 2005.

⁵ Cfr. V. FROSINI, *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981; V. ZENO-ZENCOVICH, *op. cit.*, pp. 89 ss.; G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Il diritto dell'informazione*

2/2023

In merito emergono problematiche ontologiche e giuridiche strettamente correlate alle caratteristiche tecniche che dominano la scena digitale, quali il meccanismo stesso di inferenze e correlazioni su cui si basano gli algoritmi, l'opacità e la correlata difficile intelligibilità da parte dell'essere umano (*black box*) nel *machine learning* e nel *deep learning*, la connessa difficoltà di motivazione dei risultati cui perviene la macchina, oltre a potenziali errori tecnici e *bias*⁶. Gli algoritmi, infatti, lungi dall'essere neutrali possono condurre a problematiche tecniche, ma anche a connessi problemi di ordine etico, sociale e giuridico: dipende, infatti, da come sono programmati, da cosa imparano, dalla presenza di eventuali errori e di dati privi di qualità, da *bias* e pregiudizi, dalle potenziali manipolazioni e dall'uso concreto degli uomini; di conseguenza possono essere forieri di discriminazioni, disuguaglianze, disparità.

La tecnologia, infatti, è protagonista solo teoricamente "neutrale", dal momento che nella sua valenza strumentale acquisisce il significato che gli uomini le conferiscono nell'utilizzarla, nonostante il diritto stesso ne persegua la neutralità negli atti di riferimento⁷; le tecnologie sono "lame a doppio taglio" secondo l'efficace configurazione di Bauman⁸. Di conseguenza nel contesto digitale possono emergere le asimmetrie e le disparità tipiche della società: la dimensione digitale può somigliare nel volto oscuro a quella analogica.

A questo primo aspetto che connota il rapporto tra diritto e tecnologia si lega un secondo profilo: nella dimensione digitale muta l'oggetto di

e dell'informatica, fasc. 4-5, 2012, pp. 831 ss.; G. CORASANITI, *Il diritto nella società digitale*, FrancoAngeli, Milano, 2018.

⁶ Per l'approfondimento di questi aspetti *infra*, § 3.

⁷ Il principio di neutralità sotto il profilo tecnologico è previsto esplicitamente nel considerando 27 del regolamento (UE) n. 910/2014, che ritiene auspicabile che gli effetti giuridici prodotti dal regolamento «siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti». In ossequio a tale principio il diritto deve rimanere neutro rispetto alla tecnologia senza riferirsi a livelli di sicurezza predeterminati o a tecnologie specifiche, limitandosi ad individuare l'obiettivo da perseguire senza indicare le modalità tecniche per perseguirlo. Il principio di neutralità tecnologica, che pervade la normativa europea e nazionale, si collega alla necessità di tutelare la concorrenza tra gli operatori di mercato, rispettare l'autonomia, garantire maggiore effettività e permettere l'adeguamento all'evoluzione tecnologica; G. FINOCCHIARO, *Diritto di Internet*, III ed., Zanichelli, Bologna, 2020, pp. 88 ss.

⁸ Cfr. Z. BAUMAN – D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, trad. it., GLF Editori Laterza, Roma-Bari, 2015, pp. 86 ss.; secondo Bauman le tecnologie come "lame a doppio taglio" sono pericolose da utilizzare perché tendono a colpire anche obiettivi non designati e possono servire a scopi non previsti e ad applicazioni non prefigurate.

regolazione, costituito da beni intangibili, i dati, diversi dalle *res corporales* cui il diritto è tradizionalmente abituato⁹. Oggetti e soggetti diventano digitali; i beni si trasformano in servizi; il radicato paradigma della proprietà viene scalzato dal paradigma dell'accesso ai dati, ai servizi, alla propria esistenza digitale¹⁰.

Pertanto nella realtà digitale contemporanea hanno assunto il ruolo di protagonisti i dati e le tecnologie capaci di estrarne valore come l'intelligenza artificiale, i cui elementi fondamentali risiedono proprio nei dati (l'"anima") e negli algoritmi (il "motore").

I dati sono la materia prima di cui si compone la dimensione digitale, costituendo un bene diverso dagli altri, in quanto sono suscettibili di essere utilizzati e sfruttati contemporaneamente e in luoghi diversi da un numero illimitato di soggetti, pur potendo l'accesso ad essi essere limitato dalla tecnica o dal diritto; non sono peraltro esauribili e vengono generati a ritmi esponenziali. La società odierna, dunque, assume la connotazione di *data society*, in quanto è intimamente pervasa dai dati finendo per coinvolgere e plasmare l'uomo stesso come un *data subject*¹¹; nella società digitale il benessere e lo sviluppo umano dipendono in modo significativo dai servizi basati sui dati.

Nell'evoluzione tecnologica e giuridica rileva un altro aspetto particolarmente significativo connesso alla centralità dei dati, della rete e della dimensione digitale, che caratterizza anche la contemporanea società dominata dalle tecnologie emergenti; lo sviluppo di Internet e, ancor più, del *web 2.0* delinea un modello di produzione paritetica, orizzontale e

⁹ Cfr. V. ZENO-ZENCOVICH, *op. cit.*, pp. 89 ss., che sottolinea come per secoli il giurista si sia confrontato con "la forza delle cose", di cui il paradigma è la proprietà.

¹⁰ La disponibilità e l'utilizzo temporanei di beni e servizi si impongono rispetto al tradizionale regime di proprietà; è il caso del *car sharing*, della fruizione di contenuti in *streaming* e, più ampiamente, dell'accesso ai servizi delle piattaforme digitali. Cfr. J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, trad. it., Mondadori, Milano, 2000; L. FLORIDI, *La rivoluzione dell'informazione*, trad. it., Codice edizioni, Torino, 2012, p. 15; S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, pp. 105 ss.; G. PASCUZZI, *Dematerializzazione*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, il Mulino, Bologna, 2016, p. 342: «Non è più corretto parlare di situazioni di proprietà e di possesso bensì di titolarità e di legittimazione».

¹¹ In merito alla società dell'informazione cfr., *inter alia*, M. CASTELLS, *The Information Age: Economy, Society and Culture*, 3 tomi, Blackwell, Cambridge-Oxford, 1996-1998; A. MATTELART, *Storia della società dell'informazione*, trad. it., Einaudi, Torino, 2002; G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, cit. In relazione alla *data society* cfr. F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis Lefebvre, Milano, 2019.

2/2023

collaborativa, basato sulla diffusione, sulla condivisione e sul riutilizzo, che si affianca ai consolidati modelli verticali basati sul paradigma dominicale e sul controllo di un'autorità centrale, generando nuove opportunità, ma anche inedite problematiche giuridiche; è il caso delle *distributed ledger technologies* (DLT) e della *blockchain*¹². I paradigmi della proprietà e del controllo di un'autorità centrale, caratteristici del diritto tradizionale, cedono a un approccio acefalo, transnazionale e maggiormente paritario, che impatta anche sullo spazio di riferimento e sui soggetti che concretamente producono regole.

Anche la dimensione dello spazio, infatti, subisce l'impatto della rivoluzione digitale e influisce, di conseguenza, sul diritto; muta il campo d'azione dei singoli e della società, con il superamento dei confini territoriali. Si affermano diverse coordinate spaziali, dovute alla dimensione globale di riferimento, priva di confini territoriali e "sovrani", che determina la rilevanza in materia del diritto sovranazionale.

Lo spazio/non spazio digitale porta a ridefinire sfera pubblica e privata ed emerge un nuovo assetto nelle geometrie di potere, in cui gli Stati sono depotenziati ed erosi nel loro potere sul mondo digitale a causa del territorio globale di azione e della presenza dei colossi tecnologici, "controllori del pedaggio di accesso alla vita digitale", favoriti dalla stessa dimensione sovranazionale del mondo digitale, dalla capacità di utilizzare il valore delle tecnologie, dalla libertà di commercio, dalle maglie ampie o dall'assenza di disposizioni adeguate alla tutela dei diritti nel mutato contesto¹³. I colossi tecnologici sono stati capaci di dominare la dimensione globale grazie alle possibilità e agli strumenti dell'autonomia contrattuale privata per mezzo della concreta regolazione dell'accesso ai servizi e alle utilità della rete, incidendo così sui diritti e sulle libertà dei singoli¹⁴.

Di conseguenza, mutano i soggetti che concretamente producono regole in un contesto di disintermediazione, in cui emergono nuove asimmetrie e squilibri di potere: con una provocazione le aziende *Big Tech*, quali Amazon, Apple, Facebook, Google, Microsoft, danno vita un ordine algoritmico in cui si atteggiavano da potere legislativo (dettano le regole), esecutivo (le applicano e le fanno rispettare) e giudiziario (monitorano e

¹² Cfr. G. SARTOR, *Internet e il diritto*, cit., pp. 1 ss.

¹³ Cfr. A. VENANZONI, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, in *Rivista italiana di informatica e diritto*, fasc. 1, 2020, pp. 8-9.

¹⁴ Cfr. M. MEZZA, *Algoritmi di libertà. La potenza del calcolo tra dominio e conflitto*, Donzelli, Roma, 2018, p. 62; C. ACCOTO, *Il mondo dato. Cinque brevi riflessioni di filosofia digitale*, Egea, Milano, 2017, p. 108.

giudicano le violazioni con sanzioni quali la sospensione o la disattivazione dell'*account*). Si tratta di regole ampiamente accettate, seppur più o meno consapevolmente, capaci di influire sulla vita quotidiana e sulle attività degli individui quanto le norme con efficacia vincolante prodotte dagli Stati; i nuovi "territori" costituiti dalle piattaforme digitali sono percepiti dalla collettività come spazi giuridici pubblici, sebbene privi di legittimazione democratica e guidati non dall'interesse pubblico, ma dal profitto economico¹⁵.

In tale contesto di riferimento, in cui il diritto sconta le peculiarità dell'oggetto di regolazione e deve confrontarsi con le mutate geometrie di potere della contemporaneità, negli ultimi anni prende forma un articolato *framework* giuridico a livello europeo diretto a disciplinare la dimensione digitale della vita umana, formato inizialmente prevalentemente da atti di *soft law*¹⁶ e, più di recente, da un insieme di regolamenti quali il *Data Governance Act* (regolamento UE 2022/868), il *Digital Services Act* (regolamento UE 2022/2065), il *Digital Markets Act* (regolamento UE 2022/1925), l'*Artificial Intelligence Act*, proposto il 21 aprile 2021 e il *Data Act*, proposto il 23 febbraio 2022.

Alla luce del rapporto tra diritto e tecnologia e del volto della società digitale contemporanea, il contributo intende riflettere e analizzare la configurazione odierna della regolazione giuridica europea in materia, le peculiarità che la connotano e le direzioni che emergono per il futuro. In particolare il contributo è teso ad esaminare il modello filosofico, etico e giuridico di governo della tecnologia, atto a tutelare la persona e i suoi diritti, che emerge alla luce della regolazione europea degli ultimi anni, tesa a disciplinare la dimensione digitale nei suoi diversi aspetti (*Data Governance Act*, *Data Act*, *Digital Services Act*, *Digital Markets Act*, *Artificial Intelligence Act*, etc.), ponendo attenzione anche al mutamento delle geometrie di potere e al ruolo svolto dai soggetti pubblici e privati.

¹⁵ In merito al problematico inquadramento delle piattaforme digitali quali spazi giuridici pubblici si rinvia alla vasta letteratura in materia; cfr., *inter alia*, G. DE GREGORIO, *From Constitutional Freedoms to Power: The Law of the Platforms. Protecting Fundamental Rights Online in the Algorithmic Society*, in *European Journal of Legal Studies*, 11(2), 2019, pp. 65-103; G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge, 2022; H. MICKLITZ–O. POLLICINO–A. REICHMAN–A. SIMONCINI–G. SARTOR–G. DE GREGORIO (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021.

¹⁶ *Infra*, § 2.

La regolazione europea, infatti, denota un'evoluzione del diritto sia sotto il profilo della forma e del "modo di esprimersi" del diritto¹⁷, sia sotto l'aspetto sostanziale delle soluzioni e degli strumenti concreti previsti dal legislatore, che innovano i paradigmi tradizionali¹⁸.

Nel trattare i due profili la constatazione di partenza è che il diritto e la regolazione giuridica nella dimensione digitale spesso hanno mostrato di essere imperfetti alla prova dei fatti sia nella forma che negli strumenti, rivelandosi spesso imperfetta la tutela dei diritti dell'uomo e della società di riferimento; di conseguenza il modello di governo della tecnologia delineato dal diritto deve riuscire nella complessa sfida di essere efficace e sostenibile nel peculiare contesto digitale, caratterizzato dagli aspetti sopra esaminati.

2. Il nuovo volto del diritto: i mutamenti nella forma della regolazione giuridica

Il diritto è teso a raggiungere un saggio bilanciamento tra diritti e interessi diversi per essere sostenibile nella dimensione digitale; alla luce dei connotati e delle caratteristiche della dimensione digitale, ciò è possibile solo con una *governance* efficace e abbracciando una visione transnazionale dei problemi, accompagnata dalla correlata necessità di garantire omogeneità nelle risposte offerte dai diversi ordinamenti, al fine di non generare discrasie tra la regola e ciò che intende regolare.

Sotto il primo profilo, l'esigenza di costruire una *governance* efficace emerge prepotentemente fin dagli anni '90 con l'istituzione di soggetti dotati di indipendenza e chiamati ad occuparsi della tutela di diritti e del bilanciamento tra interessi diversi: a livello nazionale con il d.lgs. 39/1993 viene istituita l'Autorità per l'informatica nella pubblica amministrazione (AIPA), attualmente Agenzia per l'Italia Digitale (AgID)¹⁹, con la legge 675/1996 nasce il Garante per la protezione dei dati personali, con la legge 249/1997 prende vita l'Autorità per le garanzie nelle comunicazioni (Agcom) e nasce anche l'Autorità Garante della Concorrenza e del Mercato

¹⁷ *Infra*, § 2.

¹⁸ *Infra*, § 3.

¹⁹ Negli anni è diventata il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA), ai sensi dell'art. 176 del d.lgs. 196/2003, il DigitPA, a seguito del d.lgs. 177/2009, e attualmente l'Agenzia per l'Italia Digitale (AgID), a seguito degli artt. 19-22 del d.l. 83/2012, convertito con modificazioni dalla legge 134/2012.

(AGCM), istituita con la legge 287/1990, che nelle sue attività si occuperà anche dei temi legati alla rete, alle nuove tecnologie e alle telecomunicazioni. Nell'applicazione concreta ed omogenea delle previsioni giuridiche e nel bilanciamento di diritti e interessi diversi, il ruolo delle autorità è fondamentale anche al fine di rispondere alle richiamate istanze di flessibilità e adattabilità, necessarie affinché le regole giuridiche possano essere efficaci ed effettive nella dimensione digitale e siano capaci di affrontare l'evoluzione tecnologica per mezzo dell'interpretazione dei principi e delle norme di riferimento.

Tale esigenza di *governance* si manifesta anche nei nuovi regolamenti europei, che prevedono l'istituzione di Comitati e gruppi di esperti a livello sovranazionale, chiamati a fornire assistenza e consulenza alla Commissione europea nell'applicazione uniforme delle norme contenute nei regolamenti; il *Data Governance Act* istituisce l'*European Data Innovation Board*²⁰, il *Digital Services Act* istituisce l'*European Board for Digital Services*²¹, il *Digital Markets Act* prevede un *high-level group for the Digital Markets Act*²² e l'*Artificial Intelligence Act* prevede l'*European Artificial Intelligence Board*²³.

In questa esigenza di *governance* emerge la necessità di recuperare uno spazio giuridico pubblico a protezione dei diritti e delle libertà della persona, alla luce dello squilibrio presente nella dimensione digitale a causa

²⁰ L'*European Data Innovation Board*, sotto forma di un gruppo di esperti, è costituito da rappresentanti delle autorità competenti di tutti gli Stati membri, del Comitato europeo per la protezione dei dati, del Garante europeo della protezione dei dati, dell'ENISA, della Commissione, dal rappresentante dell'UE per le PMI o da un rappresentante nominato dalla rete dei rappresentanti per le PMI e da altri rappresentanti di organi pertinenti di settori specifici nonché di organi con competenze specifiche della Commissione e degli spazi di dati pertinenti. Il Comitato europeo per l'innovazione in materia di dati consiglia e assiste la Commissione per i compiti previsti (art. 29 ss., regolamento UE 2022/868).

²¹ L'*European Board for Digital Services* è un gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari, che fornisce consulenza ai coordinatori dei servizi digitali e alla Commissione conformemente al regolamento per conseguire gli obiettivi previsti (art. 61 ss., regolamento UE 2022/2065).

²² L'*high-level group for the Digital Markets Act*, composto dalle reti e dagli organismi europei previsti dalla norma, può fornire alla Commissione consulenza nei settori di competenza dei suoi membri (art. 40, regolamento 2022/1925).

²³ L'*European Artificial Intelligence Board*, composto dalle autorità nazionali di controllo, di cui è prevista la designazione da parte degli Stati membri, e dall'*European Data Protection Supervisor*, è chiamato a fornire assistenza e consulenza alla Commissione, facilitando la cooperazione in materia, contribuendo agli orientamenti e alle analisi necessarie e assistendo le autorità nazionali di controllo e la Commissione europea nel garantire l'applicazione uniforme del regolamento, ai sensi dell'art. 56 ss., titolo VI, proposta di regolamento «*Artificial Intelligence Act*», COM(2021) 206 *final* del 21 aprile 2021.

2/2023

del potere assunto concretamente dai soggetti privati costituiti dalle aziende *Big Tech*; il rischio però consiste nel pericolo di far pendere la bilancia sull'uno o sull'altro diritto a protezione del quale o della tecnologia per la quale la specifica autorità è istituita e conseguentemente si muove, perdendo l'approccio olistico necessario per affrontare la complessità della dimensione digitale.

Il proliferare di organismi sovranazionali chiamati a contribuire all'applicazione efficace ed omogenea delle norme, infatti, seppur sia scelta condivisibile nello sforzo di individuare soggetti indipendenti dedicati al governo della dimensione digitale, determina la necessità conseguente di una sinergica cooperazione tra i diversi organismi, superando l'ambito settoriale di azione che rischia altrimenti di far smarrire quell'approccio olistico necessario per governare la dimensione digitale e le sue problematiche, dove le intersezioni tra l'oggetto dei diversi regolamenti sono evidenti; esemplificativamente se si parla di servizi digitali verrà in gioco anche la *data governance* e l'impiego eventuale di soluzioni di intelligenza artificiale, seppur siano oggetto di distinti regolamenti e di diversi organismi, che pertanto dovranno necessariamente interagire e cooperare tra loro.

Proprio l'esigenza di un approccio olistico è a fondamento del secondo aspetto (la logica transnazionale), dal momento che il livello cui guardare è necessariamente sovranazionale, quanto meno europeo: la realtà globale della rete, infatti, implica un mutamento nei confini geografici della regolazione e rende necessario arrivare a soluzioni condivise a livello sovranazionale e internazionale in merito alla protezione dei diritti, che nel web "vivono globalmente". La veste sovranazionale è necessaria a garantire efficacia alle norme, evitando la tensione altrimenti fisiologica tra la dimensione globale delle questioni e la dimensione territoriale delle disposizioni da applicare.

Sotto tale profilo, si manifesta fin dagli anni '90 l'impulso sovranazionale del legislatore europeo, cui conseguono in Italia numerosi e significativi atti normativi e che spinge nel nuovo millennio, in parallelo con la maggiore pervasività delle tecnologie nella vita umana, a regolare in modo sistematico e organico interi ambiti di disciplina: vengono emanati codici e testi unici, accompagnati dalla produzione di norme di rango secondario, regole tecniche e provvedimenti delle autorità indipendenti, istituite proprio per rispondere al bisogno di governare la tecnologia.

Nella società digitale odierna tali caratteristiche connotano il rapporto tra diritto e tecnologia, cui si sommano negli ultimi anni ulteriori profili che caratterizzano il volto del diritto sovranazionale, degni di osservazione.

Oltre all'estensione dell'ambito territoriale delle problematiche affrontate, tendenzialmente globale, nella regolazione di riferimento emergono anche l'ampiezza delle tecnologie, degli strumenti e dei temi oggetto di disciplina che si coniuga all'eterogeneità degli atti che ospitano le regole: non solo norme strettamente intese, *hard law*, ma anche *soft law*, atti di indirizzo, linee guida, analisi e strategie di soggetti istituzionali, autorità amministrative indipendenti, organismi, comitati, fino anche a *task force* e gruppi di esperti nominati *ad hoc*; la complessità dei fenomeni è affrontata con strumenti eterogenei prodotti non solo delle istituzioni pubbliche competenti, ma anche da soggetti privati e dalla stessa società²⁴.

Nel disciplinare la tecnologia, infatti, il diritto deve tener conto di ecosistemi di regole diverse, come quelle informatiche, che dettano "legge" nella dimensione digitale, e, altresì, quelle poste nell'ambito dell'autonomia privata dai colossi tecnologici, che regolano i "territori" costituiti dalle estese piattaforme digitali. Al fine di essere efficace, infatti, la regolazione giuridica deve essere capace di integrare i diversi ecosistemi di regole della società digitale e, di conseguenza, necessita di una genesi *multilevel*, di un approccio *multistakeholder* e dell'integrazione di fonti eterogenee, al fine di avvalersi dei diversi portatori di interessi e di una conseguente corresponsabilità da parte dei differenti produttori di norme, giuridiche o meno, della nostra contemporaneità: poteri pubblici, ma anche poteri privati, capaci di dettare regole di accesso all'esistenza digitale. Pertanto, accanto alle norme poste dalle autorità pubbliche, rilevano forme di *co-regulation* e di *self-regulation*, dove le regole sono poste da parte degli stessi destinatari delle stesse, come nel caso delle aziende *Big Tech* e della *lex*

²⁴ A. SIMONCINI, *Verso la regolamentazione della Intelligenza Artificiale. Dimensioni e governo*, in *BioLaw Journal*, fasc. 2, 2021, p. 412: le norme di *hard-law* «rappresentano un sistema di regole dotate di piena obbligatorietà in senso giuridico, ovverosia suscettibili, in caso di violazione, di applicazione giudiziaria e di esecuzione forzata. La *soft-law*, invece, è un sistema di regole non precettive, comunque caratterizzato da un diverso grado di persuasività, ovverosia in grado di svolgere effettivamente una funzione di orientamento e di indirizzo nei confronti dei loro destinatari, sebbene non suscettibili di attuazione giudiziaria». Al riguardo l'Autore sottolinea che la scelta di un sistema di governo coordinato di fonti diverse risiede nel grave deficit di effettività che ad oggi sconta il sistema normativo in questi ambiti.

*mercatoria*²⁵; in tale contesto gli Stati sono chiamati a nuove forme di cooperazione e collaborazione.

L'eterogeneità della tipologia degli atti deriva proprio dalle caratteristiche dell'oggetto di regolazione: la tecnologia è connotata dalla specificità tecnica, dal progresso scientifico e dall'evoluzione costante, che esigono qualificate competenze tecniche e comportano l'esigenza di atti puntuali, regole tecniche e strumenti flessibili per affrontarla, mentre la norma ontologicamente si caratterizza per essere generale e astratta, frutto di un lungo *iter* scaturente dal processo democratico e tesa a durare nel tempo²⁶. Di conseguenza, in materia è necessario un complesso articolato di regole diverse, atte a costruire una disciplina complessivamente sostenibile e, a tal fine, tese a garantire flessibilità e adattabilità allo sviluppo e ai cambiamenti della tecnologia, ma capaci di non rinunciare e assicurare prevedibilità e certezza del diritto, principi solidi della regolazione giuridica²⁷.

Nel quadro regolatorio europeo emerge questa tensione continua fra flessibilità e prevedibilità, al fine di garantire efficacia ma anche certezza, tutelando la persona e riuscendo a trovare un virtuoso equilibrio tra diritti, istanze e interessi diversi.

L'esigenza di garantire flessibilità e adattabilità rispetto all'incessante sviluppo tecnologico e la conseguente necessità di aggiornamento determinano nelle norme meccanismi di flessibilità, quali la valutazione e il riesame nel regolamento UE 2022/2065 (*Digital Services Act*) e nel regolamento UE 2022/1925 (*Digital Markets Act*), ma altresì nell'*Artificial Intelligence Act* l'obbligo generale di revisione del regolamento e la procedura di verifica e modifica degli allegati connessi all'individuazione delle categorie dei sistemi ad alto rischio, anche al di fuori del procedimento legislativo ordinario altrimenti necessario; nella stessa ottica è possibile leggere le previsioni relative all'attivazione del meccanismo delle *regulatory*

²⁵ U. DRAETTA, *Internet nel diritto internazionale*, in G. FINOCCHIARO – F. DELFINI (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, 13 comprende nel concetto di *lex mercatoria* «quel complesso di principi generali, clausole *standard* e modelli contrattuali applicabili alle relazioni commerciali internazionali e sviluppatasi su base consuetudinaria nell'ambito della comunità degli operatori economici internazionali a partire dal secondo dopoguerra».

²⁶ Cfr. E. D'ORLANDO, *Politica, tecnica e scienza: il sistema delle fonti di fronte al dilemma della complessità*, in *Diritto amministrativo*, fasc. 4, 2021, pp. 731 ss.

²⁷ Cfr. C. CASONATO – B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal*, fasc. 3, 2021, pp. 417-418.

sandboxes, utili ad adattare le disposizioni a una realtà particolarmente complessa²⁸. Nella stessa direzione può essere, altresì, interpretato il ricorso allo strumento dei codici di condotta per contribuire alla corretta applicazione delle norme, che ricorre nel *Digital Services Act*²⁹ e nell'*Artificial Intelligence Act*³⁰.

L'esigenza di prevedibilità e certezza del diritto, insieme alla necessità di garantire omogeneità di soluzioni, determinano il cambiamento stesso di approccio da parte dell'Unione europea con la tendenza negli ultimi anni a "inasprire" la forza degli atti normativi assunti a livello sovranazionale (da *soft law* ad *hard law*), al fine di garantirne effettività; è il caso del regolamento europeo che con la sua maggiore *vis* sugli Stati membri negli ultimi anni prende il posto della direttiva. L'Unione europea dà vita a un *framework* regolatorio composto da un quadro di regolamenti finalizzati a disciplinare la dimensione digitale della vita umana, quali il *Data Governance Act* (regolamento UE 2022/868), il *Digital Services Act* (regolamento UE 2022/2065), il *Digital Markets Act* (regolamento UE 2022/1925), l'*Artificial Intelligence Act*, proposto il 21 aprile 2021 e il *Data Act*, proposto il 23 febbraio 2022³¹.

Al riguardo è opportuno precisare che non si rinuncia all'eterogeneità di atti, necessaria a garantire effettività alle norme: in tali disposizioni, infatti, si rinvia anche ad atti di *soft law* necessari per l'applicazione delle disposizioni, come i richiamati codici di condotta.

Inoltre, seppur l'atto formale scelto per gli atti deputati a regolare la dimensione digitale sia il regolamento e non la direttiva, nei diversi atti, oltre agli esaminati meccanismi di flessibilità, sono lasciati ampi margini di applicazione agli Stati membri, che equilibrano la maggior forza dell'atto con l'esigenza di garantire anche adattabilità ed efficacia, seppur tale profilo possa causare anche incertezze e potenziali difformità nell'attuazione³².

²⁸ L'attivazione del meccanismo delle *regulatory sandboxes* consente agli Stati membri, per un periodo di tempo limitato e sotto il controllo delle autorità competenti nazionali, di sviluppare e sperimentare sistemi di intelligenza artificiale innovativi, ai fini di una successiva immissione nel mercato; art. 53 ss., titolo V, proposta di regolamento «*Artificial Intelligence Act*», COM(2021) 206 *final* del 21 aprile 2021.

²⁹ Art. 45 ss., regolamento UE 2022/2065.

³⁰ Art. 69 ss., proposta di regolamento «*Artificial Intelligence Act*», COM(2021) 206 *final* del 21 aprile 2021.

³¹ Tale tendenza ad abbandonare lo strumento della direttiva in favore del regolamento era già in atto da alcuni anni, si pensi al regolamento europeo 2016/679 sui dati personali e al regolamento europeo 2018/1807 sui dati non personali.

³² Nell'*Artificial Intelligence Act*, ad esempio, l'individuazione dei sistemi a rischio inaccettabile si connota per la presenza di concetti indeterminati ed interpretabili, che

3. Il contenuto innovativo del diritto: paradigmi, strumenti e soluzioni

Accanto a questi profili che riguardano il mutamento nella forma del diritto e nel suo esprimersi, nel quadro di regolazione europea degli ultimi anni sono contenute soluzioni e strumenti, che indicano le direzioni future e costituiscono i paradigmi innovativi della regolazione a livello sostanziale in materia, permettendo di ravvisare un contenuto innovativo del diritto.

Nel quadro regolatorio europeo degli ultimi anni, innanzitutto, oltre alla tipologia di atto e alla forma di regolazione, muta significativamente anche l'approccio sostanziale, dal momento che si sceglie di regolare e influire sulle geometrie di potere della dimensione digitale e cambia l'incisività sui diversi attori in gioco, dal momento che si intende promuovere l'innovazione, lo sviluppo e la competitività, ma anche proteggere in modo più efficace gli utenti e i loro diritti sulla scena digitale, istituendo un quadro di regole in materia di trasparenza e responsabilità, individuando obblighi a carico dei poteri economici privati. In tal senso si pongono il *Digital Services Act* (regolamento UE 2022/2065) e il *Digital Markets Act* (regolamento UE 2022/1925), che prevedono doveri di diligenza e trasparenza nei confronti degli utenti, dispongono obblighi di predisposizione di meccanismi di segnalazione da parte degli utenti e individuano responsabilità e sanzioni.

Il legislatore europeo si mostra consapevole che, al fine di costruire un solido modello di governo della tecnologia necessario a governare la società digitale, ispirato ai principi etici e ai valori degli ordinamenti democratici, è necessario superare le problematiche esistenti che emergono dal rapporto tra diritto e tecnologia e dall'oggetto di regolazione costituito dalla dimensione digitale, che a guardare bene trovano fondamento in una serie di aspetti, quali:

- le criticità insite nel funzionamento stesso della tecnologia, dei dati e degli algoritmi;
- il significativo squilibrio tra le parti in gioco, in particolare la debolezza della persona nelle sue vesti di utente e consumatore nei confronti dei colossi tecnologici;
- l'opacità e la chiusura dei processi di gestione dei dati sia da parte dei soggetti pubblici che di quelli privati;
- la conseguente incapacità del singolo di potersi tutelare in modo efficace da solo.

implica flessibilità applicativa e margini di manovra a favore degli Stati membri, ma anche possibile incertezza nell'applicazione e correlate potenziali difformità nell'attuazione.

Proprio dalle criticità emergono anche le possibili soluzioni, contenute nel quadro regolatorio europeo che caratterizzerà la futura dimensione digitale e capaci di innovare i paradigmi tradizionali e minimizzare i rischi, riequilibrando le asimmetrie a favore della collettività e proteggendo in modo efficace la persona attraverso forme diverse di tutela.

Il modello di governo della tecnologia che emerge dal quadro regolatorio europeo fa leva su alcuni nuovi strumenti, soluzioni e paradigmi, capaci di innovare profondamente il diritto, oggetto di analisi insieme agli aspetti problematici e alle criticità che li connotano.

3.1. *L'evoluzione del rapporto tra diritto e tecnologia: governance umanocentrica, incorporazione del diritto nella tecnica, supervisione e sorveglianza umana*

Un primo aspetto che emerge dal *framework* giuridico europeo riguarda il rapporto tra diritto e tecnologia, che muta e matura.

La direzione intrapresa poggia sulla costruzione di una *governance* umanocentrica, capace di conferire piena centralità alla persona, per tutelare la quale è necessario un adeguato contesto istituzionale e un bilanciamento mobile tra diritti in una logica che mantenga la tecnologia strumento nelle mani dell'uomo. L'approccio orientato a una *governance* umanocentrica emerge dagli atti a livello sovranazionale; è sufficiente pensare agli atti di *soft law* e *hard law* relativi all'intelligenza artificiale³³. Emerge un approccio olistico, in cui la persona con la sua identità funge da prisma i cui riflessi sono costituiti dai diversi diritti in gioco, indivisibili, seppur nella loro conflittualità.

Tale approccio umanocentrico può essere realizzato e implementato concretamente sfruttando la tecnologia stessa e la relazione tra regole giuridiche e regole informatiche; il diritto può avvalersi della tecnica per garantire il suo rispetto.

Sotto tale profilo la recente regolazione europea abbraccia un approccio preventivo e proattivo, che prende forma in due profili sinergici e strettamente connessi: l'incorporazione del diritto nella tecnica e il *risk-based approach*.

³³ Prima di arrivare alla proposta di regolamento sull'intelligenza artificiale, dal 2018 l'Unione europea ha dedicato una serie di atti al tema, quali comunicazioni, piani, raccomandazioni, orientamenti.

Negli atti europei degli ultimi anni emerge come paradigma capace di risolvere o quanto meno minimizzare le problematiche che affliggono il rapporto tra diritto e tecnologia, infatti, il paradigma dell'incorporazione preventiva di principi etici e giuridici, norme e rimedi nella tecnologia stessa, ossia una *legal protection by default* e *by design*, basata sull'*accountability*, presente fin dal regolamento europeo 2016/679 in materia di protezione dei dati personali³⁴. Il diritto può avvalersi della tecnologia per garantire il suo rispetto, generando un modello di "diritto nella tecnica" (*code is law – law is code*). Si tratta di un approccio proattivo, che tutela la persona fin dalla progettazione, per impostazione predefinita e per mezzo della valutazione d'impatto, capace di far leva sulla conformazione dei sistemi tecnologici e sulla sicurezza, da una parte, e sulla responsabilizzazione e sulla consapevolezza dei soggetti, dall'altra, al fine di confinare le repressioni prevalentemente *ex post* alla tutela sanzionatoria successiva, senza reprimere eccessivamente la libera circolazione dei dati e lo sviluppo economico.

Tale prospettiva è ulteriormente sviluppata nell'*Artificial Intelligence Act*, che si basa su un approccio proattivo basato sul rischio, coadiuvato anche da un correlato sistema sanzionatorio, e sulla sua categorizzazione preventiva, distinguendo quattro categorie, cui si collega una regolazione differenziata: rischio inaccettabile, alto, basso, minimo.

Il *risk-based approach*, che mira a una protezione preventiva, capace di ridurre o eliminare la probabilità stessa delle violazioni, è abbracciato dall'Unione europea per la capacità di raggiungere un equilibrio nella tutela dei diversi interessi in gioco, dal momento che è teso alla tutela dei diritti della persona, ma è anche orientato alla crescita economica e al mercato, giacché il produttore di soluzioni di intelligenza artificiale può considerare la *legal compliance* come un costo di produzione che entra nel costo economico della propria attività piuttosto che affrontare l'alea di dover eventualmente rispondere di violazioni³⁵. Nel caso dell'intelligenza artificiale il sistema di responsabilità distingue in base alle categorie di operatori di sistemi di intelligenza artificiale ad alto rischio o meno; la responsabilità dell'operatore può essere giustificata dal fatto che sta controllando un rischio associato alla specifica tecnologia. Tale approccio proporzionato al rischio e teso a differenziare parallelamente il regime

³⁴ Si tratta dei principi *data protection by design* e *by default*, cui si affianca il *data protection impact assessment* (artt. 25 e 35, regolamento UE 2016/679).

³⁵ Cfr. A. SIMONCINI, *Verso la regolamentazione della Intelligenza Artificiale. Dimensioni e governo*, cit., pp. 413 ss.

regolatorio è consapevole della pluralità ed eterogeneità delle soluzioni tecnologiche di intelligenza artificiale, in cui può variare sensibilmente l'autonomia che le connota, la trasparenza che è possibile garantire e il controllo umano esercitabile. Anche il concetto del rischio, del resto, emerge fin dal regolamento in materia di *data protection* e dagli strumenti ivi previsti.

L'approccio proattivo, che prende vita nell'incorporazione preventiva del diritto nella tecnica e nell'approccio basato sul rischio, non è scevro da criticità, da affrontare al fine di assicurare un'implementazione sostenibile del modello di governo della tecnologia, quali in particolare la "rigidità" ontologica del codice informatico stesso, che si scontra con la flessibilità necessaria al bilanciamento "mobile" idoneo a una tutela efficace ed effettiva dei diritti, oltre a un'opacità linguistica, dal momento che il linguaggio è informatico e non è quello naturale delle norme giuridiche³⁶. L'altra problematica di tale prospettiva sta nel fatto che in tal modo il rispetto dei principi giuridici e l'equilibrio tra diritti sono di fatto delegati a coloro che sono chiamati a sviluppare le soluzioni tecnologiche e alle categorie di operatori nel mercato con conseguenti possibili rischi.

Il mutamento e la maturazione del rapporto tra diritto e tecnologia prende forma anche in un terzo aspetto da garantire nel rapporto che lega l'uomo e la macchina, ossia la supervisione e sorveglianza umana, la non esclusività della decisione algoritmica della macchina. In tale direzione, nella regolazione dedicata all'intelligenza artificiale, la necessità di mantenere servente la tecnologia rispetto all'uomo emerge nell'attenzione che viene tributata alla supervisione e alla sorveglianza umana, tesa a prevenire e minimizzare rischi e pericoli, in linea con l'approccio proattivo e preventivo che connota il modello di *governance* della tecnologia; tale profilo emerge prepotentemente anche nelle sentenze nazionali relative all'impiego di algoritmi in ambito pubblico³⁷.

³⁶ G. LO SAPIO, *La trasparenza sul banco di prova dei modelli algoritmici*, in *federalismi.it*, fasc. 11, 2021, pp. 242 ss.

³⁷ Il caso riguardava l'utilizzo di un sistema informatico, basato su algoritmi, da parte del Ministero dell'Istruzione nell'assegnazione delle sedi nei procedimenti di mobilità dei docenti nella scuola; l'algoritmo ha condotto a decisioni particolarmente discutibili, che, di conseguenza, sono state contestate dagli interessati e hanno determinato una serie di sentenze di particolare interesse per i principi in esse espressi. Cfr., *inter alia*, TAR Lazio, sez. III bis, 21 marzo 2017, n. 3742; TAR Lazio, sez. III bis, 22 marzo 2017, n. 3769; TAR Lazio, sez. III bis, 10 settembre 2018, nn. 9224-9930; Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270; TAR Lazio, sez. III bis, 27 maggio 2019, n. 6606; TAR Lazio, sez. III bis, 13 settembre 2019, nn. 10963-10964; Consiglio di Stato, sez. VI, 13 dicembre 2019, nn. 8472-8474;

Al fine di costruire un modello antropocentrico, infatti, è necessario mantenere equilibrio tra la componente umana e la componente macchina, attraverso la garanzia dello “*human in the loop*”; al riguardo rileva il fatto che la tecnologia non è più soltanto un mezzo per realizzare azioni, ma sempre più spesso è essa stessa a prendere autonomamente decisioni significative per la persona umana e la sua libertà.

A tal fine l’*Artificial Intelligence Act* prevede misure concrete da applicare per garantire una sorveglianza umana sostanziale ed evitare il rischio che concretamente la decisione umana possa essere “attratta” dai risultati della macchina; il problema, infatti, sta nelle influenze e nella capacità “attrattiva” a livello pratico che la soluzione offerta dalla macchina può avere e nella correlata difficoltà per l’uomo che se ne serve di discostarsi con la propria valutazione da quanto emerge dal sistema tecnologico, finendo per conformarsi al risultato suggerito: in tal modo, di conseguenza, si svuota sostanzialmente l’autonomia della decisione umana³⁸.

Al riguardo però occorre interrogarsi se e come sia possibile conciliare la garanzia della supervisione e della sorveglianza umana con sistemi di *machine* e *deep learning*, capaci di apprendere autonomamente, che operano secondo processi decisionali opachi e non prevedibili per gli stessi programmatori, rispetto ai quali pertanto devono essere verificate le effettive possibilità per l’uomo di mettere in discussione i risultati cui perviene la macchina, controllare la correttezza dei dati e correggere gli *output*. A ben vedere l’*explainability*, tra poco oggetto di analisi, costituisce anche la condizione necessaria per la supervisione umana e per l’eventuale correzione del funzionamento del sistema, dal momento che solo se l’essere umano è in grado di comprendere il modo in cui il sistema di intelligenza

Consiglio di Stato, sez. VI, 4 febbraio 2020, n. 881; TAR Lazio, sez. III bis, 24 giugno 2021, n. 7589.

³⁸ Art. 14, proposta di regolamento «*Artificial Intelligence Act*», COM(2021) 206 *final* del 21 aprile 2021, che prevede misure atte a consentire a chi è affidata la sorveglianza umana di comprendere e interpretare il sistema di intelligenza artificiale, intervenire sul funzionamento del sistema o interromperlo, decidere in modo autonomo se utilizzarlo e «restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull’output prodotto da un sistema di IA ad alto rischio (“distorsione dell’automazione”)». In tal senso A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, fasc. 4, 2019, 1149 ss., secondo cui quando viene inserito un automatismo decisionale in un procedimento deliberativo, l’automatismo tende ad attrarre la decisione, diventando difficile prescindere e rendendo nella pratica “servo” l’uomo, che ne è teoricamente “padrone”.

artificiale decide, può operare un controllo effettivo e, se necessario, correggerne gli *output*³⁹.

3.2. *Trasparenza algoritmica: comprensibilità, explainability e contestabilità della tecnologia*

Sinergicamente a tali aspetti, al fine di superare l'opacità e la chiusura dei processi di gestione dei dati, è necessario garantire nella dimensione digitale una declinazione rafforzata della trasparenza, una trasparenza sostanziale algoritmica che assicuri conoscibilità, comprensibilità e sindacabilità, rendendo gli algoritmi oggetto della piena cognizione e del pieno sindacato dal parte del giudice: tale principio si traduce nell'assicurare non solo informazioni e accesso ai dati, ma anche la conoscenza della logica degli algoritmi, accompagnata dalla consapevolezza in merito alle conseguenze e all'impatto sulla persona.

Nei confronti di dati, algoritmi e intelligenza artificiale, pertanto, devono essere attribuiti e riconosciuti il diritto alla comprensibilità, capace di informare e rendere consapevole l'interessato, e il diritto alla contestabilità, idoneo a consentire all'interessato, anche per mezzo di un giudice, di valutare e di sindacare la decisione a cui perviene la tecnologia. Tali diritti si traducono più ampiamente nel diritto del singolo di mantenere la propria autonomia e autodeterminazione nei confronti della macchina: questo diritto comporta l'esigenza di comprensione dei meccanismi di funzionamento e una sorta di correlato dovere di "spiegare" in capo alla soluzione di intelligenza artificiale o, meglio, in capo a chi ne è responsabile⁴⁰. Secondo il Consiglio di Stato, nell'utilizzo di algoritmi nell'attività della pubblica amministrazione deve essere osservato un

³⁹ B. MARCHETTI, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in *BioLaw Journal*, fasc. 2, 2021, pp. 367 ss.

⁴⁰ Cfr. A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, fasc. 1, 2019, 7. Al riguardo G. CARULLO, *Decisione amministrativa e intelligenza artificiale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2021, pp. 445 ss. sottolinea, come precisato anche nella relativa giurisprudenza amministrativa nazionale afferente all'impiego di algoritmi in ambito pubblico, che l'esame del codice sorgente è elemento essenziale per la comprensione della decisione, dal momento che permette di verificare se le regole informatiche scritte in fase di programmazione dell'algoritmo applichino fedelmente il dettato normativo; pertanto il codice sorgente in quanto testo deve essere considerato, di norma, parte integrante della motivazione, insieme alla documentazione tecnica relativa al codice sorgente stesso.

nuovo meta-principio di legalità algoritmica, che si declina nei principi di conoscibilità e comprensibilità (trasparenza algoritmica), non discriminazione algoritmica e non esclusività della decisione algoritmica (il necessario coinvolgimento umano, *human in the loop*)⁴¹.

A livello europeo l'attenzione alla trasparenza algoritmica è presente fin dal regolamento 2016/679 in materia di *data protection*, dal momento che il titolare del trattamento è tenuto a fornire all'interessato, tra le informazioni necessarie per garantire un trattamento corretto e trasparente, «l'esistenza di un processo decisionale automatizzato, compresa la profilazione [...] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»⁴². Su tali informazioni esiste, altresì, un diritto di accesso, riconosciuto all'interessato esplicitamente dall'art. 15 del regolamento (UE) 2016/679.

L'*Artificial Intelligence Act* mostra particolare attenzione per la trasparenza, che secondo le disposizioni europee deve essere "appropriata", e dispone siano fornite informazioni chiare e adeguate all'utente sia in caso di sistemi "ad alto rischio", sia in caso di sistemi "a basso rischio". Il regolamento europeo, infatti, prevede che ogni sistema ad alto rischio sia disegnato e sviluppato in modo da assicurare un appropriato livello di trasparenza (*sufficiently transparent*)⁴³, mostrando in tal modo consapevolezza circa la necessità di misure proporzionate, senza imporre obblighi irrealizzabili alla luce delle caratteristiche tecnologiche, come tali destinati ad una concreta inefficacia⁴⁴. Emerge con evidenza sotto tale profilo l'esigenza di sostenibilità del diritto, più volte richiamata.

Nel quadro regolatorio europeo, alla trasparenza algoritmica si accompagna la necessaria trasparenza da parte di chi governa gli algoritmi stessi, coniugandosi pertanto l'esigenza di trasparenza delle macchine con la necessità di una correlata trasparenza da parte degli uomini che le gestiscono; in tal senso rilevano le disposizioni del *Digital Services Act* (regolamento UE 2022/2065), che impongono alle piattaforme doveri di trasparenza e diligenza in merito agli algoritmi utilizzati, essendo tenute ad obblighi di motivazione nei confronti degli utenti e alla valutazione dei

⁴¹ Consiglio di Stato, sez. VI, 13 dicembre 2019, n. 8472. Sul meta-principio di legalità algoritmica cfr., altresì, A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, cit., pp. 1149 ss.

⁴² Art. 13, paragrafo 2, lett. f) e art. 14, paragrafo 2, lett. g), regolamento (UE) 2016/679.

⁴³ Art. 13, proposta di regolamento «*Artificial Intelligence Act*», COM(2021) 206 *final* del 21 aprile 2021

⁴⁴ Cfr. C. CASONATO – B. MARCHETTI, *op. cit.*, pp. 426 ss.

rischi sistemici collegati⁴⁵. L'esigenza di garantire trasparenza è presente e sottesa anche alle disposizioni del regolamento UE 2022/1925 (*Digital Markets Act*), che pone obblighi in capo ai *gatekeeper*⁴⁶, nella consapevolezza che le condizioni alle quali i *gatekeeper* forniscono servizi pubblicitari online agli utenti commerciali, compresi inserzionisti ed editori, risultano spesso opache e poco trasparenti⁴⁷.

La trasparenza degli algoritmi e di coloro che li governano garantisce il rispetto del diritto alla comprensione, alla spiegabilità e alle correlate sindacabilità e contestabilità, valorizzando, in tal modo, il ruolo della persona: garantire che l'uomo possa comprendere la macchina assicura che l'intelligenza artificiale rimanga strumentale rispetto a quella umana e la tecnologia mantenga la sua funzione "servente" rispetto all'uomo e alle sue decisioni, soprattutto laddove incidano su diritti e libertà.

Al riguardo, la natura degli algoritmi pone il problema se esista sempre una logica comprensibile, dato il funzionamento degli stessi e la conseguente possibile non intelligibilità secondo criteri logico-razionali⁴⁸. L'autonomia, infatti, connota e differenzia l'intelligenza artificiale dalla logica dei software tradizionali, dove l'impostazione deterministica *if this, than that* indica un funzionamento del tutto predeterminato nel programma, che prevede gli *input* e gli *output*: proprio in questo aspetto si scorge la natura "intelligente" della macchina, che è capace di apprendere attraverso i dati in modo autonomo. Nell'apprendimento automatico (*machine learning*), infatti, anziché fornire tutta la conoscenza alla macchina, l'uomo le fornisce un metodo di apprendimento, da applicare ai dati cui la macchina ha accesso, per estrarre automaticamente da quei dati le indicazioni su come svolgere il compito ad essa affidato⁴⁹. Negli algoritmi

⁴⁵ Artt. 4, 34 e 35, regolamento UE 2022/2065.

⁴⁶ Il *gatekeeper* è «un'impresa che fornisce servizi di piattaforma di base, designata a norma dell'articolo 3», ossia che «a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro» (artt. 2, paragrafo 1, n. 1, e 3, paragrafo 1, regolamento UE 2022/1925).

⁴⁷ Considerando 45, regolamento UE 2022/1925.

⁴⁸ Cfr. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, fasc. 1, 2019, pp. 77 ss.; A. SIMONCINI – S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di Filosofia del diritto*, fasc. 1, 2019, pp. 97 ss.

⁴⁹ F. LAGIOIA–G. SARTOR, *L'intelligenza artificiale per i diritti dei cittadini: il progetto Claudette*, in *Ragion pratica*, fasc. 1, 2020, pp. 88 ss. sottolineano come i sistemi di intelligenza artificiale

2/2023

di *machine learning* e *deep learning* l'intelligenza artificiale stessa estrapola le nozioni necessarie per l'assunzione di una determinazione, analizzando grandi quantità di dati ed apprendendo da questi i parametri numerici (la rappresentazione matematico-numerica, il cosiddetto modello, generato nella fase di apprendimento o *training*), necessari per adottare decisioni e utilizzarli nella successiva fase di esecuzione⁵⁰; il modello solitamente non è direttamente intelligibile da parte dell'essere umano (*black box*), aspetto che rileva particolarmente sotto la lente giuridica, come sarà più avanti osservato⁵¹.

Pertanto, l'approccio dell'intelligenza artificiale non è fondato su spiegazioni causali e logico-deduttive, tipiche del ragionamento umano, basato su ipotesi predeterminate e nessi di causalità, ma si affida a connessioni e inferenze tra dati e poggia sull'approccio statistico e sulla probabilità, determinando talvolta difficoltà di comprensione circa le motivazioni (il "perché") delle risposte fornite⁵².

Pertanto garantire la trasparenza algoritmica può essere particolarmente complesso a fronte di una congenita opacità che caratterizza gli algoritmi, che si declina in un'opacità strutturale, derivante dal funzionamento degli stessi e dal fatto che resta non comprensibile persino ai programmatori l'iter logico seguito dalla macchina per giungere al risultato partendo dai dati a disposizione, cui si somma l'opacità

abbiano fatto un vero salto di qualità, dando luogo a numerose applicazioni di successo in diversi settori, quando l'attenzione si è spostata dalla rappresentazione logica della conoscenza alla possibilità di applicare metodi di apprendimento automatico a grandi masse di dati. In tale contesto negli anni più recenti hanno avuto particolare rilevanza le tecniche di apprendimento profondo (*deep learning*), basate su reti neurali a molti strati, che riproducono alcune caratteristiche astratte del cervello umano.

⁵⁰ L'apprendimento automatico da parte della macchina può essere o meno supervisionato dall'uomo, ossia può o meno ricevere indicazioni dall'esterno; l'analisi dei dati consiste in un processo di approssimazione, che genera il rischio di trarre conclusioni imprecise e discriminatorie, laddove i dati non siano corretti o non siano debitamente annotati, in modo da poter essere correttamente utilizzati e interpretati dalla macchina.

⁵¹ Tali algoritmi si differenziano dagli algoritmi condizionali o deterministici (*if this, than that*), che si limitano ad applicare regole informatiche predefinite ed espresse in linguaggio di programmazione. Cfr. G. CARULLO, *op. cit.*, pp. 434 ss.

⁵² In tal senso A.C. AMATO MANGIAMELLI, *Intelligenza artificiale, big data e nuovi diritti*, in *Informatica e diritto*, fasc. 1, 2022, pp. 9 ss.; C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, numero speciale, 2019, pp. 101-130; P. MORO, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *Rivista di diritto dei media*, fasc. 3, 2019, p. 19; A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, cit., pp. 1149 ss.; A. SIMONCINI – S. SUWEIS, *op. cit.*, p. 92.

linguistica già precedentemente richiamata, dovuta al linguaggio informatico e non a quello naturale⁵³.

Tale aspetto può risultare particolarmente problematico in caso di utilizzo dell'intelligenza artificiale in ambiti giuridici quali l'amministrazione pubblica e la giustizia, dal momento che sia i provvedimenti amministrativi (art. 3, legge 241/1990) sia quelli giurisdizionali (art. 111, comma 6, Costituzione) devono essere necessariamente accompagnati da una motivazione; l'opacità delle motivazioni di un provvedimento amministrativo o giurisdizionale impedisce qualsiasi controllo sull'esercizio della funzione, potendo portare all'annullamento delle decisioni impugnate sotto tale profilo⁵⁴.

3.3. Data governance *tra protezione e circolazione*

Un altro paradigma che emerge nella regolazione europea e caratterizza il modello di governo della tecnologia attiene all'oggetto stesso della regolazione, ossia i dati.

Nel *framework* giuridico europeo la *governance* dei dati oscilla tra protezione/controllo a tutela dei diritti del singolo e circolazione/apertura dei *big data*⁵⁵ (*open big data*) sia in ambito pubblico che privato alla luce dei benefici conseguibili per la collettività, con una spinta recente verso la circolazione e l'apertura – e anche verso la prospettiva della valorizzazione economica e della commercializzazione dei dati –, dal momento che l'apertura, insieme alla trasparenza, può contribuire in modo decisivo a sanare le asimmetrie informative, mettendo a disposizione della collettività i dati.

L'apertura dei dati è capace di determinare una “sanatoria” in direzione di democratizzazione, provocando una perdita di potere per i detentori degli stessi, valorizzando la natura di beni comuni non solo di dati e informazioni, ma anche degli interessi generali oggetto di protezione come trasparenza, democrazia, sviluppo economico, culturale e sociale. La ricostruzione come *open big data* si attaglia alla qualificazione dei dati come beni collettivi e a titolarità diffusa, dei quali possiedono quelle caratteristiche di non esclusività e non rivalità, al netto di concrete pretese

⁵³ G. LO SAPIO, *op. cit.*, pp. 242 ss.

⁵⁴ Cfr. C. CASONATO, *op. cit.*, pp. 119 ss.

⁵⁵ I *big data* consistono in enormi volumi di dati, provenienti da fonti diverse e analizzati per mezzo di algoritmi, *data mining*, *big data analytics*, *machine learning* e altre tecniche.

2/2023

di appropriazione e restrizioni surrettizie capaci di renderli di fatto “proprietà” di pochi soggetti. In conformità alla loro natura di “beni comuni” necessitano di una capacità di disposizione da parte della comunità che può tradursi nel diritto al riutilizzo da assicurare per mezzo dell’apertura dei dati nel rispetto dei diritti.

In tale direzione, accanto alle norme e alle strategie tese all’apertura dei dati in ambito pubblico⁵⁶, di recente rilevano la comunicazione della Commissione europea «*Una strategia europea per i dati*», COM(2020) 66 final del 19 febbraio 2020, che mostra consapevolezza circa il fatto che il valore dei dati risiede nel loro utilizzo e riutilizzo e dell’esistenza di squilibri in termini di potere di mercato, e il regolamento UE 2022/868 sulla *governance* europea dei dati, il *Data Governance Act*, volto a promuovere la disponibilità dei dati utilizzabili, rafforzando la fiducia negli intermediari di dati e potenziando i meccanismi di condivisione dei dati in tutta l’Unione europea, che integra la direttiva (UE) 2019/1024 del 20 giugno 2019. In questa direzione si pone anche il *Data Act*, proposto il 23 febbraio 2022, che abbraccia un approccio *as open as possible and as closed as necessary*⁵⁷.

In merito al governo dei dati, accanto a tale spinta verso la circolazione e l’apertura, nella riflessione si affaccia la ricerca di nuove forme di tutela del singolo che giunge anche alla prospettiva della valorizzazione economica dei dati personali, ossia l’attribuzione agli stessi di un valore economico, fino alla loro commerciabilità e monetizzazione.

⁵⁶ A livello normativo rileva la direttiva 2003/98/CE del 17 novembre 2003, dedicata al riutilizzo dell’informazione nel settore pubblico, modificata dalla direttiva 2013/37/UE del 26 giugno 2013. Al fine di poter sfruttare pienamente il potenziale dell’informazione del settore pubblico a vantaggio dell’economia e della società, è stata adottata la direttiva (UE) 2019/1024 del 20 giugno 2019, relativa all’apertura dei dati e al riutilizzo dell’informazione del settore pubblico, che ha provveduto, per mezzo della tecnica della rifusione, alla revisione della direttiva 2003/98/CE, modificata dalla direttiva 2013/37/UE. A livello strategico al riguardo è particolarmente significativa anche la comunicazione della Commissione europea «*Dati aperti – Un motore per l’innovazione, la crescita e una governance trasparente*», COM(2011) 882 def. del 12 dicembre 2011.

⁵⁷ Il *Data Act* prevede alcune misure quali la condivisione dei dati da impresa a consumatore e da impresa a impresa; l’obbligo di rendere accessibili i dati generati dall’uso di prodotti o servizi correlati agli utenti che hanno diritto di accedere ai dati; il diritto degli utenti di accedere ai dati generati dall’uso di prodotti o servizi correlati e di utilizzarli; obblighi per i titolari dei dati tenuti per legge a mettere a disposizione i dati; l’obbligo per i titolari di dati di mettere a disposizione di enti pubblici e istituzioni i dati sulla base di necessità eccezionali; l’eliminazione degli ostacoli all’effettivo passaggio da un fornitore di servizi di trattamento dei dati a un altro; l’interoperabilità e le garanzie nei contesti internazionali; etc.

Nella riflessione recente, rinvigorita anche da interventi normativi e giurisprudenziali⁵⁸, il dato personale si staglia come un diamante dai diversi riflessi: oggetto di un diritto fondamentale con i connessi connotati di indisponibilità, imprescrittibilità e assolutezza, ma anche base fondamentale su cui si erge la dimensione digitale che come tale può assumere e di fatto assume anche valore economico come controprestazione, anche alla luce del fatto che costituisce preziosa risorsa per le attività svolte dalle piattaforme digitali. A ciò si legano i diversi ruoli assunti dal soggetto: interessato sotto il profilo della protezione dei dati personali e utente/consumatore nell'accesso al servizio digitale. Pertanto emerge la natura ambivalente dei dati personali, considerati ora come oggetto di un diritto fondamentale, ora come bene di natura economica⁵⁹.

L'ambivalenza del resto è presente nella stessa normativa in materia di protezione dei dati personali, posta a presidio sia della tutela degli interessati sia della libera circolazione dei dati, come emerge fin dalla denominazione stessa del regolamento 2016/679⁶⁰. Sotto tale profilo il diritto anela e persegue il bilanciamento, ma si trova nella dimensione digitale di fronte alla tensione tra protezione e controllo, che connotano la tradizionale ottica giuridica proprietaria europea a tutela dei diritti, e circolazione e apertura, che emergono nella regolazione europea recente e arrivano a spingersi finanche alla valorizzazione economica e alla commerciabilità dei dati.

Oltre alle previsioni del regolamento 2016/679⁶¹, nell'interpretazione del dato personale come bene che può essere valorizzato economicamente rileva anche la direttiva 2019/770, recepita dagli artt. 135-octies e seguenti del d.lgs. 206/2005, che prevede la propria applicazione anche nel caso in cui, anziché un prezzo, il consumatore fornisca o si impegni a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dal professionista

⁵⁸ *Infra*, più avanti nel testo.

⁵⁹ Cfr. S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws – Rivista di diritto dei media*, n. 3, 2019, pp. 146 ss.

⁶⁰ Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

⁶¹ Art. 1, comma 3, regolamento UE 2016/679: «La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali». Al riguardo rilevano, altresì, i considerando 4, 6, 9 e 10 e il diritto alla portabilità dei dati, riconosciuto agli interessati, di cui all'art.20, regolamento UE 2016/679.

ai fini della fornitura del contenuto digitale o del servizio digitale o per consentire l'assolvimento degli obblighi di legge cui è soggetto il professionista e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti⁶².

La soluzione di compromesso raggiunta nella versione finale del testo della direttiva evita l'utilizzo del termine controprestazione con riguardo ai dati personali, precisando anzi che i dati non possono essere «considerati una merce», e riafferma in ogni caso la prevalenza della normativa in materia di protezione dei dati personali; la normativa precisa che i dati personali non devono essere intesi propriamente come una controprestazione a favore dell'operatore economico, ma come la prestazione di un consenso al loro trattamento, da esprimersi secondo la normativa di riferimento. Tale soluzione pare essenzialmente nominalistica, in quanto, a prescindere dalla qualifica formale dei dati come controprestazione, il caso in cui un servizio sia erogato a fronte del consenso al trattamento resta parificato, a livello di disciplina, a quello in cui è previsto un corrispettivo in denaro⁶³. A livello normativo rileva anche la direttiva 2019/2161/UE, che prende espressamente atto del fatto che i contenuti digitali e i servizi digitali sono spesso forniti online attraverso contratti che prevedono, da parte del consumatore, «la comunicazione di dati personali al professionista»⁶⁴.

Al riguardo nell'ottica della valorizzazione economia del dato personale rileva, altresì, la vicenda mossa dall'Autorità Garante della Concorrenza e del Mercato (AGCM) *versus* Facebook (provvedimento del 29/11/2018, n. 27432) con le correlate sentenze del TAR Lazio (sentenza del 10/01/2020 nn. 206 e 261) e del Consiglio di Stato (sentenze del 29/03/2021 n. 2630 e n. 2631), dove si rinviene una chiara apertura all'approccio negoziale dei dati personali⁶⁵. Le sentenze del Consiglio di Stato parlano di “messa a

⁶² Art. 135-octies, d.lgs. 206/2005.

⁶³ Art. 3 e considerando 24, direttiva 2019/770; cfr. S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., pp. 135 ss.

⁶⁴ La normativa, in coerenza con le previsioni della direttiva 2019/770, interviene sulla direttiva 2011/83/UE per estendere le tutele previste per le forniture di servizi digitali in cambio di denaro anche alle ipotesi di contratti di servizi digitali nel cui ambito il consumatore fornisce al professionista dati personali senza pagare alcun prezzo, dal momento che «data la loro somiglianza e la loro interscambiabilità», i servizi digitali a pagamento e i servizi digitali forniti contro dati personali devono essere soggetti alle stesse norme.

⁶⁵ Al riguardo cfr. A. LEONE, *Servizi digitali zero price e diritti dei consumatori*, in *Il Diritto Industriale*, n. 3, 2022, pp. 233 ss. e F. MIDIRI, *Proteggere i dati personali con le tutele del consumatore*, in *Giornale di diritto amministrativo*, n. 5, 2021, pp. 609-620.

disposizione dei dati” e muovono verso «l’esigenza di garantire “tutele multilivello”», capaci di ampliare i diritti della persona, protetta nella dimensione informativa in senso stretto dal regolamento UE 2016/679 e nella dimensione commerciale dalla disciplina consumeristica, interpretando di conseguenza le norme in materia di *data protection* e quelle a tutela del consumatore in termini di complementarietà e non di esclusione reciproca⁶⁶.

Il riconoscimento della negoziabilità dei dati assume la meritoria finalità di mettere in luce e sottrarre il trattamento all’opacità che oggi caratterizza i cosiddetti mercati impliciti, in cui i dati personali divengono oggetto di appropriazione e sfruttamento al di fuori di un esplicito rapporto contrattuale⁶⁷.

A frenare la prospettiva della valorizzazione economica dei dati personali, però, oltre alle caratteristiche che connotano il diritto e che creano un argine alla qualifica come bene di scambio (assoluto, indisponibile, intrasmissibile, imprescrittibile) e allo stretto rapporto tra il dato personale e la persona con la sua identità, che non gli permetterebbe di compierne atti di disposizione, è opportuno sottolineare che il diritto alla protezione dei dati personali non ha un contenuto omogeneo e meramente individuale ed è anzi volto in via strumentale a tutelare interessi eterogenei, che vanno oltre quelli dei singoli interessati di volta in volta coinvolti, ossia non rappresenta in sé un bene finale da tutelare, ma è strumentale alla tutela di altri interessi. Tali interessi non sono solo di natura individuale, ma riguardano anche la collettività; nella disciplina di riferimento il diritto alla protezione dei dati personali tutela interessi individuali, ma è fortemente presente l’esigenza di tutela anche di interessi collettivi⁶⁸. In quest’ottica, la limitazione dello sviluppo di un mercato di dati personali può essere

⁶⁶ Secondo le parole del Consiglio di Stato si tratta di «un diritto personalissimo [...] “sfruttato” a fini commerciali, indipendentemente dalla volontà dell’interessato-utente-consumatore». Secondo il TAR Lazio la cessione dei dati è qualificabile come «contro-prestazione del servizio offerto dal *social network*, in quanto dotati di valore commerciale». Al riguardo, come espresso dal Consiglio di Stato, anche secondo il TAR Lazio le due normative si pongono «in termini di complementarietà, imponendo, in relazione ai rispettivi fini di tutela, obblighi informativi specifici, in un caso funzionali alla protezione del dato personale, inteso quale diritto fondamentale della personalità, e nell’altro alla corretta informazione da fornire al consumatore al fine di fargli assumere una scelta economica consapevole».

⁶⁷ E. BATTELLI, *Negoziabilità dei dati personali e modelli di valorizzazione economica*, in *Rivista di diritto dell’impresa*, n. 1, 2022, p. 29.

⁶⁸ S. THOBANI, *Il mercato dei dati personali: tra tutela dell’interessato e tutela dell’utente*, cit., pp. 144 ss.; F. MIDIRI, *Proteggere i dati personali con le tutele del consumatore*, cit., pp. 609-620.

interpretata come volta in buona parte alla tutela di interessi collettivi con lo scopo di evitare che la raccolta di una mole di informazioni determini effetti pregiudizievoli per la società con il rischio di classificazione e discriminazione degli individui, alterando gli equilibri disposti dalla normativa europea e, in particolare, dal regolamento europeo 2016/679⁶⁹.

Ad avviso di chi scrive il pericolo nella valorizzazione economica e nella commerciabilità dei dati personali sta soprattutto nel fatto che le presunte maggiori tutele richiamate a suo sostegno sono sempre confinate in un rapporto bilaterale come quello contrattuale, che nella tutela effettiva ha scricchiolato (si pensi al consenso) e che in tale contesto si ripropone applicando le regole contrattuali, sollevare la cui violazione di nuovo è compito rimesso all'utente, soggetto debole. In considerazione del fatto che l'obiettivo è garantire maggiore tutela all'interessato, il rischio è di aumentare o meglio diversificare le possibilità di tutela della persona grazie a strumenti contrattuali, ma rimanendo sempre nel rapporto bilaterale e quindi ponendo sempre in capo ad un soggetto debole le tutele e la possibilità di azionarle. Nel quadro europeo si manifesta una tendenza ad attribuire all'interessato il controllo dei propri dati, con lo scopo di realizzare una sorta di "*data subject empowerment*", rendendolo soggetto attivo e, di conseguenza, maggiormente libero. Ma proprio questo desta dubbi alla luce delle sorti che ha avuto il consenso a livello concreto.

Forse invece, anche in considerazione del diritto di cui si tratta e delle ricadute a cascata sull'applicazione di una serie di norme e, più ampiamente, sul modello di *governance*, oltre all'attenzione ai pericoli della mercificazione, può essere opportuno riflettere piuttosto sulla costruzione di un'autodeterminazione collettiva che, consapevole dei valori collettivi in gioco ma anche degli effetti collettivi che ogni operazione anche singola può avere, immagini forme di negoziazione e tutela collettiva, decidendo *ex ante* ed *ex post* anche al posto del soggetto⁷⁰.

3.4. *Revisione delle forme di tutela della persona*

Proprio alla luce degli interessi collettivi in gioco, insieme ai profili esaminati, nel quadro regolatorio europeo si affaccia anche una revisione delle forme di tutela del singolo. L'attuale significativo squilibrio tra le parti

⁶⁹ Cfr. G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Il Diritto dell'informazione e dell'informatica*, fasc. 3, 2020, pp. 635-674.

⁷⁰ *Infra*, § 3.4.

nella dimensione digitale, infatti, si traduce nel rischio di “solitudine” del singolo, spesso inconsapevole e in ogni caso incapace di potersi tutelare in modo efficace da solo.

I valori della dignità, dello sviluppo della persona e dell’uguaglianza a fronte delle possibili discriminazioni, che gli algoritmi sono capaci di realizzare, interessano tutta la collettività e la loro violazione danneggia non solo il singolo che ne è vittima, ma l’intero ordinamento democratico; parimenti, di conseguenza, può essere opportuno dare forma concreta alla capacità di disposizione della collettività attraverso una tutela collettiva dell’individuo, che non si sostituisca, ma si affianchi a quella individuale⁷¹. Del resto la “massa”, grazie alle inferenze algoritmiche, orienta in modo automatizzato decisioni e predizioni anche laddove il singolo non si riconosca e se ne discosti: nelle configurazioni odierne dei dati e degli algoritmi emerge l’impatto collettivo e sociale del loro utilizzo⁷². Si tratta di uno scenario che valorizza la natura di beni comuni non solo di dati e informazioni, ma anche degli interessi generali oggetto di protezione come trasparenza, democrazia, sviluppo.

Alla luce di tali aspetti e della congenita debolezza dello strumento del consenso individuale, la dimensione collettiva di tutela dei diritti può tradursi nell’introduzione di strumenti di negoziazione e protezione collettiva: può configurarsi una forma di autodeterminazione informativa della collettività e forme di tutela collettiva dei diritti, capaci di coadiuvare quelle individuali, in linea con l’approccio preventivo e tecnologico esaminato, che decide *by design* e *by default*, al posto del singolo, al fine di tutelarlo. In concreto la negoziazione collettiva potrebbe coadiuvare l’autonomia negoziale del singolo, vietando per mezzo di norme imperative alcune operazioni anche se il consenso sussiste (ad esempio nel caso in cui ne consegua una violazione di diritti) o imponendole anche se manca (ad esempio al fine di perseguire un interesse generale): si tratterebbe di deroghe *in melius* al consenso individuale⁷³. Del resto la normativa, che si basa sui regolamenti europei 2016/679 e 2018/1807 e si erge sulla dicotomia tra dato personale e dato non personale, rischia di non essere adeguata alla dimensione digitale, dal momento che i *big data* si nutrono di disponibilità

⁷¹ Cfr. A. MANTELEO, *I Big Data nel quadro della disciplina europea della tutela dei dati personali*, in *Il Corriere giuridico*, ed. speciale, 2018, pp. 54 ss.

⁷² Cfr. «*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*», adottate il 23 gennaio 2017 dal Comitato consultivo della Convenzione 108.

⁷³ M.F. DE TULLIO, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, fasc. 4, 2016, pp. 665 ss.

2/2023

e utilizzo dei dati, mentre la *data protection* aspira al controllo dei dati e anche alla “chiusura” degli stessi se necessaria a tutela della persona. Il concetto stesso di dato personale può essere insufficiente, come nel caso di dati afferenti a gruppi o comunità sulla cui base possono essere prese decisioni che incidono anche sul singolo che non ha prestato il consenso e non ha ceduto dati personali.

Tale approccio, che si traduce nell’autodeterminazione informativa della collettività e in forme di tutela collettiva dei diritti, è teso a ristabilire uno spazio giuridico pubblico, si concilia con l’autodeterminazione individuale per rafforzarla e permette di evitare rischi di mercificazione della persona.

Un riferimento significativo al riguardo è contenuto nella disciplina in materia di protezione dei dati personali e, in specifico, nell’art. 80 del regolamento (UE) 2016/679, secondo paragrafo, che attiene al momento della protezione della persona a seguito di una violazione e si traduce in un’esperibile direzione di tutela della stessa: la protezione è liberata dalla necessità di azione da parte dell’individuo stesso e può essere attivata da organizzazioni e associazioni nel momento in cui siano violati quei “beni pubblici” e quei valori collettivi protetti dalla disciplina⁷⁴.

In tale direzione può essere letto anche il regolamento UE 2022/868 (*Data Governance Act*), che prevede il consenso all’utilizzo dei dati per scopi altruistici e il consenso all’utilizzo di dati personali con l’aiuto di un “servizio di intermediazione di dati”, il cui compito consiste nell’aiutare i singoli individui a esercitare i propri diritti a norma del regolamento⁷⁵.

4. Conclusioni: prospettive e scenari filosofico-giuridici della futura dimensione digitale

⁷⁴ «Gli Stati membri possono prevedere che un organismo, organizzazione o associazione [...], indipendentemente dal mandato conferito dall’interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all’autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti di cui un interessato gode a norma del [...] regolamento siano stati violati in seguito al trattamento» (art. 80 del regolamento UE 2016/679, secondo paragrafo).

⁷⁵ Il “servizio di intermediazione dei dati” è «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, all’altro, anche al fine dell’esercizio dei diritti degli interessati in relazione ai dati personali», ad esclusione dei servizi previsti dalla norma (art. 2, paragrafo 1, n. 11, regolamento UE 2022/868). I servizi di intermediazione dei dati sono regolati dall’art. 10 e seguenti del regolamento UE 2022/868.

Le prospettive indicate, che emergono dal *framework* giuridico europeo degli ultimi anni (rapporto tra diritto e tecnologia basato sulla *governance* umanocentrica, sull'incorporazione del diritto nella tecnica e sulla supervisione e sorveglianza umana; trasparenza algoritmica, *explainability* e contestabilità della tecnologia; *data governance* tra protezione e circolazione; revisione delle forme di tutela della persona) permettono di ridurre le esaminate problematiche che affliggono il rapporto tra diritto e tecnologia. Innanzitutto tali soluzioni intervengono sulle asimmetrie e sull'opacità contribuendo a "svelare" preventivamente problemi, consentendo di progettare la soluzione tecnologica in modo diverso. E poi trasparenza, apertura e forme collettive di tutela permettono di intervenire *ex post*, laddove il problema non sia emerso *ex ante*, consentendo di proteggere in modo efficace la persona.

Alla luce di tali profili, il modello giuridico che prende forma nella regolazione in materia si serve della tecnologia, che può previamente implementare principi e valori etico-giuridici, deve essere comprensibile e connotata dalla sorveglianza umana sostanziale, oltre a basarsi sul *risk-based approach*, sulla *governance* e sull'*accountability* da parte di chi governa la tecnologia; l'insieme di questi strumenti e misure è teso a risolvere o quanto meno a stemperare le problematiche giuridiche relative.

Nel quadro regolatorio europeo emerge un'evoluzione del diritto, capace di servirsi della tecnica per i propri scopi, dirigendola con approccio etico verso i valori della società democratica del futuro: emerge prepotentemente l'esigenza di recuperare uno spazio giuridico pubblico a protezione dei diritti e delle libertà della persona.

Nello sforzo regolatorio europeo degli ultimi anni si assiste a un rinnovamento del diritto che passa da una costruzione di matrice globale e *multistakeholder* ed è guidato da un approccio etico-filosofico-giuridico, orientato verso la tutela dei diritti e lo sviluppo democratico. Gli Stati sono chiamati a produrre norme nella consapevolezza che l'ordinamento "nazionale" non può più esaurire l'ambito di regole applicabili, riconoscendo la presenza e il riferimento fornito da una pluralità di ulteriori sistemi statuali, sovranazionali o extrastatali, in ragione di una necessaria corresponsabilità da parte dei differenti produttori di norme, giuridiche o meno. A tali fini è opportuno immaginare, come opportunamente fanno gli atti recenti di regolazione europea, autorità, organismi e comitati sovranazionali dedicati al governo della tecnologia dotati di un certo grado di indipendenza rispetto a quei poteri che possono avere svariati interessi a orientarlo verso specifiche direzioni (poteri pubblici e mercato).

Del resto il cambiamento pervasivo determinato dallo sviluppo delle tecnologie e dalla centralità assunta dai dati investe i complessi equilibri consolidati tra diritti e libertà, il bilanciamento tra interessi contrapposti, il rapporto tra poteri e la tenuta dei principi democratici fondamentali, influenzando le direttrici culturali ed etiche del futuro; garantire i diritti e le libertà nel cyberspazio costituisce la sfida del nostro tempo.

Fin dall'origine delle tecnologie nel dialogo del diritto con la tecnica la riflessione ha dovuto concentrarsi su un necessario bilanciamento e un saggio equilibrio fra gli estremi contrapposti di estensioni eccessive e restrizioni soffocanti, fra le quali da sempre oscilla l'evoluzione tecnologica. In questo scenario si pone una chiara responsabilità pubblica nel garantire effettiva tutela alla persona, affrontando complessi bilanciamenti tra diritti che nella dimensione digitale si intrecciano e confliggono, mossi da tensioni diverse.

La regolazione europea recente risponde all'esigenza di porre principi e norme generali e astratte in materia e di dettagliare gli aspetti più tecnici e flessibili in atti di *soft law* cercando di non lasciare i diritti "senza legge", destinandoli altrimenti a incontrare una tutela solo nel momento patologico del conflitto, grazie alle interpretazioni e al ruolo supplente svolto dai giudici delle Corti e dalle autorità amministrative indipendenti poste a tutela dei diritti, come spesso è accaduto nel passato⁷⁶.

Le scelte filosofiche, etiche e giuridiche fondamentali del modello europeo di governo della tecnologia che emerge dal quadro regolatorio coinvolgono il ruolo della persona, gli interessi collettivi, la società, le geometrie di potere, il rapporto tra pubblico e privato.

Ciò porta con sé alcuni interrogativi. Quale forma del diritto è necessaria perché le norme possano essere effettive? Quali nuovi poteri e quale nuovo modello di *governance* delle autorità indipendenti sono adeguati al mutato contesto? Quale orizzonte giuridico di Internet⁷⁷?

Al riguardo, come esaminato, emerge nel quadro regolatorio europeo e più in generale nelle norme che trattano il rapporto tra diritto, diritti e tecnologia, oltre alla tensione tra protezione/controllo *versus* circolazione/apertura, anche la tensione tra certezza/prevedibilità *versus*

⁷⁶ Esemplicativamente è il caso della sentenza della Corte di Giustizia dell'Unione europea del 13 maggio 2014, causa C-131/12, cosiddetta *Google Spain* e, più ampiamente, è il caso dei provvedimenti delle autorità garanti, cruciali nel bilanciamento tra interessi contrapposti e nella concreta applicazione della disciplina.

⁷⁷ Parlava di «orizzonte giuridico dell'Internet» V. FROSINI, *L'orizzonte giuridico dell'Internet*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2000, pp. 271 ss.

flessibilità/adattabilità per garantire efficacia; sussiste infatti l'esigenza di una regolamentazione del mercato, al fine di evitare l'abuso da parte delle *digital companies*. Proprio allo scopo di circoscrivere tale potere, coniugando il diritto dei singoli al controllo dei propri dati con l'esigenza della loro circolazione, necessaria allo sviluppo del mercato, sono stati approvati i nuovi regolamenti europei. La sfida dell'ordinamento è quella di trovare un punto di caduta e un equilibrio tra tutela della persona e promozione del mercato; del resto compito del diritto è operare un ragionevole bilanciamento tra diritti ed interessi diversi.

In questo contesto, è necessario un rafforzamento dello spazio giuridico pubblico, evidentemente andato perduto nell'asimmetria contemporanea dei rapporti tra utenti e piattaforme, che passa dal ruolo delle autorità sovranazionali e delle autorità amministrative indipendenti nazionali, capaci ontologicamente di trovare quell'equilibrio tra certezza e flessibilità e creare, di conseguenza, un diritto sostenibile. Di conseguenza la riflessione in materia deve concentrarsi anche sull'opportunità di creare nuovi modelli di *governance* e una ridefinizione delle competenze delle autorità (come Garante per la protezione dei dati personali e AGCM), consapevoli, certamente più degli individui interessati, del valore che i dati assumono negli ambiti rispettivamente affidati alla loro regolazione, dando vita a un'applicazione normativa congiunta e a una forte collaborazione tra autorità. Questo approccio è necessario anche per i nuovi comitati e organismi creati dai regolamenti europei, che dovranno valersi di una stretta collaborazione e cooperazione⁷⁸. Ciò va nella direzione di un approccio orizzontale che scardina i sistemi regolatori verticali, meno adatti da sempre al volto orizzontale della rete e della dimensione digitale, ed evita il rischio di autorità che possono far pendere la bilancia verso l'uno o l'altro diritto o tecnologia per cui sono istituite, abbracciando invece il necessario approccio olistico sicuramente conforme alla complessità digitale e all'intreccio tra diritti e interessi diversi.

Sicuramente è oggi quanto mai necessario cercare quello che il Maestro Frosini chiamava «l'orizzonte giuridico di Internet», ossia provare a individuare l'"ordinamento giuridico digitale" e il modello di governo della tecnologia cui siamo e dovremmo essere indirizzati, che vede una nuova relazione tra diritto e tecnica capace di valorizzare la costruzione del diritto stesso come scienza che nasce per garantire prevedibilità e certezza alle relazioni umane, attribuendo diritti e doveri, riuscendo però a tutelare in modo efficace la persona e la società rispetto alla tecnologia con soluzioni

⁷⁸ *Supra*, § 2.

2/2023

e strumenti dotati di flessibilità e adattabilità: un diritto, forse imperfetto, ma sostenibile, capace di rafforzare e non impattare negativamente sulle libertà della persona e sull'autodeterminazione collettiva grazie a un saggio equilibrio tra diritti e interessi, facendo leva su un approccio olistico, al cui centro situare la persona.



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

FEDERICO CASA

Il filosofo del diritto e le discriminazioni digitali

ABSTRACT - This contribution essentially aims to answer three questions: (i) what is meant by digital discrimination; (ii) what attitude the philosopher of law must adopt towards the consequences, even negative ones, of the use of artificial intelligence; (iii) whether the emergence of artificial intelligence and of the logic of its reasoning impose a rethinking of the very idea of law, experience and legal science.

KEYWORDS - legal experience - legal science - logarithm - digital discrimination - devide digital

FEDERICO CASA*

Il filosofo del diritto e le discriminazioni digitali**

SOMMARIO: 1. *Premessa* - 2. *“Digital divide” e discriminazioni digitali* - 3. *Il filosofo del diritto, l’intelligenza artificiale e le disuguaglianze digitali* - 4. *L’intelligenza artificiale e un rinnovato senso dell’esperienza e della scienza giuridica*.

1. Premessa

Il presente contributo mira essenzialmente a rispondere a tre questioni.

L’intento del presente contributo è comprendere che cosa si intenda per *“digital divide”* e discriminazioni digitali, la portata di tali fenomeni, la rilevanza degli stessi e una loro possibile valutazione con riferimento agli effetti positivi e negativi dell’utilizzo dell’intelligenza artificiale in ambiti tradizionalmente estranei alla medesima, come quello del diritto.

In séguito, occorrerà comprendere in che senso e per quali ragioni il filosofo del diritto debba interessarsi alle discriminazioni digitali, perlopiù intese quale effetto negativo dell’affermazione incondizionata e irreversibile dell’intelligenza artificiale e delle modalità del suo procedere in buona parte delle attività umane.

Da ultimo, si tratterà di verificare se l’applicazione dell’intelligenza artificiale all’esperienza giuridica modifichi il significato stesso del diritto e se pertanto possa ancora essere attribuita una qualche valenza alle elaborazioni della scienza giuridica; si tratterà comprendere se la necessità di regolare l’intelligenza artificiale consenta di poter avere alcune informazioni sul significato del diritto nell’esperienza umana.

2. “Digital divide” e discriminazioni digitali

Non vi è dubbio alcuno che le disuguaglianze e le discriminazioni sociali e personali precedano la genesi dell’intelligenza artificiale; si tratta di una questione che in questa sede non ha neppure senso discutere¹.

* Professore associato di Filosofia del diritto nell’Università di Trento.

** Contributo sottoposto a valutazione anonima.

¹ Per due prospettive opposte sull’incremento delle disuguaglianze economiche nel corso dell’ultimo secolo, cfr. T. PIKETTY, *Il capitale nel XXI secolo* (2014), Firenze-Milano, 2018; M. FERRARIS, *Documanità*, Laterza, Bari-Roma, 2021.

“*Digital divide*” significa soprattutto non solo mancato accesso agli strumenti messi a disposizione dall’intelligenza artificiale, ma anche “analfabetismo digitale”, inteso nel senso che l’utente non è esautorato dall’ambiente digitale ma dalla partecipazione al circuito di fruizione e creazione della conoscenza nel *cyberspazio*. Accanto a questo si pone il problema delle analisi delle discriminazioni digitali che, a differenza del divario digitale, e detto molto banalmente, rappresentano lo studio delle disuguaglianze generate o aggravate dall’intelligenza artificiale.

Occorre allora subito rilevare che degli otto miliardi della popolazione umana due persone su tre accedono regolarmente a Internet e di queste oltre il novanta per cento utilizza piattaforme *social*, con numeri quadruplicati negli ultimi dieci anni e in crescita di oltre dieci punti percentuali solo rispetto al 2021; in media ogni utente vi trascorre quasi sette ore ogni giorno, di cui due ore e mezza sui *social media*². D’altro canto, effettivamente la pandemia si è rivelata come una delle molte forme di «decelerazione (acceleratoria) funzionale», che hanno costellato la storia della modernità e determinato il progresso tecnologico, rendendo “obsoleto” ciò che era già vecchio, e “indispensabile” ciò che era considerato come nuovo³.

Pertanto, se il divario digitale va attenuandosi, la questione rilevante è comprendere se l’utilizzo dell’intelligenza artificiale rappresenti un fattore di miglioramento delle condizioni di vita e quindi attraverso il suo sviluppo sia persino possibile un superamento delle disuguaglianze. Oppure la pratica dell’intelligenza artificiale costituisca un aggravamento della diversità tra le persone e i gruppi sociali.

Tutto ciò impone anche un ripensamento della pur recente categoria giuridica della vulnerabilità, che, come è noto, è presa in considerazione dalla scienza giuridica a partire dalla sua “dimensione situazionale”. E ciò con particolare riferimento ai diversi contesti in cui le discriminazioni, le offese e la violenza diventano “in negativo” determinanti nel produrre il mancato riconoscimenti dei diritti, compromettendo l’accesso a ciò che si ritiene importante⁴. D’altro canto, la nozione di vulnerabilità, così come è

² E. CREMONA, *I poteri privati nell’era digitale. Libertà costituzionale, regolazione del mercato, tutela dei diritti*, ESI, Napoli, 2022, p. 21.

³ H. ROSA, *Accelerazione e alienazione. Per una teoria critica del tempo nella tarda modernità*, Einaudi, Torino, 2015, *passim*.

⁴ Cfr. O. GIOLO, B. PASTORE (a cura di), *Vulnerabilità. Analisi multidisciplinare di un concetto*, Carocci, Roma, 2018, p. 88 ss.; ID., *Soggetti vulnerabili, orientamento sessuale, eguaglianza: note sulla logica di sviluppo del diritto*, in *GenIUS*, 2, 2018, pp. 105 ss.

stata costruita soprattutto dalla dottrina civilistica⁵, informa la progettualità della vita individuale e si connette alla libertà e uguaglianza degli esseri umani⁶; vulnerabile è chi è esposto al rischio di un danno⁷. Da questo punto di vista, al diritto si chiede di governare la molteplicità dei rapporti e delle relazioni guardando alle persone vulnerabili, la cui autonomia e dignità possono essere minacciate, evitandosi in questo modo l'esclusione e la marginalizzazione, che ostacolano l'autodeterminazione e lo sviluppo della personalità⁸. Lungo questo percorso teorico, il punto di riferimento non può che essere rappresentato da una concezione sostanziale dell'uguaglianza; e ciò per evitare che la vulnerabilità sociale e quella economica producano ulteriori ingiustizie, sul presupposto del valore positivo di alcune differenze da proteggere⁹. L'esperienza giuridica, in questi termini, opera attraverso una fitta trama costituita da pluralità di centri di produzione normativa, di fonti e di Corti, chiamati a garantire trattamenti omogenei di istanze non differibili sotto il segno per l'appunto dell'uguaglianza e dell'attuazione dei diritti¹⁰. In questo senso al diritto è affidato il compito di evitare che la vulnerabilità divenga discriminazione¹¹, e ciò non solo con riferimento a chi si trovi in una situazione di debolezza in senso soggettivo (i minori, gli anziani, i malati, i disabili, le persone di etnia diversa rispetto a quella prevalente), ma anche in una condizione di vulnerabilità economica e sociale (i poveri, gli immigrati, i rifugiati i consumatori indifesi)¹².

Da ultimo, nell'intento di comprendere la rilevanza delle categorie giuridiche, occorre osservare che da una parte si auspica la costruzione di un diritto comune dei soggetti vulnerabili¹³, dall'altra pare persino opportuno ripensare il paradigma classico di persona, e sostituirlo con l'ibrido, anche detto *cyborg*, determinato dall'ibridazione dell'uomo con la

⁵ A. GENTILI, *La vulnerabilità sociale. Un modello teorico per il trattamento legale*, in *R. crit. d. priv.*, 1, 2019, pp. 41 ss.

⁶ S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, p. 211.

⁷ Cfr. E. PARIOTTI, *Vulnerabilità ontologica e linguaggio dei diritti*, in *Ars Interpretandi*, 2019, p. 158.

⁸ E. BELVISI, *Dignità umana e diritti fondamentali: una questione di riconoscimento*, in T. CASADEI (a cura di), *Diritti umani e soggetti vulnerabili. Violazioni, trasformazioni, aporie*, Giappichelli, Torino, 2012, pp. 72 ss.

⁹ E. BATTELLI, *Vulnerabilità della persona e debolezza del contraente*, in *Riv. dir. civ.*, I, 2022, p. 943.

¹⁰ L. FERRAJOLI, *Manifesto per l'uguaglianza*, Laterza, Roma-Bari, 2018, pp. 4 ss.

¹¹ G. ZANETTI, *Filosofia della vulnerabilità*, Carocci, Roma, 2019, pp. 13 ss.

¹² N. LIPARI, *Vulnerabilità esistenziale e strumenti di tutela*, in *Annali SISDiC*, 2, 2018, pp. 2-4.

¹³ P. CENDON, *Verso un nuovo diritto dei soggetti deboli*, in *Pol. d.* 1994, pp. 484 ss.,

macchina¹⁴. Dal punto di vista più strettamente giuridico, il *cyborg* è, infatti, considerato una costruzione utile, perché in grado di dare conto di una corporeità costruita e non più data, che può divenire conforme alle possibili autodeterminazioni dell'individuo¹⁵.

Ciò chiarito, occorre ancora osservare che il divario digitale finisce allora per consolidare l'emarginazione di chi sia già posto ai confini della vita pubblica, persino rafforzando la capacità di controllo di alcuni gruppi su altri (si pensi all'utilizzo dei flussi informativi)¹⁶, tanto che, secondo alcune prospettive, questo potrebbe anche divenire un fattore di disparità dal punto di vista democratico¹⁷.

Vale, infatti, la pena di rilevare che le variabili che più spesso influenzano il *digital divide* sono la presenza d'infrastrutture di rete, la disponibilità dell'*hardware* di base, i costi di connessione alla rete. Con riferimento poi a determinate società, il divario digitale dipende soprattutto dalla presenza delle c.d. "barriere architettoniche digitali", vale a dire gli ostacoli alla massima fruibilità delle infrastrutture e il livello d'istruzione degli utenti, poiché è evidente il rapporto tra l'accesso agli strumenti informatici, l'informazione e il livello d'istruzione dell'utente. Notoriamente, altre variabili sono la lingua, il contenuto dei siti e l'età, perché alcune acquisizioni sono evidentemente generazionali¹⁸.

La definizione di *digital divide* è stata coniata dalla sociologia e dalla politica americana ai tempi dell'amministrazione Clinton. Con questa dizione s'intendono ancora oggi indicare le differenze che si generano tra coloro che hanno modo di accedere alle tecnologie informatiche¹⁹ e alla società dell'informazione e coloro che per le più svariate ragioni non ne hanno la possibilità²⁰; oppure che, pur avendone la facoltà, non sono in grado di comprendere appieno il loro funzionamento e così utilizzare le

¹⁴ Cfr. G. VATTIMO, *Il transumanesimo. Una nuova filosofia per il XXI secolo*, Armando Editore, Roma, 2010; R. MARCHESINI, *Post human. Verso nuovi modelli di esistenza*, Bollati Boringhieri, Torino, 2002, pp. 527-538;

¹⁵ S. VANTIN, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per la persona, la pubblica amministrazione, le imprese*, Cedam, Milano, 2021, pp. 27-60.

¹⁶ Cfr. M. GIULIANO, *Regolare l'infosfera*, in *Cont. e impr.*, 2021, pp. 886-890.

¹⁷ T. CASADEI, "Una questione di accesso"? *Democrazia e nuove tecnologie. Il caso dell'istruzione*, in S. SALARDI, M. SAPORITI, M. VETIS ZAGANELLI (a cura di), *Diritti umani e tecnologie morali. Una prospettiva comparata tra Italia e Brasile*, Giappichelli, Torino, 2022, pp. 26-30.

¹⁸ Cfr. M. CASTELLS, *Galassia internet* (2001), tr. it., Feltrinelli, Milano, 2002.

¹⁹ L. SARTOR, *Il digital divide*, Bologna, 2006, p. 7.

²⁰ J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, Mondadori, Milano, 2000, p. 319.

nuove forme di comunicazione e informazione (ostacoli cognitivi)²¹; oppure, infine, che, pur usando tutti gli strumenti dell'intelligenza artificiale, anzi, proprio perché se ne servono, all'esito, subiscono una importante discriminazione (in questo senso si discute di "discriminazioni digitali")²². Infatti, dal punto di vista statistico, gli studi sull'argomento non si occupano di verificare la disponibilità degli strumenti ma anche la possibilità di accedere alle informazioni, tanto è vero che sul tema le statistiche non riguardano solo le conseguenze della mancata connessione ma anche gli effetti degli accessi stessi²³.

Da altro punto di vista ancora, occorre considerare la natura «intersezionale» della discriminazione digitale; si pensi alla rete e alla spersonalizzazione della vittima, alla de-responsabilizzazione dell'autore, all'odio nei confronti di alcuni soggetti vulnerabili²⁴. Con maggiore riferimento, invece, alla natura del funzionamento degli algoritmi che regolano la logica dei programmi, si abbia riguardo, sempre in termini di discriminazioni digitali, ai rapporti tra la datificazione operata dai *big data* e la possibile discriminazione in relazione alla ricerca del lavoro; all'introduzione dei *bias* (pregiudizi anche inconsci) del progettista nella programmazione degli algoritmi²⁵; agli effetti negativi del "*data training*", il quale inevitabilmente finisce per rendere stereotipi alcuni gruppi più vulnerabili e al "*data model*", che spesso attua discriminazioni intenzionali per coprire forme di discriminazione diretta²⁶.

La classificazione delle discriminazioni digitali più feconda ci pare quella proposta con riferimento ai rapporti tra l'intervento del diritto in funzione antidiscriminatoria e le disuguaglianze stesse. Occorre allora distinguere le modalità di tutela di determinati individui o gruppi meritevoli di protezione, con riferimento ai quali l'attenzione si concentra sui *bias* che penalizzano determinati soggetti (si pensi al *rating* delle donne nella *gig economy*), dalle discriminazioni digitali c.d. «veridittive», che mirano a validare pregiudizi e stereotipi e da quelle c.d. «predittive», che

²¹ Cfr. N. IRTI, *Norma e luoghi. Problemi di geodiritto*, Laterza, Roma-Bari, 2006, p. 61.

²² D. DONATI, *Digitale divide e promozione della diffusione delle ICT*, in F. MERLONI (a cura di) *Introduzione all'e-Government. Pubbliche amministrazioni e società dell'informazione*, Giappichelli, Torino, 2005, pp. 209-211.

²³ A. BUONGIOVANNI, *Il digital divide in Italia*, in P. TARALLO (a cura di), *Digital divide. La nuova frontiera dello sviluppo globale*, Franco Angeli, Milano, 2003, p. 109.

²⁴ S. VANTIN, *op. cit.*, pp. 17-26.

²⁵ N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, il Mulino, Bologna, pp. 21-30.

²⁶ *Op. cit.*, pp. 38-42.

consentono di confermare passate discriminazioni, così rinvigorendo e promuovendo disuguaglianze radicate. Si è correttamente fatto notare che in questi casi l'intervento del legislatore rischia comunque di fallire il proprio obiettivo; infatti, se gli algoritmi sono ritenuti neutrali rispetto ai fattori di rischio, i gruppi più vulnerabili saranno sottorappresentati; se, invece, si cerca negli algoritmi la soluzione del problema, in termini di ricerca dell'uguaglianza sociale, tali gruppi di persone saranno considerati intrinsecamente svantaggiati²⁷.

Con particolare riferimento sempre alle discriminazioni digitali, si tratterà ora di verificare se e in che misura tali effetti, derivanti dall'utilizzo dell'intelligenza artificiale, interessino il diritto e in che senso il filosofo del diritto se ne debba occupare.

Il successivo paragrafo è dedicato proprio alla disamina di tali questioni.

3. Il filosofo del diritto, l'intelligenza artificiale e le disuguaglianze digitali

Pur espressa in termini molto semplicistici, possiamo condividere l'affermazione che obiettivo dell'intelligenza artificiale è soprattutto simulare il funzionamento del cervello e della mente umana, a prescindere, almeno tradizionalmente, dai condizionamenti che questa subisce per effetto del contesto delle relazioni sociali, dell'ambiente e della cultura²⁸. Detto in termini altrettanto banali, e tralasciando le discussioni epistemologiche solitamente proposte in letteratura in relazione al "test di Turing" e al "gioco della camera cinese di Searle", i cui risultati epistemologici paiono oggi persino controvertibili, nel senso che non è più così vero che l'elaboratore non sia in grado di comprendere il significato semantico dei propri risultati²⁹, è necessario precisare che un settore molto importante dell'informatica giuridica è lo studio del pensiero

²⁷ S. VANTIN, *Discriminazioni e vulnerabilità nell'epoca della rete globale*, in T. CASADEI, S. PIETROPAOLI, *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Cedam, Milano, 2021, pp. 238-239, con puntuali riferimenti alla legislazione europea.

²⁸ F. FAGGIN, *Irriducibile. La coscienza, la vita, i computer e la nostra natura*, Mondadori, Milano, 2022, pp. 59-78.

²⁹ T. CASADEI, S. PIETROPAOLI, *Intelligenza artificiale: fine o confine del diritto?*, in *op. cit.*, pp. 219-232.

computazionale³⁰. Sono quelle analisi che mirano a indicare quali siano le classi di problemi, che possano ottenere una soluzione attraverso l'utilizzo di un algoritmo³¹. Solo per inciso, sia consentito affermare che occorre prestare attenzione alla considerazione che quello di algoritmo è un concetto che non va in alcun modo confuso con il linguaggio di programmazione del *software*. Il primo costituisce l'indicazione al programma delle operazioni logiche, attraverso le quali è possibile risolvere un problema, mentre il secondo, anche detto linguaggio c.d. "formalizzato", costituisce un misto di linguaggio comune e di matematica, che il programma è in grado di comprendere, al fine di eseguire le operazioni algoritmiche miranti a risolvere le questioni che gli sono state poste³². Proprio il pensiero computazionale, cioè l'idea che alcuni problemi, compresi in parte quelli giuridici, possano essere riformulati attraverso un codice binario, costituisce un tema di grande interesse. Infatti, il rischio è rendere "necessariamente computazionale" una questione³³, che, in realtà, è molto più complessa rispetto alle semplificazioni che questa subisce al fine di essere "normalizzata", e ciò per poter essere governata da un algoritmo³⁴.

Tutto ciò ha generato in importanti settori della filosofia, non solo giuridica, una significativa sfiducia, ci sia consentito dire un po' provocatoriamente, tutta heideggeriana, nei confronti di queste scienze e delle tecniche applicate a settori della vita umana, che ancora non avevano visto imporsi il riduzionismo imposto dalla logica computazionale. Infatti, in questi ambiti rimaneva tradizionalmente decisiva la capacità di giudizio e quella creativa dell'uomo, in alcun modo sostituibile o simulabile (si pensi anche solo al rapporto tra la creazione dell'opera d'arte e l'intelligenza artificiale)³⁵. In ogni caso, anche solo in relazioni ad alcuni temi legati all'esperienza giuridica, occorre fare riferimento al *legal design* e all'idea, che

³⁰ M. DURANTE, *Potere computazionale. L'impatto delle ICT su diritto, società, sapere*, Meltemi, Milano, 2019, pp. 231-277.

³¹ U. PAGALLO, *Teoria giuridica della complessità*, Giappichelli, Torino, 2006, pp. 173-189.

³² S. CRAFA, *Dalle competenze alla consapevolezza digitale: capire la complessità e la non neutralità del software*, in P. MORO (a cura di), *Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea*, Franco Angeli, Milano, 2021, pp. 63-78.

³³ D. CARDON, *Le pouvoir des algorithmes*, in *Pouvoir*, 2018, pp. 63 ss.

³⁴ M. DURANTE, *op. cit.*, pp. 9-45.

³⁵ Cfr. R. BODEI, *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*, il Mulino, Bologna, 2019, pp. 330-342; G. ZICCARDI, *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina, Milano, 2019, pp. 37-41, 51-52; C. O'NEIL, *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano le democrazie* (2016), Milano, 2016.

periodicamente ricorre, a fini di certezza di prevedibilità delle decisioni³⁶, di assegnare all'algoritmo il potere decisorio delle controversie giuridiche³⁷.

Ancóra, con particolare riferimento alle discriminazioni digitali³⁸, occorre rilevare che, una volta implementati alcuni dati di partenza, forniti quelli necessari per eseguire le operazioni richieste e "allenato" il programma, è chiesto al *software* di eseguire alcune operazioni logiche (algoritmo), miranti a risolvere un determinato problema. Può darsi che la soluzione sia corretta, rispetto alle modalità con le quali sia stato posto il problema e alle informazioni fornite al programma, ma il risultato svantaggi per le più svariate ragioni alcuni soggetti o alcuni gruppi di soggetti³⁹.

D'altro canto, proprio con riferimento all'ambito giuridico, in letteratura è oggi prevalente la tesi, secondo la quale l'incredibile numero di dati e informazioni che oggi l'uomo ha a disposizione ha finito persino per modificare la realtà, si potrebbe dire quasi a livello ontologico, ancor prima che in senso epistemologico. Infatti, il rapporto tra questa mole di dati elaborati da algoritmi e l'interazione di questi con i mezzi d'informazione hanno già modificato il rapporto stesso tra l'uomo e il mondo; anzi, entrambi appaiono avere subito una trasformazione. Ne è derivata, secondo queste prospettazioni, una realtà costituita da *bit* e algoritmi, che ha sostituito quel mondo galileiano che poteva essere rappresentato simbolicamente. Si tratta di una concezione del cosmo non sottoposto né a un dio programmatore, né alle leggi della fisica, ma costituito da una realtà indefinita e non sempre facilmente precisabile, risultato di combinazioni imprevedibili⁴⁰. Donde il successo, anche in ambito giuridico, di quelle teorie epistemologiche che attribuiscono particolare importanza al principio d'indeterminazione proprio della fisica quantistica⁴¹ e affermano il c.d. "antinaturalismo", che è proprio anche dell'ermeneutica giuridica, secondo il quale solo ipotizzandosi una "famigliarità" preliminare (la precomprensione) tra l'interprete e l'oggetto

³⁶ F. COSTANTINI, *Giustizia Elettronica e digitalizzazione giudiziale: contesto europeo ed esperienza italiana*, in T. CASADEI, S. PIETROPAOLI, *op. cit.*, pp. 105-119.

³⁷ A. BERTOLINI, *Human-Robot. Iteration and Deception*, in *Oss. dir. civ e comm.* 2018, pp. 658 ss.

³⁸ A. CHANDER, *The Racist Algorithm?*, in *115 Michigan L. rev.*, 2017, pp. 1023.

³⁹ S. CRAFA, *op. cit.*, pp. 73-75.

⁴⁰ L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (2014), Raffaello Cortina, Milano, 2017, pp. 27-65.

⁴¹ F. LAUDISA, *La causalità*, Carocci, Roma, 2000, pp. 99-100.

della conoscenza, questo diviene accessibile e comprensibile⁴². Certo, magari non spiegabile e/o descrivibile, né pertanto prevedibile, ma in ogni caso è tema ormai ricorrente che l'oggettività della conoscenza giuridica scientifica abbia ceduto il passo alla ricerca della giustizia nel caso particolare⁴³.

Ne è derivato un vero e proprio timore della filosofia, anche giuridica, nei confronti dell'affermazione dell'intelligenza artificiale in tutti gli ambiti della vita umana, in cui decisioni sempre più importanti sono affidati ad algoritmi. Da questo punto di vista, la paura più rilevante è che il diritto stesso sia sostituito da un algoritmo, e così s'instauri una sorta di governo tecnocratico degli algoritmi, cui è devoluta ogni potestà decisoria⁴⁴. La tentazione appare, quindi, quella di limitare l'utilizzo dell'intelligenza artificiale, foriera di discriminazioni sempre più rilevanti⁴⁵.

D'altro canto, oggi non è nemmeno più in discussione l'idea che il programma apprenda facendo, a tutto concedere, si discute solo delle modalità teoriche attraverso le quali sia possibile implementare il *learning*. Infatti, nella costruzione degli algoritmi che apprendono, da una parte, si fronteggiano i simbolisti, secondo i quali occorre fornire al programma un minimo di conoscenze iniziali, le quali però consentono d'identificare quelle conoscenze che sono ancora mancanti, e ciò al fine di procedere al completamento della deduzione (si tratta della deduzione inversa), che consente di generalizzare i dati a disposizione a casi non ipotizzati. Dall'altra, i connessionisti, secondo i quali occorre ragionare come se l'organo dell'apprendimento fosse il cervello, con la conseguenza che, andando a ritroso, si confronta il risultato ottenuto con quello desiderato e in relazione a queste si modificano le relazioni tra le reti neurali). D'altro canto, gli evoluzionisti ritengono che la madre di ogni forma di apprendimento sia la selezione naturale, e conseguentemente mettono in relazione i programmi del computer con il modo in cui la natura fa evolvere gli organismi. Di contro, i baynesiani, i quali ritengono che, siccome il problema principale di ogni programma è l'incertezza associata

⁴² S. NANNINI, *Cause e ragioni: modelli di spiegazione delle azioni umane nella filosofia analitica*, Editori Riuniti, Roma, 1992, pp. 204-205.

⁴³ F. VIOLA, G. ZACCARIA, *Diritto e interpretazione. Lineamenti di una teoria ermeneutica del diritto*, Laterza, Roma-Bari, 1999, pp. 129-133, 259-267, 454-459.

⁴⁴ C. SARRA, *Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining*, in ID., P. MORO (a cura di), *Tecnodiritto. Temi e problemi d'informatica e robotica giuridica*, Franco Angeli, Milano, 2017, p. 42.

⁴⁵ L. FLORIDI, *op. cit.*, pp. 237-254; cfr. anche G. DA EMPOLI, *La rabbia e l'algoritmo*, Marsilio, Venezia, 2017, pp. 20-21.

all'inferenza, occorre ridurre ogni margine di errore attraverso la notissima inferenza probabilistica. Da ultimo, per gli analogisti è necessario individuare la regola di una situazione, al fine di poterla applicare a contesti somiglianti⁴⁶.

Dal punto di vista epistemologico, tali analisi sono utilissime, perché consentono di affermare che i procedimenti dell'informatica e del pensiero computazionale altro non sono se non quelli della scienza. Infatti, la discussione tra la logica dei simbolisti e il probabilismo dei baynesiani, quali modelli ai fini della migliore implementazione degli algoritmi, costituisce una tra le più tradizionali dispute del Novecento.

Eppure, tali risultati non sono sempre controllabili; anzi, spesso il programmatore non è nemmeno in grado di ripercorrere le operazioni logico-deduttive, che hanno procurato un determinato *output*. Infatti, fermi gli errori di programmazione e i difetti di funzionamento degli algoritmi, possono essere di molteplice natura anche gli errori riguardanti le informazioni, che sono alla base del generarsi delle disuguaglianze digitali. Questi possono riguardare i *data training*, che sono i dati con i quali viene sviluppato l'algoritmo, gli *input data*, che sono i dati in virtù dei quali l'algoritmo compie le scelte per le quali è stato elaborato, e i *feedback data*, le quali sono le informazioni che sono immesse nel sistema per perfezionarlo, i quali possono risentire dell'intento di orientare la scelta oppure dei semplici pregiudizi del programmatore. Peraltro, i codici che contengono gli algoritmi sono predisposti da tecniche ingegneristiche e informatiche non sempre facilmente comprensibili. A ciò si aggiunga che il contenuto del programma è persino protetto dalle leggi industriali, i cui codici, spesso, non appaiono del tutto comprensibili nemmeno da coloro che li programmano, tanto è vero che sono difficilmente valutabili anche gli errori di programmazione⁴⁷.

Da altro punto di vista, sono persino i dati e le informazioni messe a disposizione del programma che generano risultati in grado di costituire nuove disuguaglianze. E ciò perché le informazioni non sono mai neutre, ma perlopiù il prodotto di una complessa rete di rapporti sociali, che incorporano già essi strutture sociali di potere e in questo modo finiscono per rafforzarle. D'altro canto le organizzazioni che impongono *standards* tratti da *data analysis* si traducono in sistemi c.d. "disciplinari", produttori

⁴⁶ Di particolare interesse sul tema P. DOMINGOS, *L'Algoritmo Definitivo. La macchina che impara da sola e il futuro del nostro mondo* (2015), tr. it., Bollati Boringhieri, Torino, 2016, pp. 77-82.

⁴⁷ N. ABRIANI, G. SCHNEIDER, *op. cit.*, pp. 46-58.

forme di “normalizzazione” che riproducono sottostanti scelte di valore e strutture eventualmente anche ingiuste. Sempre con riferimento ai dati e alle informazioni, non vi è dubbio che già solo il rapporto con questi produca disuguaglianze, poiché occorre considerare, in primo luogo, coloro che generano dati. Basti pensare alla profilazione degli individui, per effetto della quale “la persona è considerata una miniera a cielo aperto”; l’algoritmo diviene una sorta d’inconscio tecnologico, in cui i dati di partenza non sono estratti, ma persino forniti da coloro i quali, a loro volta, sono discriminati. Vi sono, in secondo luogo, coloro i quali sono in grado di raccogliere dati e informazioni; in terzo luogo, coloro che a questi sono in grado di applicare degli algoritmi⁴⁸.

Per converso, da una parte i giuristi (su cui *infra*) che hanno affrontato il tema delle disuguaglianze digitali⁴⁹, dall’altra le istituzioni nazionali ed europee ritengono che l’intelligenza artificiale possa, invece, concorrere alla diminuzione delle disuguaglianze; nello stesso senso, anche quegli informatici che abbiano inteso illustrare il significato del loro lavoro e gli innumerevoli vantaggi che derivano alle attività umane⁵⁰.

Con riferimento più esplicitamente al nostro ordinamento, gli studiosi del diritto costituzionale hanno sostenuto, infatti, non solo che la nozione di libertà informatica abbia trovato riconoscimento nel diritto positivo, ma anche che non sia nemmeno necessario istituire nuovi diritti aventi un contenuto nuovo, inerente non più a beni ma a dati, poiché è sufficiente un’interpretazione evolutiva di quelli già esistenti⁵¹.

Non vi è dubbio che nessuno oggi proponga l’idea che i procedimenti algoritmici dell’intelligenza artificiale siano neutrali; eppure, anche molti giuristi ritengono che, pur potendo costituire motivo di discriminazioni, essa abbia complessivamente un effetto positivo⁵². Infatti, le legislazioni

⁴⁸ C. SARRA, *Dalla cibernetica alla Data Ethics. Linee di sviluppo dell’etica applicata alla rivoluzione informatica*, in P. Moro (a cura di), *op. cit.*, pp. 36-41.

⁴⁹ Cfr. S. AMATO, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020, pp. 100 ss.; L. PALAZZANI, *Dalla bio-etica alla tecno-etica: nuove sfide al diritto*, Giappichelli, Torino, 2017, pp. 374 ss.

⁵⁰ P. DOMINGOS, *op. cit.*, pp. 302-325.

⁵¹ Con riferimento alla robotica, cfr. U. RUFFOLO, *Intelligenza artificiale ed automotive: le responsabilità self-driving*, in ID., (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l’etica*, Giuffrè, Milano, 2020, pp. 153 ss.; cfr. anche G. SARTOR, *Gli agenti software: nuovi soggetti del cyberdiritto?*, in *Contr. e impr.*, 2022, pp. 485 ss.

⁵² Cfr. G. SCHNEIDER, *Intelligenza artificiale, governance societaria e responsabilità sociale d’impresa: rischi e opportunità*, in F. DONATI, A. PAJNO, A. PERRUCCI (a cura di), *La rivoluzione dell’intelligenza artificiale: profili giuridici*, il Mulino, Bologna, 2022.

nazionale ed europea affermano che, quale difesa rispetto al potere informatico, è sufficiente il diritto di libertà informatica, al quale, certo, è attribuito anche un significato non solo in negativo, poiché esso impone un comportamento da parte dello Stato, che consenta la partecipazione di ogni cittadino al circuito delle informazioni⁵³. Tale diritto è considerato oggi un diritto della personalità, cui corrisponde l'interesse del soggetto a essere rappresentato nella sua vera identità e a comunicare agli altri ciò che consente di esprimere la propria personalità. Quindi non più libertà da, ma libertà di partecipare alla società tecnologica; si tratta di una nuova forma di libertà costituzionale, non più soltanto la libera espressione del pensiero, ma anche la facoltà di costituire un rapporto, trasmettere e richiedere informazioni e quindi poter disporre di ogni potere che deriva dalla telematica⁵⁴. In questa prospettiva, il diritto di accesso agli strumenti informatici non è pertanto solo strumentale al diritto della libera espressione, ma anche al pieno sviluppo della persona umana, e quindi anche diritto sociale⁵⁵, che, come tale, presuppone un comportamento attivo da parte dello Stato⁵⁶. D'altro canto, in questa prospettiva occorre valutare la digitalizzazione del procedimento amministrativo, simbolicamente iniziata con la legge 7 agosto 1990 n. 241 e ancora oggi in corso di attuazione, culminata con il D.Lgs. 7 marzo 2005, n. 82 (C.A.D.)⁵⁷ e non poco modificata dal D.Lgs. 26 agosto 2016, n. 179⁵⁸.

4. *L'intelligenza artificiale e un rinnovato senso dell'esperienza e della scienza giuridica.*

Siano allora consentite a questo punto due indicazioni, conseguenti l'una all'altra, che discendono tutte dalla medesima concezione

⁵³ L. NANNIPIERI, *La dimensione costituzionale del digital divide. In particolare gli ostacoli cognitivi alla proiezione dell'individuo nello spazio virtuale*, in M. NISTICÒ, P. PASSAGLIA (a cura di), *Internet e Costituzione*, Giappichelli, Torino, 2014, pp. 189-220

⁵⁴ A. PIN, *Diritti costituzionali e intelligenza artificiale*, in P. MORO (a cura di), *op. cit.*, pp. 49-54.

⁵⁵ T.E. FROSINI, *Liberté, égalité, internet*, Editoriale Scientifica, Napoli, 2016, pp. 49-77, 219-233.

⁵⁶ G.M. ESPOSITO, *Al confine tra algoritmo e discrezionalità. Il pilota automatico tra procedimento e processo*, in *Rass. d. civ.*, 2019, pp. 399 ss.

⁵⁷ Cfr. M. MANCARELLA, *Algoritmo e atto amministrativo informatico: le basi del CAD*, in *Dir. internet*, 2019, pp. 469 ss.

⁵⁸ S. VANTIN, *op. cit.*, pp. 242-245.

dell'esperienza giuridica.

La prima è strettamente correlata al rapporto tra una determinata idea del diritto e le discriminazioni, anche quelle digitali.

Non vi è dubbio che, risalendo a un'antropologia individualistica, la quale pone al centro della riflessione la difesa dei diritti individuali di libertà, la giustizia coincide con la tutela dell'autodeterminazione individuale e l'attribuzione a ogni individuo libero di risorse e beni secondo i meriti, le capacità, il contributo che egli fornisce alla società, e ciò nella prospettiva della minimizzazione delle funzioni dello Stato (*minimum State*) e della massimizzazione dello spazio al libero mercato (*maximal market*). L'argomento alla base di questo modello di giustizia è la considerazione macro-allocativa, secondo la quale la società non è responsabile delle disuguaglianze, considerando i risultati della "lotteria naturale" e della "lotteria sociale" come "sfortunati", non iniqui e ritenendo che la società non sia tenuta a compensare le differenze o a riparare i danni⁵⁹.

Non troppo diversi appaiono essere, con riferimento al tema che ci occupa, i risultati di una teoria utilitarista, nella quale la giustizia coincide con la garanzia di un certo livello di qualità della vita, intesa come benessere nel bilanciamento piacere e dolore; la distribuzione mira a dare al maggior numero possibile d'individui la soddisfazione dei loro interessi, per garantire sul piano macro-allocativo la convenienza, l'efficienza e la produttività sociale, ossia il prevalere di benefici sui costi (si pensi a tutto il tema delle esternalità). Tale scelta, se espressa in termini radicali, non risolve il problema delle discriminazioni, tanto meno di quelle digitali, assunte come fisiologiche, e comunque ampiamente ripagate dai vantaggi che complessivamente la società ne riceve⁶⁰.

Solo da una prospettiva antropologica relazionale, può essere affermata la tesi che la società debba "farsi carico" delle disuguaglianze, comprese quelle digitali, sussistendo un dovere sociale di solidarietà e cooperazione, che deriva proprio dall'impossibilità per il giurista di prescindere dal riconoscimento dell'altro, che coincide con la natura stessa del diritto⁶¹. Ciò assume un duplice significato: la valenza egualitaria dell'assegnare a ogni persona in modo uguale, che significa dare a ciascuno quella porzione di bene comune, che appartiene, cui ognuno ha diritto, in

⁵⁹ Si tratta della notissima tesi di R. NOZICK, *Anarchia, stato e utopia. I fondamenti filosofici dello "Stato minimo"* (1974), tr. it., Firenze, 2000.

⁶⁰ L. PALAZZANI, *Giustizia distributiva, scarsità di risorse e Covid-19: sfide etiche e giuridiche*, in *L'Ircocervo*, 2021, 1, pp. 154-157.

⁶¹ T. GRECO, *La legge della fiducia. Alle radici del diritto*, Laterza, Roma-Bari, 2021, pp. 143-161.

quanto parte della comunità; e il contenuto profondo di dare all'indigente ciò di cui ha bisogno con il riconoscimento particolare e il sostegno delle situazioni di debolezza e fragilità. In tale senso la libertà individuale è subordinata al bene comune⁶². Eppure, è solo in una prospettiva antropologica relazionale che la giustizia assume il significato di rispettare la dignità di ogni essere umano, riconoscendo sul piano sociale a ciascuno ciò che gli spetta ontologicamente, in forza della stessa natura umana, indipendentemente dal conferimento o attribuzione da parte di una volontà esterna (a causa della posizione sociale, l'età o la qualità di vita). Le "spettanze" obiettive che vanno riconosciute a ogni uomo sono la vita, quale valore essenziale e il bene comune, quale valore co-esistenziale. Secondo questo modo di intendere la giustizia, radicato nell'uguaglianza, ogni essere umano ha sostanzialmente gli stessi diritti di qualsiasi altro essere umano pur nella diversità esistenziale: a ogni uomo vanno riconosciuti simmetricamente gli stessi diritti di ogni altro e reciprocamente gli stessi doveri, evitando privilegi arbitrari. Il criterio di giustizia si configura nella considerazione indisgiungibile del bene individuale e del bene sociale⁶³. E ciò consente di comprendere come le qualità individuali e i fondamenti etici della società siano finalizzati all'affermazione del bene comune e all'instaurarsi di rapporti di convivenza improntati al criterio della giusta misura⁶⁴.

La seconda.

Seguendo alcune di queste prospettive, effettivamente Internet e la *digital economy* rappresentano uno degli esempi più rimarchevoli della *deregulation*. Eppure, ora non sembra più percorribile né l'idea di uno *cyberspazio* autoregolato⁶⁵, né quella di una regolamentazione meramente tecnica⁶⁶, che lasci poi all'attivismo e alla creatività delle Corti il compito di rimediare alle violazioni dei diritti e al ripristino delle fratture⁶⁷.

Non vi è dubbio che le grandi piattaforme digitali (Amazon, Apple, Google, Meta, Microsoft) sono in grado di imporre a miliardi di utenti le proprie regole, nella forma dei termini e delle condizioni di servizio, tanto

⁶² J.M. FINNIS, *Legge naturale e diritti naturali* (1992), Giappichelli, Torino, 1996, pp. 161-167; F. GENTILE, *Ordinamento giuridico tra virtualità e realtà*, Cedam, Padova, 2000, pp. 38-43.

⁶³ J.M. FINNIS, *op. cit.*, pp. 173-178.

⁶⁴ A. SCERBO, *Diritto e virtù*, in ID., M. LA TORRE (a cura di), *Una introduzione alla filosofia del diritto*, Rubbettino, Soveria Mannelli, 2003, pp. 117-162.

⁶⁵ M. BASSINI, *Internet e libertà di espressione. Proposte costituzionali e sovranazionali*, Aracne editrice, Roma, 2019, pp. 31 ss.

⁶⁶ Cfr. N. IRTI, *Il diritto nell'età della tecnica*, Editoriale Scientifica, Napoli, 2007, pp. 21 ss.

⁶⁷ E. CREMONA, *op. cit.*, p. 32.

è vero che ormai la discussione riguarda la questione se queste regole possano dirsi condizioni di mercato o veri e propri atti normativi, alla cui produzione però (i destinatari degli stessi), gli utenti non partecipano in alcun modo⁶⁸.

Si è detto in modo suggestivo, che la crisi della normazione di Stato consente di riscoprire la sostanziale congenialità della nozione di «autonomia», che avrebbe caratterizzato le costituzioni giuridiche medievali⁶⁹; ma la situazione ci pare ancora diversa, quantomeno perché l'asimmetria tra le piattaforme e gli utenti non ha oggi uguali.

Il dato più rilevante è rappresentato dal fatto che l'avvento dell'intelligenza artificiale ha persino messo in discussione il paradigma pubblico/privato⁷⁰, così come è già accaduto nelle materie commercialistiche⁷¹. Ciò mette in crisi ogni ipotesi di *deregulation*, ma anche di *self-regulation*; eppure la dimensione globale e la natura tecnica del fenomeno rende impensabile il ricorso alle forme classiche della normazione pubblica. Lo scenario che pare allora aprirsi è quello di una *co-regulation*, in cui, in linea generale, alcuni poteri di normazione sono ceduti al potere privato, ottenendo però l'utente, quale corrispettivo, la fissazione da parte delle istituzioni di principi generali e il controllo giurisdizionale di merito sull'effettivo rispetto di questi principi, i quali, dal punto di vista teorico-generale, vanno ad incidere sul dogma dell'insindacabilità dell'autonomia privata⁷². Da questo punto di vista, il tema della discriminazione algoritmica è affidato al filone della regolazione dell'intelligenza artificiale⁷³ e alle decisioni della giurisprudenza europea e nazionale⁷⁴.

Ciò che allora interessa rilevare, a prescindere dalla scelta del

⁶⁸ G. TEUBNER, *Diritti ibridi: costituzionalizzare le reti di governance private* in Id., *La cultura del diritto nell'epoca della globalizzazione*, tr. it., Roma, 2005, pp. 128 ss.

⁶⁹ P. GROSSI, *Un diritto senza Stato (la nozione di autonomia come fondamento della costituzione giuridica medievale)*, in *Quad. fior.*, 25, 1996, p. 268.

⁷⁰ A. SIMONCINI, *Sovranità e potere digitale*, in T.E. FROSINI, O. POLLICINI, E. APA, M. BASSINI, *Diritti e libertà in Internet*, Firenze, 2017, pp. 19 ss.

⁷¹ M. BIANCHINI, *Profili di ibridazione tra interessi pubblici e privati nei "microsistemi normativi" delle società pubbliche e dei contratti pubblici*, in *Giur. comm.*, 1, 2021, pp. 838-887.

⁷² E. CREMONA, *op. cit.*, pp. 196-228.

⁷³ Cfr. la Proposta di AI Act presentata dalla Commissione Europea in data 21 aprile 2021, con riferimento al divieto di sviluppo e di uso di sistemi di intelligenza artificiale per fini discriminatori.

⁷⁴ Cfr. Trib. Bologna 31 dicembre 2020, in *www.iusinitinere.it*, che ha dichiarato illegittimo un algoritmo che declassava i *riders* senza alcuna distinzione tra coloro che si assentavano senza alcun motivo e quelli che lo facevano per motivi di salute e/o di sciopero.

paradigma regolatorio prescelto, è che l'intelligenza artificiale e le discriminazioni che essa comporta pongono importanti problemi di teoria del diritto e di teoria delle fonti. Pertanto, siano consentite alcune notazioni, quantomeno con riferimento al rapporto tra l'intelligenza artificiale e la scienza giuridica. Infatti, lo sviluppo senza precedenti e in ogni ambito della vita umana dell'intelligenza artificiale pone al giurista il problema della sua disciplina⁷⁵. Tale compito non può che spettare alla scienza giuridica, chiamata allora, e mai come in questo caso, non solo a descrivere l'esperienza giuridica, ma anche a comprenderla, in assenza della quale non è nemmeno ipotizzabile una sua disciplina da parte del legislatore.

Eppure, una delle discussioni oggi più diffuse, quantomeno tra i giuristi, riguarda il problema se ancora abbia senso discutere di scienza giuridica, l'importanza delle sue elaborazioni teoriche e il rapporto di queste con la costruzione del sistema. Oppure, se, preso atto della natura orizzontale delle fonti, della loro frammentarietà e comunque del pluralismo degli atti normativi e regolatori, sia preferibile rinunciarvi e ricercare la giustizia in quella porzione di ordinamento che si riscontra nel caso particolare, finanche nel caso singolare, e ciò attraverso il ricorso ai principi, alle clausole generali e all'attività interpretativa delle autorità giurisdizionali, sullo sfondo naturalmente delle proclamazioni dei diritti umani⁷⁶.

La complessità delle articolate discussioni politiche, etiche e giuridiche sull'intelligenza artificiale sembrano rendere più sicura e maggiormente praticabile questa seconda soluzione; e ciò anche sulla base dell'idea che essa, giorno dopo giorno, genera un diritto che non appare più agevolmente descrivibile, difficilmente prevedibile, quantomeno risalendo alle categorie giuridiche conosciute. Da altro punto di vista, un intero saggio già oggi potrebbe essere dedicato agli importanti sforzi di quei giuristi, che, invece, intendono adattare le categorie giuridiche ai nuovi ambiti: ai contratti⁷⁷ delle piattaforme digitali⁷⁸; alle responsabilità che discendono dalla diffusione della robotica⁷⁹; alla rappresentazione giuridica degli eventi

⁷⁵ G. RESTA, *Governare l'innovazione: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. d.*, 2019, pp. 199-237.

⁷⁶ F. VIOLA, 1990-2020. *Una storia del diritto naturale*, Giappichelli, Torino, 2021, pp. 119-123.

⁷⁷ M. GIULIANO, *Regolare l'infosfera*, in *Cont. e impr.*, 2021, 1, pp. 885-958.

⁷⁸ D. D'ALBERTI, *Google e le nuove autorità private: la metamorfosi dal fatto al diritto*, in *Riv. dir. civ.*, I, 2021, pp. 745-778.

⁷⁹ G. DE ROSA, *Quali regole per i sistemi automatizzati intelligenti?*, *ivi*, I, 2021, pp. 823-851; E. PALMERINI, *Robotica e diritto: suggestioni intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ.*, 2016, pp. 172 ss.

che avvengono in rete quale beni giuridici e l'individuazione della disciplina giuridica applicabile, i quali mettono in discussione la tradizionale opposizione tra situazioni giuridiche reali e obbligatorie e il rapporto tra fatti giuridicamente non rilevanti e beni⁸⁰.

È pur vero che da più parti si afferma in letteratura che, siccome le categorie giuridiche sono figlie della Pandettistica ottocentesca, a sua volta espressione di un ordinamento giuridico che vedeva nello Stato l'unica fonte del diritto, da almeno settant'anni sono divenute inutili, in quanto del tutto incapaci di dare conto della mutata realtà politica, sociale, economica e persino tecnica (si pensi per l'appunto all'intelligenza artificiale), dovendo perlopiù esser sostituite dai principi⁸¹, dai giudizi di valore degli interpreti⁸² e dagli interventi «creativi» della giurisprudenza⁸³.

Eppure, le categorie non sono rinunciabili; esse altro non sono se non modelli di spiegazione dell'esperienza giuridica "inventati" dai giuristi, al fine di dare conto della realtà giuridica, che si costituisce nel diritto positivo, ma non solo. Anzi, le prassi giuridiche che derivano dall'intelligenza artificiale negano l'idea del normocentrismo, ma non per questo non abbisognano della descrizione e comprensione, che è propria della scienza. Certo, prima di dibattere di scienza giuridica, occorrerà discutere di una teoria del diritto, cui può derivare una puntuale concezione epistemologica (genesì e confutazione delle teorie, idea del progresso della scienza e possibilità di comparare le diverse teorie, rapporto con la storia e la sociologia della scienza, il realismo e la verità, il ruolo delle assunzioni metafisiche), e metodologica (il ruolo del sistema, la funzione dell'interpretazione, il significato della giustificazione attraverso gli argomenti).

In questa sede non s'intende difendere una particolare teoria giuridica ma solo la necessità di una metodologia giuridica. Certo, come appare evidente dalla stessa disamina delle disuguaglianze digitali, l'oggetto delle analisi scientifiche (dei giuristi) non può essere limitato al diritto positivo, pur non potendosene prescindere. Anzi, l'intelligenza artificiale, da una parte, pone proprio il problema del significato della positività del diritto,

⁸⁰ E. INDRACCOLO, *Gli eventi come beni e pluralità dei loro statuti*, ESI, Napoli, 2022, pp. 210-256.

⁸¹ G. VETTORI, *La forza dei principi. Ancora un inizio*, in *Pers. e merc.*, 2019, p. 3.

⁸² Cfr. A. GENTILI, *Crisi delle categorie e crisi degli interpreti*, in *Riv. dir. civ.*, I, 2021, pp. 633-660, il quale illustra le teorie più diffuse che nell'ambito della scienza giuridica intenderebbero rinunciare all'utilizzo delle categorie giuridiche.

⁸³ L. FERRAJOLI, *Contro il creazionismo giudiziario*, Mucchi, Modena, 2018, pp. 46-47.

dall'altro, esalta la funzione della scienza giuridica e la sua capacità di apprestare e proporre le teorie, e ciò al pari delle scienze naturali, che siano in grado di meglio rappresentare l'esperienza, per divenire poi orientamento e guida all'attività del legislatore, il quale, non vi è dubbio, nel diritto positivo fissa provvisoriamente le sue determinazioni. Ma questa è già una teoria del diritto (di formazione giusnaturalista), che qui non interessa difendere.

Occorre piuttosto riflettere sulla considerazione, e si pensi anche solo al problema delle discriminazioni generate dall'intelligenza artificiale, che la ricerca dello scienziato giuridico prenda le mosse sempre da un problema, il quale spesso coincide con il sopravvenuto difficile rapporto di una disposizione giuridica con i fatti della vita che interessano il diritto; oppure anche con la genesi di questioni e avvenimenti del tutto sconosciuti all'ordinamento giuridico. In altri termini, il giurista ha a che fare con norme (o con la loro assenza) e fatti, che impongono il ripensamento della teoria giuridica prevalente e la proposizione di un'altra teoria. Infatti, se le risposte della dogmatica diventano insufficienti, occorre comprendere, facendo le opportune concretizzazioni, se effettivamente vi sia una distanza non più colmabile tra quello che sono gli accadimenti fattuali e le indicazioni contenute nel diritto positivo. In tal caso, occorre risalire alla teoria e comprendere se, opportunamente corretta, soprattutto partendo dagli enunciati "periferici", il cui mutamento porterebbe il minor danno possibile all'edificio della scienza giuridica (il sottosistema), sia possibile fornire una risposta ai problemi che gli accadimenti procurano. È poi necessario capire se la difficoltà incontrata dipende da un difetto d'inferenza, oppure se le correzioni, che devono essere apportate alla teoria, consentano di rispondere al quesito, ma tali soluzioni comportino conseguenze giuridiche non compatibili con la coerenza del settore giuridico del quale il giurista si sta occupando. In quest'ultimo caso occorre abbandonare la teoria e nei casi più gravi il modello stesso che ne costituisce il fondamento, a volte tutto ciò impone il ripensamento del paradigma che ha generato i modelli utilizzati. Una volta proposta una teoria, è poi necessario procedere alla sua confutazione; a séguito di tale attività di falsificazione, i giuristi adattano, modificano e ampliano l'ambito di applicazione della teoria proposta, e così il rapporto di questa con quella porzione dell'esperienza giuridica, che essi intendono comprendere e spiegare. La confutazione della teoria giuridica non è solo un tentativo di falsificazione della stessa, ma anche l'individuazione, rispetto allo schema generale di riferimento, di un riscontro a quanto formulato, accrescendo in

questo modo la conoscenza del diritto⁸⁴.

Si tenga, infine, presente, che una teoria giuridica consta non solo di una serie di presupposti di natura filosofico-metafisica, ma anche di alcune assunzioni⁸⁵, che a loro volta risentono, solo per fare qualche esempio ricavato dalle scienze naturali, di una particolare idea della logica o della matematica⁸⁶. Inoltre, una teoria giuridica si caratterizza sia per l'esistenza di alcune conoscenze che costituiscono lo 'sfondo' su cui essa si colloca (le elaborazioni della giurisprudenza, la dogmatica giuridica, i comportamenti consolidati dei destinatari delle norme giuridiche), sia per la vera e propria attività di modellizzazione, da cui deriva la teoria scientifica. Una teoria giuridica è connotata da una sorta d'idealizzazione dell'esperienza giuridica, alla quale segue, anche ai fini della confutazione, la concretizzazione della medesima, la quale non solo ha una propria indipendenza e autonomia, ma soprattutto ha un suo importante ruolo conoscitivo.

Se condividiamo questi assunti, il problema non sono le categorie giuridiche, le quali per il giurista non sono allora prescindibili, ma l'adeguatezza delle medesime a dare conto della mutata esperienza giuridica⁸⁷, che mai come oggi appare rivoluzionata, quantomeno in quegli ambiti dell'ordinamento in cui sono più rilevanti gli influssi dell'intelligenza artificiale; donde lo sviluppo senza precedenti delle questioni di diritto dell'informatica. Ci si potrebbe persino domandare se l'intelligenza artificiale sia in grado di modificare l'idea stessa di diritto che occorre condividere; probabilmente una risposta è ancora prematura, ma di certo essa impone anche allo scienziato giuridico di riflettere sul proprio metodo, sulla concezione dell'esperienza giuridica e quindi sulle assunzioni metafisiche delle proprie teorie scientifiche.

⁸⁴ E. AGAZZI, *L'oggettività scientifica e suoi contesti* (2014), Bompiani, Milano, 2018, pp. 573-598.

⁸⁵ E. BUNGE, *Philosophie de la Physique*, Parigi, 1973, pp. 229 ss.

⁸⁶ U. BOTTAZZINI, *Il calcolo sublime: storia dell'analisi infinitesimale da Euler a Weierstrauss*, Torino, 1981, p.13.

⁸⁷ V. VELLUZZI, *Tra teoria e dogmatica II. Altri sei studi sull'interpretazione*, Edizioni ETS, Pisa, 2020, pp. 110 ss.



ORDINES

Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730

NUMERO 2 – DICEMBRE 2023

ARIANNA MACERATINI

Virtual information and digital discriminations: some reflections

ABSTRACT - Digital information currently appears to be of central importance since, whether or not it is shared in the public sphere, it can favor an expansion of the conditions of political, economic and social equality, as well as extremize previous inequalities and create new ones. If, in fact, the participation of some types of digital data certainly appears to be of collective interest, it is accompanied by an improper use which results in a progressive concentration of knowledge capable of leading to dangerous cognitive asymmetries and power imbalances, with risky implications for democracy, unknowns made even more serious by the difficulty of tracing its spatial coordinates and of offering adequate legal regulation. In the virtual world, a further and serious risk of inequality is, then, represented by the use of predictive logic that informs the automatic processes of digital data processing, raising crucial questions about any dangers of discrimination to the detriment of social categories and groups that could be penalized from automatic decision-making, with the enhancement of traditional gaps and outlining new digital disparities that bring to the fore the crucial issues of transparency and algorithmic explainability. Finally, it can be noted that the exclusion from access or from an efficient use of digital technologies risks deepening pre-existing generational, social, economic and cultural distances. These problems have been dramatically highlighted by the recent Covid-19 pandemic which, in revealing the essential role of telecommunications networks and the possession of an adequate digital culture, has, at the same time, exacerbated the digital divide. Looking ahead, the speed of technological innovation seems to require the adoption of targeted "use policies" and conscious regulation actions combined with a strong commitment to continuous education and training aimed not only at those directly involved in the management of digital technologies, but extended to every citizen, enhancing the inclusion of the most vulnerable right from the design phase of technological solutions, resulting in the possibility of exercising an active citizenship.

KEYWORDS - Digital information - concentration of knowledge - predictive algorithms
- digital discrimination - right of access - fundamental rights

2/2023

ARIANNA MACERATINI*

Informazione virtuale e discriminazioni digitali: alcuni spunti di riflessione**

SOMMARIO: 1. *Introduzione* – 2. *La concentrazione della conoscenza* – 3. *Il «capitalismo della sorveglianza»* – 4. *Algoritmi e disuguaglianze* – 5. *Accesso e informazione*

1. Introduzione

Nella società dell'informazione, le innovazioni scientifiche e tecnologiche hanno ridisegnato il mondo affermando una dimensione globale, dettando nuovi ritmi e regole all'economia e cambiando le modalità dell'agire politico con l'incidere tanto nelle relazioni sociali quanto nella percezione che l'individuo ha di se stesso¹. In tale contesto, l'informazione digitale risulta di centrale rilevanza potendo, la sua condivisione o meno nella sfera pubblica, favorire un ampliamento delle condizioni di uguaglianza politica, economica e sociale, quanto acuire disuguaglianze pregresse e crearne di inedite.

Nella prima direzione, la partecipazione di alcune tipologie di dati digitali appare di sicuro interesse collettivo, offrendo un contributo fondamentale nella gestione di rilevanti sfide future: è questo il caso delle città intelligenti dove la condivisione dei dati può aiutare a gestire il traffico in modo più efficiente, contenere i livelli di inquinamento, regolare il consumo di acqua, di energia e delle risorse naturali, nonché contribuire ad aumentare il livello della sicurezza urbana. La messa in comune di dati e dei modelli di analisi predittiva potrebbero, inoltre, essere proficuamente introdotti nella moderna gestione agricola, nel contrasto al riscaldamento globale e ai cambiamenti climatici, ma è soprattutto quello della ricerca scientifica, della medicina e delle numerose applicazioni dell'intelligenza artificiale nell'ambito dell'accessibilità e del supporto ai soggetti più fragili il campo in cui la condivisione dei dati, in primo luogo dei *big data*, può implementare la ricerca in direzione di una maggiore tutela della salute e

* Ricercatrice in Filosofia del diritto e professore aggregato di Informatica giuridica presso l'Università degli Studi di Macerata.

** Contributo sottoposto a valutazione anonima.

¹ Cfr. S. RODOTÀ, *L'uomo nuovo di Internet*, Lectio magistralis del 28.10.2005, in <https://www.privacy.it/archivio/rodo20051028.html>

dell'ambiente², delineando i caratteri di una scienza e, più in generale, di una società aperta e partecipativa, nel rispetto dei diritti umani e digitali³. In tal senso, possiamo qui solo accennare alla proposta della Commissione europea, del 3 maggio 2022, sullo «Spazio europeo dei dati sanitari» (EHDS), un ambiente digitale di raccolta delle informazioni sanitarie che, con la connessione dei *database* dei Paesi appartenenti all'Unione e tramite la tutela del flusso dei dati sanitari scambiati tra questi ultimi, consentirebbe all'Europa di compiere un salto qualitativo nella modalità di erogazione delle cure, promuovendo, nel settore, un mercato unico digitale dei servizi e dei prodotti.

Anche nel terreno della Pubblica Amministrazione, l'impiego condiviso di informazioni significative assume un centrale risalto, ponendosi alla base della digitalizzazione e della trasparenza dell'attività amministrativa⁴. Gli *open data* rappresentano, infatti, fondamentali elementi dei modelli di governo democratico⁵, rivolti ad un miglioramento generale delle condizioni di vita⁶. In tali casi – fatte salve le dovute limitazioni per lo più riferibili alla tutela dei dati personali e alla garanzia dei diritti di proprietà intellettuale – i dati digitali possono accrescere le condizioni di eguaglianza⁷, sollecitando governanti e cittadini alla partecipazione democratica, in un percorso tracciato, tra le molteplici disposizioni in questo senso, dall'art. 19 della Dichiarazione Universale dei Diritti dell'Uomo, nonché dall'art. 21 della nostra Costituzione, a sostegno della libertà di manifestazione del pensiero che vede, come corollario, un accesso alla conoscenza libero e giuridicamente garantito⁸.

² Cfr. C. FARALLI, *Diritti e nuove tecnologie*, in Tigor: rivista di scienze della comunicazione e dell'argomentazione giuridica, 2/2019, pp. 43-52; L. PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale*, Studium, Roma, 2020, pp. 16-21.

³ Cfr. S. LEONELLI, *Big data nel mondo della salute: bene comune o interesse privato?* in G. BALBO, P. JARRE, *Manuale di InformEtica*, Loescher, Torino, 2021, pp. 121-125.

⁴ Cfr. F. FAINI, *Data Society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè, Milano, 2019, p. 29.

⁵ Cfr. M. NOUSSAN, *Qualità e fruibilità degli open data*, in G. BALBO, P. JARRE, *Manuale di InformEtica*, cit., p. 128.

⁶ Per un approfondimento del concetto di *open data* e un'analisi degli aspetti più rilevanti della regolazione di tale tipologia di dati digitali, si rimanda a F. FAINI, *op. cit.*, pp. 117-160.

⁷ Sulle potenzialità dei *big data* nella prevenzione delle violazioni dei diritti umani, si veda L. NOSARI, *Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani*, in: <https://www.cyberlaws.it>.

⁸ Cfr. J. DREXL, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in: Max Plank Institute for Innovation and Competition Research, dicembre 2016, paper n. 16, pp. 1-28.

2. La concentrazione della conoscenza

Ad un'informazione virtuale finalizzata al potenziamento individuale e collettivo, si affianca, tuttavia, un utilizzo improprio che ha come esito una concentrazione progressiva della conoscenza, capace di condurre a pericolose asimmetrie cognitive e a squilibri di potere⁹, con rischiosi risvolti per la democrazia¹⁰. In questo senso, una pressante incognita è rappresentata dallo sfruttamento economico dei dati digitali, spesso ottenuti in assenza di un consenso pienamente consapevole dei soggetti interessati, ma tramite interazioni nel web¹¹ – da parte di un esiguo numero di operatori del settore in grado di controllare la ricchezza informativa¹². Gli *Over the Top* (OTT) sono costituiti da poteri pubblici e privati i quali, regolando l'accesso ai servizi e alle utilità della Rete, producono una potente concentrazione informativa basata su regole di fatto, orientate al profitto ed avulse da ogni forma di legittimazione democratica¹³. Sono, in tal modo, posti in essere «meccanismi di controllo di dubbia legittimità e tali da esercitare un potere autoregolativo che aspira a farsi sovrano»¹⁴ che si riflette sulla piena esplicazione dei diritti di libertà e sul futuro stesso della democrazia¹⁵, incognite rese ancor più gravi dall'evidente difficoltà di tracciarne precise coordinate spaziali e di offrirne un'adeguata regolamentazione giuridica¹⁶.

In particolare, le piattaforme informative determinano una vistosa asimmetria tra i versanti del mercato centrata su modelli di integrazione verticale¹⁷ da cui deriva una spiccata polarizzazione della conoscenza. A tale fenomeno si unisce, poi, un intenso sistema di filtraggio e di blocco delle informazioni *on line* finalizzato all'individuazione di contenuti ritenuti

⁹ Cfr. F. FAINI, *op. cit.*, p. 392.

¹⁰ Cfr. F. BARCA, *Fare della giustizia sociale la bussola della trasformazione digitale: strategia e strumenti*, in G. BALBO, P. JARRE, *Manuale di InformEtica*, cit., pp. 157-161.

¹¹ Cfr. F. FAINI, *op. cit.*, p. 316.

¹² Cfr. ad es. C. CASONATO, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal, Rivista di Biodiritto*, 1/2019, 178 sgg; V. ZENO-ZENCOVICH, *Uber: modello economico e implicazioni giuridiche*, in *MediaLaws*, 2018, pp. 140-143.

¹³ Cfr. F. FAINI, *op. cit.*, p. 9.

¹⁴ A. ALPINI, *Digital divide, censura digitale e antropocentrismo dei dati*, in *Comparazione e diritto civile*, 3/2021, p. 880.

¹⁵ Cfr. F. FAINI, *op. cit.*, 63. Sulle difficoltà di stabilire giuridicamente la proprietà dei big data e, più in generale, delle informazioni prodotte mediante l'IoT, cfr. *ivi*, pp. 196-200.

¹⁶ Cfr. C. CASONATO, *Potenzialità e sfide*, cit., p. 178.

¹⁷ Cfr. M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, il Mulino, Bologna, 2019, pp. 51-53.

pericolosi *a priori*, una pratica che, sebbene in molti casi si rivolga a materiali e a pagine virtuali di presunto carattere terroristico o estremistico, comporta, tuttavia, un'inquietante torsione del diritto all'informazione che appare consegnato ad una sorta di censore privato verso il quale è possibile ricorrere solo in seconda istanza, mediante un eventuale ricorso all'autorità giudiziaria¹⁸. Le questioni qui delineate divengono ancor più rilevanti considerando le responsabilità dei soggetti pubblici nella duplice veste di produttori e utilizzatori di dati digitali, frequentemente ottenuti dal settore privato, informazioni tramite le quali si potrebbe, potenzialmente, instaurare un monitoraggio di massa sostenuto dai rapporti negoziali stabiliti con le grandi aziende tecnologiche¹⁹. In questo modo, il *big data divide*, determinato dalla concentrazione delle informazioni *on line* in mano ai governi e ai colossi tecnologici²⁰, sembra erodere il confine tra pubblico e privato²¹, ponendosi contro il principio di uguaglianza sostanziale²² che si traduce, qui, in un effettivo controllo dei dati personali quale valore non relegato ad una dimensione meramente individuale, ma aperto ad una valutazione dei rischi per la collettività²³. Secondariamente, l'asimmetria di relazione sussistente tra l'esiguo numero di piattaforme *on line* e i fruitori dei servizi digitali, alimentata dalla chiusura dei processi di gestione dei dati²⁴, sembra porsi a sfavore della costruzione giuridica di un mercato trasparente dei dati²⁵ visto che le informazioni raccolte dagli OTT, diventando di dominio di pochi *players*, sollevano inedite problematiche sulla concorrenza «rendendo di difficile applicazione gli istituti tipici della

¹⁸ Cfr. A. ALPINI, *Digital divide*, cit., 891. Nel contesto preso in esame, dove il potere giurisdizionale sembra assumere un ruolo centrale, si rileva l'indispensabilità della presenza di fonti sovraordinate e imperative, norme fisiologicamente deputate ad una regolazione dei beni in conflitto che risulti il più possibile sottratta alle logiche del profitto, cfr. F. FAINI, *op. cit.*, p. 411.

¹⁹ Cfr. F. FAINI, *op. cit.*, pp. 183-187.

²⁰ Cfr. F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche. Temi e problemi*, Giappichelli, Torino, 2021, p. 417.

²¹ Sull'elusione, nel web, della linea di demarcazione tra sfera pubblica e ambito privato a fini principalmente propagandistici si veda G. ZICCARDI, *Tecnologie per il potere. Come usare i social network in politica*, R. Cortina Ed., Milano, 2022, pp. 37-71.

²² Cfr. G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Politica del diritto*, 1/2019, p. 113.

²³ Cfr. F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, cit., p. 430.

²⁴ Cfr. *ivi*, p. 427.

²⁵ Cfr. M. DELMASTRO, A. NICITA, *op. cit.*, 31. Il diritto alla portabilità dei dati personali, sancito dall'art. 20 del GDPR, sembra corrispondere a questa logica, cfr. *ivi*, pp. 129-30.

disciplina quali mercato rilevante, prezzi discriminatori e abuso di posizione dominante»²⁶.

Nel tentativo di stare al passo con la rapidità evolutiva delle tecnologie digitali e di far fronte al prevalere di «un'ideologia tecnofila secondo la quale tutto ciò che è tecnicamente fattibile deve essere fatto»²⁷, si aprono, dunque, inediti spazi regolativi e normativi volti a preservare la dimensione virtuale quale luogo di libertà, individuale e collettiva, generando nuove forme di solidarietà civile alimentate dall'informazione²⁸. Nella prospettiva di un'efficace tutela del diritto all'informazione, così come di un'effettiva disponibilità e gestione dei dati personali, la titolarità di questi ultimi potrebbe utilmente essere delineata come un'*essential facility* di carattere immateriale dalla quale far discendere l'obbligo, per i giganti dell'informazione, e fatte salve specifiche tutele, di aprire i dati²⁹: «l'apertura dei big data in ambito pubblico, ma anche in ambito privato può contribuire a sanare le asimmetrie informative, mettendo a disposizione della collettività i dati, anche se inevitabilmente è capace di provocare una perdita di potere per i detentori degli stessi»³⁰. Ciò contribuirebbe, inoltre, al riconoscimento di una peculiare responsabilità informativa a carico degli OTT, riconducendo i processi economici al nucleo dei diritti fondamentali della persona³¹.

L'impatto sociale dei dati digitali e degli algoritmi di utilizzo porta ad emergere, oltre ad un'idea della conoscenza come bene pubblico globale a titolarità diffusa³², l'esigenza di concepire le informazioni digitali quali beni comuni, valorizzando gli interessi generali di trasparenza e democrazia ad essi sottesi³³ e promuovendo le condizioni di un'autentica partecipazione

²⁶ F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, cit., p. 421.

²⁷ P. JARRE, *Introduzione*, in G. BALBO, P. JARRE, *Manuale di InformEtica*, cit., p. 12.

²⁸ Cfr. M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne, Canterano, 2018, p. 25. Com'è noto, in Italia il D. lgs. 25 maggio 2016, n. 97 ha introdotto il cosiddetto accesso generalizzato, subordinato alla richiesta del cittadino, alla quale segue l'eventuale risposta dell'Amministrazione statale. Tale procedimento rivela, tuttavia, la sua distanza da un'*open data policy* e dalla piena attuazione del principio di trasparenza, in grado di alimentare un'efficace rete di condivisione, interoperabilità e riutilizzo della conoscenza, cfr. *ivi*, 46-73. Sul recepimento del paradigma *open* nell'ordinamento giuridico italiano, cfr. *ivi*, pp. 29 ss.

²⁹ Cfr. *ivi*, p. 13.

³⁰ F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, cit., p. 428.

³¹ Cfr. M. OREFICE, *op. cit.*, p. 13.

³² Cfr. S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014, 72; cfr. F. FAINI, *op. cit.*, p. 66.

³³ Cfr. F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, cit., p. 429.

democratica. Tale necessità è stata, del resto, rilevata dalla Risoluzione del Parlamento Europeo del 16 marzo 2017, sull'«E-democracy nell'Unione Europea: potenziale e sfide» – la quale, all'art. 16, invita gli Stati membri ad astenersi dall'adottare misure di arbitraria limitazione dell'accesso ad Internet – nonché dal recente progetto di regolamento «*Artificial Intelligence Act*» elaborato dalla Commissione europea COM(2021) 206 *final* del 21 aprile 2021, diretto ad introdurre una disciplina antidiscriminatoria e di tutela delle vulnerabilità sociali, seguendo quanto stabilito, in termini di *soft-law*, dalla «Risoluzione sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto» del 2017.

La consapevolezza della complessità dell'ambiente virtuale e della continuità di azione tra quest'ultimo e il mondo analogico³⁴ porta ad emergere, infine, l'indispensabilità di norme condivise nella regolazione delle risorse digitali e di una tutela dei dati personali in evoluzione, tale da considerare le informazioni *on line* come componenti essenziali della cittadinanza digitale e dell'identità personale, accompagnando il riconoscimento dell'autodeterminazione informativa a una reale redistribuzione del potere in Rete³⁵.

3. Il «capitalismo della sorveglianza»

In direzione opposta, il potere dei «latifondisti della conoscenza»³⁶ rende per lo più formale la proclamata libertà della Rete, rappresentando il pretesto di azione di un «capitalismo della sorveglianza» il quale, nell'imporre il proprio dominio con l'illusione della sicurezza assoluta per i consociati, produce *equivalenza senza eguaglianza*, riconducendo le scelte individuali al minimo comune denominatore del mercato virtuale³⁷. Ciò conduce all'affermazione di una logica economica pervasiva e parassitaria la quale, non limitandosi ad influenzare la produzione e il consumo di beni e servizi, si spinge sino alla predizione e alla parallela modifica dei comportamenti, compresi quelli politici ed elettorali, per distorcere

³⁴ Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, R. Cortina Ed., Milano, 2017, pp. 44-55.

³⁵ Cfr. S. RODOTÀ, *Il mondo nella rete*, cit., p. 72.

³⁶ Cfr. M. OREFICE, *op. cit.*, p. 158.

³⁷ Cfr. S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019, p. 394.

l'organizzazione delle notizie in ricerca mediante *political chatbots*³⁸ in grado di rovesciare i più basilari principi democratici e il significato stesso del concetto di sovranità popolare³⁹. In tal modo, la profilazione individuale, sollecitata dal massiccio impiego dei *big data* e implementata dai più attuali algoritmi predittivi e decisionali contribuisce a selezionare i contenuti determinanti per la formazione dell'opinione pubblica, da segnalare al singolo così come all'agenda politica⁴⁰. Ne consegue la creazione di *filter bubbles*, nicchie di informazione volte a mostrare all'utente le informazioni che l'algoritmo ha individuato per lui come potenzialmente interessanti⁴¹, un fenomeno aggravato dall'opacità di funzionamento degli algoritmi⁴² e tale da favorire processi di omologazione sociale⁴³ che portano a scomparire l'unicità della persona tra navigazioni, *click* e *like*⁴⁴ per delineare una sorta di "pluralismo ovattato", cioè, filtrato dalle preferenze di chi fruisce dell'informazione digitale, a fronte del quale si è parlato di un diritto del singolo alla discontinuità e all'incoerenza⁴⁵.

Così, a dispetto dell'enorme potenzialità del digitale di diffondere dati e di creare legami sociali, la *clusterizzazione* delle informazioni rende ardua la conoscenza di opinioni diverse dalle proprie⁴⁶, in una condivisione apparente di pensieri e azioni quotidiane⁴⁷ affidata alla tipica modalità di scrittura emotiva del web⁴⁸.

Si può comprendere, di conseguenza, come la Rete possa trasformarsi da spazio astrattamente aperto ad ambito ristretto da precise corrispondenze, facendo sorgere gravi interrogativi sulla libertà di

³⁸ Per una definizione e un'analisi degli *chatbots* in ambito politico, nonché dei loro deleteri riflessi sul sistema democratico dei diritti, si rimanda a G. ZICCARDI, *Tecnologie per il potere*, cit., pp. 129-138; pp. 209-217.

³⁹ Cfr. S. ZUBOFF, *op. cit.*, cit., pp. 511 ss.

⁴⁰ Cfr. M. DELMASTRO, A. NICITA, *op. cit.*, p. 91.

⁴¹ Cfr. A. C. AMATO MANGIAMELI, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto. Journal of Legal Philosophy*, 1/2019, p. 109.

⁴² Cfr. D. TALIA, *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*, Rubettino, Catanzaro, 2018, p. 97.

⁴³ Cfr. C. CASONATO, *Costituzione e intelligenza artificiale: un'agenda per il futuro*, in *BioLaw Journal, Rivista di Biodiritto*, 2/2019, pp. 714-715.

⁴⁴ Cfr. F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, cit., p. 418.

⁴⁵ Cfr. C. M. REALE, M. TOMASI, *Libertà d'espressione, nuovi media e intelligenza artificiale: la ricerca di un nuovo equilibrio nell'ecosistema costituzionale*, in *DPCE online*, 1/2022, p. 331.

⁴⁶ Cfr. A. ROSSETTI, *Per un'educazione digitale consapevole*, in G. BALBO, P. JARRE, *Manuale di InformEtica*, cit., p. 139.

⁴⁷ Cfr. D. TALIA, *op. cit.*, p. 97.

⁴⁸ Cfr. Z. BAUMAN, *Consumo, dunque sono*, Laterza, Roma-Bari, 2010, p. 96.

espressione, sul pluralismo e sulla correttezza informativa⁴⁹. Alla vastità di informazione *online* corrisponde, infatti, una maggiore quantità di disinformazione⁵⁰ sostenuta da *fake news* in grado di acquisire progressiva autorevolezza in base ad un meccanismo estraneo alla verifica delle fonti, ma centrato sul numero delle condivisioni e, pertanto, capace di minare una comprensione responsabile delle notizie⁵¹. Frequentemente, poi, l'informazione scorretta è determinata dal fenomeno del *reverse censorship* consistente nel sommergere i messaggi sgraditi in un mare di informazioni più o meno autentiche, una pratica aggravata dalla diffusione di messaggi provenienti da *robot* capaci di creare una fittizia popolarità intorno a precise opinioni⁵². La qualità dell'informazione dipende, in definitiva, dalla capacità di critica e di discernimento del fruitore finale⁵³ ed, al riguardo, va qui ricordata la scorciatoia mentale del «pregiudizio di conferma» per il quale, nella selezione delle informazioni rilevanti, ci si sente, in genere, maggiormente attratti da quelle che confermano le convinzioni soggettive di partenza: in questa breccia si inserisce la selezione contenutistica operata dall'algoritmo a suggerire interessi in base a preferenze espresse⁵⁴, un procedimento che stabilisce un doppio filtro informativo, determinato dalla congiunta azione della selezione algoritmica dei contenuti e dal pregiudizio di conferma⁵⁵. Tali problematiche mettono, dunque, in questione l'algoritmo quale filtro di contenuti⁵⁶ e in grado di delineare «un pensiero cristallizzato»⁵⁷ che, nel massimizzare l'incontro tra domanda e offerta di informazioni, rischia di emarginare processi e decisioni legati al significato più profondo delle cose, per affermare una dimensione puramente misurabile⁵⁸.

⁴⁹ Cfr. M. DELMASTRO, A. NICITA, *op. cit.*, p. 115; C. CASONATO, *Costituzione e intelligenza artificiale*, cit., pp. 714-715.

⁵⁰ Cfr. ad es. D. TALIA, *op. cit.*, p. 13.

⁵¹ Un approfondimento di questo delicato tema in G. ZICCARDI, *Tecnologie per il potere*, cit., pp. 197-208.

⁵² Cfr. A. ALPINI, *Digital divide*, cit., p. 885.

⁵³ Cfr. M. DELMASTRO, A. NICITA, *op. cit.*, p. 93.

⁵⁴ Cfr. *ivi*, p. 95.

⁵⁵ Cfr. *ivi*, p. 97.

⁵⁶ Sull'algoritmo decisionale nella pronuncia giudiziaria e sui limiti di tale impiego, si veda A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto Journal of Legal Philosophy*, 1/2019, pp. 96-102; A. C. AMATO MANGIAMELLI, *Algoritmi e big data*, cit., pp. 115-16.

⁵⁷ D. TALIA, *op. cit.*, p. 98.

⁵⁸ Cfr. *ivi*, p. 120.

4. Algoritmi e diseguaglianze

Nel virtuale, un grave rischio di diseguaglianza è, dunque, rappresentato dall'impiego della logica predittiva che informa i procedimenti automatici di elaborazione dei dati digitali, in grado non solo di apprendere ma di modificare autonomamente l'esperienza in base ai risultati ottenuti⁵⁹, un rischio riferibile, in primo luogo, ai *big data* i quali, per la loro quantità ed estrema velocità di impiego, sfuggono al controllo, su cui si fonda la protezione dei dati personali, riuscendo a fornire i migliori risultati proprio nelle analisi in cui non sono predefiniti gli obiettivi al momento della raccolta⁶⁰.

Vengono, così, sollevati cruciali interrogativi circa eventuali pericoli di discriminazione a svantaggio di categorie e gruppi sociali che potrebbero risultare penalizzati dal processo decisionale automatico⁶¹, potenziando tradizionali divari e tratteggiando nuove disparità digitali. «L'algoritmo disegna le modalità di funzionamento di larghe aree delle nostre organizzazioni sociali e così ridistribuisce poteri. Incarna anzi le nuove forme del potere e ne modifica la qualità (...). Nella vita quotidiana s'insinua il germe di nuove discriminazioni, nasce il cittadino non più libero, ma 'profilato', prigioniero di meccanismi che non sa o non può controllare»⁶². Tale condizione può verificarsi, inoltre, indipendentemente da errori o inesattezze riferibili alla procedura informatica⁶³, come nel caso dell'utilizzo di un algoritmo predittivo costruito su un set di dati *ab origine* discriminatorio, dando luogo ad una sua connotazione «strutturalmente» incostituzionale e, di riflesso, a decisioni sbilanciate⁶⁴, assecondando la logica *garbage in/garbage out* adottata dai sistemi automatici⁶⁵. Va, infatti, ricordato come i procedimenti di *machine learning* stabiliscano correlazioni senza esaminare i nessi di causalità producenti gli effetti rilevati, non essendo, in altri termini, in grado di comprendere il perché degli stessi e

⁵⁹ Cfr. ad es. P. Merialdo, *Aspetti etici circa la trasparenza degli algoritmi. Esplicabilità dell'intelligenza artificiale*, in G. Balbo, P. Jarre, *Manuale di InformEtica*, cit., p. 76.

⁶⁰ Cfr. F. Faini, S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, cit., p. 423.

⁶¹ Cfr. M. F. De Tullio, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 4/2016, p. 662.

⁶² S. Rodotà, *Il mondo nella rete*, cit., pp. 38-39.

⁶³ Cfr. G. De Minico, *op. cit.*, pp. 93-97.

⁶⁴ Cfr. A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal, Rivista di BioDiritto*, 1/2019, pp. 84-86.

⁶⁵ Cfr. P. Zuddas, *op. cit.*, p. 7.

supportando, di conseguenza, anche esiti fuorvianti⁶⁶. Consistenti pregiudizi possono, poi, derivare, oltre che dalla configurazione del set di dati, dal funzionamento dell'algoritmo⁶⁷, una questione che si complica in relazione all'elaborazione automatica di caratteri solo formalmente neutri, ma frequentemente ricorrenti in categorie sensibili, come nel caso delle *proxies*, spesso individuate autonomamente dal sistema informatico nell'apprendimento dal set di dati e, pertanto, difficilmente rilevabili⁶⁸. Tale procedimento renderebbe sempre più arduo risalire alle decisioni più distanti le quali, a loro volta, potrebbero essere fondate su trascorse selezioni algoritmiche discriminatorie⁶⁹, derivandone delle vere e proprie trappole invisibili⁷⁰. E 'evidente, poi, come decisioni formalmente corrette ed assunte su basi statistiche possano non risultare esatte in relazione al singolo caso, offrendo la statistica indicazioni di tendenze e *pattern* comportamentali⁷¹ maggiormente attendibili quanto più calibrate su di un effetto complessivo, piuttosto che locale⁷², ottenuto raggruppando i soggetti in classi omogenee⁷³. Gli stessi dati, infine, possono non essere oggettivi, ma offrire una rappresentazione del reale opportunamente modificata e finalizzata ad orientare i comportamenti tramite le informazioni prevalentemente diffuse⁷⁴. Numerosi esempi di quanto esposto provengono dal settore assicurativo, dalle pratiche di *credit scoring*, dal *dynamicprice*⁷⁵ – costituito dall'offerta di beni a prezzi differenziati a seconda di una presunta disponibilità ad acquistare dei consumatori, calcolata sulla base di tracce di dati rilasciate nel corso di precedenti ricerche o in rapporto alla fedeltà ad un determinato sito *on line* – dai sistemi di riconoscimento facciale, da programmi di giustizia predittiva – celebre il caso *Compass* nella

⁶⁶ Cfr. F. S. NUCCI, *RenAIssance e lo 'AI for Good': la strategia italiana per l'intelligenza artificiale*, in G. BALBO, P. JARRE, *Manuale di InformEtica*, cit., p. 97.

⁶⁷ Cfr. G. GRAZIANO, V. G. SAPUPPO, *Bias e Gender gap: le nuove discriminazioni del Machine Learning* in <https://generazioneepsilon.it/2021/04/21/bias-e-gender-gap-le-nuove-discriminazioni-del-machine-learning/>

⁶⁸ Cfr. S. TOMMASI, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, in *Revista de Direito Brasileira*, 10/2020, p. 115.

⁶⁹ Cfr. *ibidem*.

⁷⁰ Cfr. *ibidem*.

⁷¹ Cfr. M. NOUSSAN, *op. cit.*, p. 129.

⁷² Cfr. S. TOMMASI, *op. cit.*, p. 115.

⁷³ Cfr. A. C. AMATO MANGIAMELI, *Intelligenza artificiale, big data e nuovi diritti*, in *Rivista Italiana Di Informatica E Diritto*, 1/2022, p. 4.

⁷⁴ Cfr. A. C. AMATO MANGIAMELI, M. N. CAMPAGNOLI, *Strategie digitali. # diritto_educazione_tecnologie*, Giappichelli, Torino, 2020, pp. 58-59.

⁷⁵ Cfr. S. TOMMASI, *op. cit.*, pp. 120-121.

2/2023

valutazione della possibilità di recidiva di soggetti sottoposti a procedimento penale e rivelatosi discriminatorio in base al colore della pelle - e dal mondo del lavoro, basti ricordare il caso Deliveroo e l'utilizzo dell'algoritmo *Frank* nella selezione dei *rider* più veloci e laboriosi, non in grado di distinguere l'assenza dal lavoro per futili motivi da quella dovuta all'esercizio di diritti costituzionali quali il diritto di sciopero o il diritto alla salute, nonché i molteplici casi di discriminazione lavorativa algoritmica riferibili ad Amazon. Per tale ragione, la necessità di affermare i principi di uguaglianza e di non discriminazione, nell'ambito di provvedimenti assunti tramite l'intelligenza artificiale, è stata affermata in molteplici sedi come esemplarmente dimostra l'assiduo operato della European Commission for the Efficiency of Justice nel contrasto alle discriminazioni algoritmiche⁷⁶.

In definitiva, «la tesi della neutralità della tecnologia, che ha il pregio di sottolineare la responsabilità di chi la adopera, trascura il fatto che il concreto ruolo di una tecnologia deriva anzitutto dalla sua forma e dalle sue specifiche modalità d'uso, che contribuiscono a definirne senso e portata sociale»⁷⁷. Appare, dunque, di fondamentale rilevanza garantire, oltre alla qualità del *dataset*, la sua più ampia rappresentatività⁷⁸, focalizzando il momento della tutela non soltanto sul risultato della decisione algoritmica, ma, preventivamente, sui criteri e sulle modalità della programmazione, con il delineare i tratti di un'intelligenza artificiale sussidiaria e orientata da una costante sorveglianza umana⁷⁹. L'algoritmo può infatti, come si è detto, ereditare e riproporre radicati pregiudizi in una versione matematizzata, con imponenti ripercussioni sociali, politiche, giuridiche ed economiche⁸⁰ sollevando, in primo luogo in ambito giuridico e nel settore della giustizia predittiva, un problema di tracciabilità della decisione automatizzata, la cui complessità esclude, nella maggior parte dei casi, un controllo di congruità delle motivazioni decisionali⁸¹, come richiesto anche dall'art.13, dall'art. 22

⁷⁶ Sul punto, cfr. C.M. REALE, M. TOMASI, *op. cit.*, p. 333.

⁷⁷ S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, p. 28.

⁷⁸ Cfr. S. TOMMASI, *op. cit.*, p. 114.

⁷⁹ Cfr. C. CASONATO, *Costituzione e intelligenza artificiale*, cit., p. 722. Sulla *collaborative intelligence* si veda H.J. WILSON, P.R. DAUGHERTY, *Collaborative Intelligence: Humans and AI Are Joining Forces*, in *Harvard Business Review*, 2018, <https://hbr.org/2018/07/collaborative-intelligence-humans-and-ai-are-joining-forces>

⁸⁰ Cfr. A.C. AMATO MANGIAMELI, M.N. CAMPAGNOLI, *op. cit.*, p. 74.

⁸¹ Cfr. C. CASONATO, *Potenzialità e sfide*, cit., p. 180.

e dal Considerando n. 71 del GDPR⁸². A tal proposito, va messo in luce come, per chi veda violato un suo diritto, la dimostrazione che la decisione lesiva sia stata presa unicamente sulla base di un algoritmo appaia spesso una *probatio diabolica*, in quanto il decisore avrà sempre la possibilità di sostenere di essersi avvalso dell'algoritmo, non essendo stato propriamente sostituito da esso, senza considerare l'evidente forza cogente di ogni automatismo valutativo il quale, sollevando il decisore dal peso della motivazione, consente di conferire alla decisione gli attributi inattaccabili di una presunta scientificità e oggettività⁸³. D'altro canto, l'intelligenza artificiale potrebbe offrire un contributo positivo in termini di *debiasing* facendo emergere pregiudizi impliciti, in primo luogo laddove sia consentito produrre elementi di fatto idonei a fondare, in termini precisi e concordanti, la presunzione dell'esistenza di atti, patti o comportamenti discriminatori⁸⁴. In ogni caso, e in attesa di un consolidato orientamento giurisprudenziale su questi temi, si ritiene rispettato il principio di non esclusività della decisione algoritmica qualora il decisore umano sia in grado di motivare l'adesione alla valutazione automatica offrendo chiarimenti, in termini comprensibili, delle logiche a sostegno dell'autonomia decisionale⁸⁵. Se non sembra, infatti, possibile e neanche necessario comprendere ogni specifica fase del processo decisionale⁸⁶, i temi della trasparenza e della spiegabilità algoritmica si mostrano di fondamentale interesse nel dibattito sull'intelligenza artificiale, mettendo in luce la necessità di corredare la formula tecnica con osservazioni e delucidazioni in grado di tradurre la stessa in regola giuridica, rendendola il più possibile afferrabile⁸⁷. In questo modo, il diritto a conseguire una

⁸² Più esplicita nel riconoscere il diritto a un trattamento automatizzato il più possibile non discriminatorio, nel caso di decisione derivata da un trattamento di dati automatizzato, appare la Direttiva 2016/680/UE, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti alla prevenzione, indagine, accertamento di reati o esecuzione di sanzioni penali, cfr. S. TOMMASI, *op. cit.*, p. 120.

⁸³ Cfr. A. SIMONCINI, *op. cit.*, p. 81.

⁸⁴ Si veda P. PERLINGIERI, «Controllo» e «conformazione» degli atti di autonomia negoziale, in E. CATERINI, L. DI NELLA et. al (a cura di), *Scritti in onore di Vito Rizzo*, Edizioni Scientifiche Italiane, Napoli, 2017, pp. 1629 ss.

⁸⁵ Cfr. C. CASONATO, *Costituzione e intelligenza artificiale*, cit., pp. 722-723.

⁸⁶ Cfr. A. ALPINI, *Sull'approccio umano-centrico all'Intelligenza Artificiale. Riflessioni a margine del "Progetto europeo di orientamenti etici per una IA affidabile*, in *Comparazione e diritto civile*, 3/2021, pp. 4 ss.

⁸⁷ Cfr. S. TOMMASI, *op. cit.*, p. 119

motivazione⁸⁸ verrebbe esteso ad ogni decisione assunta automaticamente e capace di incidere sulla posizione giuridica dell'interessato⁸⁹. In secondo luogo, il diritto di ottenere una decisione in grado di produrre effetti giuridicamente rilevanti, riflettendosi significativamente sulla persona, che non sia interamente automatizzata, come previsto dall'art. 22 GDPR, si riconduce all'individuazione delle funzioni esercitate nel procedimento informatico e alla definizione delle sfere di responsabilità⁹⁰, elementi di difficile precisazione visto che, concretamente, possono mutare i livelli della partecipazione umana alla decisione⁹¹. Pressanti incognite gravano, dunque, sulle cosiddette «scelte etiche» degli agenti artificiali e sulla configurazione di forme di responsabilità da attribuire agli atti da essi compiuti, problemi per i quali possono non risultare sufficienti le consolidate categorie giuridiche⁹², evidenziando la necessità di un approccio proattivo ai sistemi di intelligenza artificiale, sin dalla fase di progettazione e nella prevenzione di eventuali disfunzioni⁹³. Questo appare, d'altro canto, il percorso intrapreso dall'«*Artificial Intelligence Act*» il quale, nell'intento comunitario di promuovere il progresso tecnologico assicurando un alto livello di protezione della salute, della sicurezza e dei diritti fondamentali degli individui, affronta anche il tema dell'utilizzo dell'intelligenza artificiale con finalità o modalità discriminatorie. Al riguardo, minimizzare il rischio di discriminazione algoritmica e sancire, contemporaneamente, un adeguato livello di trasparenza costituiscono specifici obiettivi del progetto formulato tenendo espressamente conto dei principi affermati dalla Carta dei diritti fondamentali dell'Unione europea, in particolare l'art. 21 sul divieto di discriminazione e, più in generale, di tutto il *corpus* del diritto antidiscriminatorio prodotto dall'Unione⁹⁴. Tale documento si sviluppa su di una valutazione del rischio in termini crescenti di basso, medio e alto, con riferimento alla possibilità di compressione dei diritti fondamentali e in rapporto alla disciplina antidiscriminatoria

⁸⁸ Tale diritto è previsto dall'art.111, 6 comma della Costituzione per i provvedimenti giurisdizionali e dall'art.3 della legge 241 del 1990 per quelli amministrativi.

⁸⁹ Cfr. C. CASONATO, *Costituzione e intelligenza artificiale*, cit., pp. 722-723.

⁹⁰ Cfr. *ivi*, 724. Sull'inadeguatezza delle tradizionali norme sulla responsabilità, si veda A. C. AMATO MANGIAMELI, M.N. CAMPAGNOLI, *op. cit.*, pp. 67-70.

⁹¹ Cfr. F. FAINI, *op. cit.*, p. 200; F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, cit., p. 421.

⁹² Cfr. *ivi*, p. 441.

⁹³ Cfr. *ivi*, p. 414, p. 448.

⁹⁴ Cfr. R. DE CARIA, *L'AI Act e il divieto di discriminazioni*, in *MediaLaw*, 2022, <https://www.medialaws.eu/lai-act-e-il-divieto-di-discriminazioni/>

dell'Unione europea⁹⁵ chiarendo come il contrasto alle discriminazioni debba avvenire sia nella progettazione sia nell'addestramento del *dataset*, ponendo particolare attenzione all'opacità algoritmica in relazione ai sistemi di IA ad alto rischio.

Nel delineare i tratti di un progresso tecnologico e informatico socialmente inclusivo⁹⁶, appare dunque questione fondamentale offrire una precisa direzione allo sviluppo e agli impieghi collettivi delle nuove tecnologie, in vista di una progressiva democratizzazione delle stesse⁹⁷, valorizzando, nel rapporto sempre più intenso tra uomo e macchina, i criteri della precauzione e della prudenza di fronte ad ogni eventuale rischio di discriminazione algoritmica⁹⁸. Con le parole di Cathy O'Neil nel denunciare i "danni collaterali", sul piano della disuguaglianza, derivati dall'impiego congiunto di big data e algoritmi predittivi: «L'ingiustizia, sia essa provocata dall'avidità o dal pregiudizio, accompagna l'uomo da sempre (...). Ma il processo decisionale umano, benché spesso viziato, ha una grande virtù, e cioè di potersi evolvere (...). I processi basati sui Big Data codificano il passato. Non inventano il futuro, cosa per la quale occorre la percezione che solo l'uomo possiede. Dobbiamo esplicitamente inglobare i valori più nobili nei nostri algoritmi, creando modelli basati sui Big Data che seguano la nostra guida etica. E talvolta questo comporta di dover anteporre l'equità al profitto»⁹⁹.

⁹⁵ Così recita, infatti, la disposizione in esame: "La presente proposta integra [...] il diritto dell'Unione in vigore in materia di non discriminazione con requisiti specifici che mirano a ridurre al minimo il rischio di discriminazione algoritmica, in particolare in relazione alla progettazione e alla qualità dei set di dati utilizzati per lo sviluppo dei sistemi di IA, integrati con obblighi relativi alle prove, alla gestione dei rischi, alla documentazione e alla sorveglianza umana durante l'intero ciclo di vita dei sistemi di IA".

⁹⁶ Cfr. L. PEYRON, *Il digitale per l'uomo e non l'uomo per il digitale*, cit., p. 182.

⁹⁷ Cfr. L. FLORIDI, *Il Verde e il Blu*, in G. Balbo, P. Jarre, *Manuale di InformEtica*, cit., p. 36. Si vedano, a tal proposito, i principi enucleati, nel 2018, dall'European Group on Ethics in Science and New Technologies presso la Commissione europea nel documento *Statement on Artificial Intelligence, Robotics and 'Autonomous Systems'*.

⁹⁸ Cfr. S. RODOTÀ, *Il mondo nella rete*, cit., p. 40.

⁹⁹ C. O'NEIL, *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia*, Bompiani, Milano, 2017, pp. 293-294. Sulla necessità di delineare un *tecno-diritto* quale insieme di norme e procedure prodotte dalla sinergia tra tecnica e diritto, di corredare i più attuali sistemi di intelligenza artificiale con principi etici e giuridici ed, infine, di tratteggiare nuove soluzioni giuridiche maggiormente adeguate nell'attribuzione di responsabilità, si veda A.C. AMATO MANGIAMELI, M.N. CAMPAGNOLI, *op. cit.*, pp. 69-71.

5. Accesso e informazione

La rilevanza della conoscenza nell'era digitale delinea, come si è visto, nuove vulnerabilità precipuamente associate al mondo virtuale e all'informazione in esso veicolata, nell'assenza di effettive condizioni di parità che consentano all'innovazione di fornire i migliori servizi¹⁰⁰, in modo particolare ai più anziani e ai portatori di disabilità, bisognosi di un'assistenza informatica specifica e ulteriore¹⁰¹, problemi e sfide di fronte alle quali la disciplina vigente sembra, talvolta, arrancare¹⁰². In particolare, il superamento del tradizionale concetto di informazione, quale strumento di pertinenza e di disponibilità soggettiva, a favore di procedimenti sempre più autonomi nell'assunzione di decisioni rilevanti per l'uomo e la sua libertà¹⁰³, conduce a delineare l'accesso ad Internet come un diritto fondamentale della persona, svincolandone la tutela dall'eventuale attenzione e dalla consapevolezza informatica del soggetto interessato, in ogni caso parte debole nel rapporto con le forze di mercato¹⁰⁴. Le tecnologie digitali, in altri termini, impongono una sensibile ridefinizione delle modalità conoscitive e, più in generale, di approccio alla realtà, tale che l'esclusione dall'accesso o da un efficiente utilizzo delle stesse rischia di approfondire preesistenti distanze generazionali, sociali, economiche e culturali¹⁰⁵. Pertanto, superando la classica e riduttiva dicotomia tra *have* e *have-nots*, il *digital divide* indica, più propriamente, la distanza «tra chi dispone degli strumenti e delle competenze utili ad accedere e ad usufruire proficuamente delle opportunità offerte dalle tecnologie di comunicazione e chi ne è escluso»¹⁰⁶ ricomprendendo, tra gli strumenti, la copertura di Rete del territorio e la disponibilità di connessione, mentre, per ciò che concerne le competenze, l'alfabetizzazione informatica appare quale primaria causa di discriminazione¹⁰⁷. L'assunzione di un'ottica multidimensionale porta,

¹⁰⁰ Cfr. S. TOMMASI, *op. cit.*, p. 124.

¹⁰¹ Cfr. *ibidem*.

¹⁰² Cfr. E. STRADELLA, *La regolazione della Robotica e dell'intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, in *MediaLaws*, 2019, p. 86.

¹⁰³ Cfr. A. SIMONCINI, *op. cit.*, p. 69.

¹⁰⁴ Cfr. F. FAINI, *op. cit.*, p. 33.

¹⁰⁵ Cfr. S. VANTIN, *Digital divide. Discriminazioni e vulnerabilità nell'epoca della rete globale*, in T. CASADEI, S. PIETROPAOLI, *Diritto e tecnologie informatiche*, Wolters Kluwer, Lavis, 2021, p. 233.

¹⁰⁶ P. ZUDDAS, *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio Costituzionale*, 3/2020, p. 286.

¹⁰⁷ Cfr. *ibidem*.

dunque, ad emergere le problematiche ricollegabili al divario digitale o, meglio, ai divari digitali espressi dalle «molteplici linee di esclusione, spesso sovrapposte, che riducono l'accesso e l'utilizzo delle tecnologie, perlopiù a causa di diseguaglianze pregresse, quali ad esempio il genere, il livello di istruzione, l'età e il reddito, il cui impatto non grava soltanto sull'equità ma anche sotto il profilo dell'efficienza e dello sviluppo economico»¹⁰⁸. Va, infatti, rilevato come, attualmente, il divario digitale rappresenti una delle più significative cause di esclusione sociale essendo l'accesso ad Internet e la capacità di operarvi con consapevolezza tra i più significativi presupposti di una piena espressione personale e di una completa partecipazione alla vita sociale, politica ed economica¹⁰⁹, richiamando quanto disposto dagli artt. 2 e 3 della Costituzione e facendone derivare il compito dei pubblici poteri di rimuovere gli ostacoli all'accessibilità e alla fruizione della Rete¹¹⁰.

Tale necessità è stata drammaticamente evidenziata dalla recente pandemia da Covid-19 la quale, nel rilevare il ruolo essenziale delle reti di telecomunicazione e del possesso di un'adeguata cultura digitale nello svolgimento di imprescindibili funzioni pubbliche e nel godimento di fondamentali diritti sociali (salute, istruzione, lavoro), ha, d'altro canto, acuito il *digital divide* tra coloro che hanno accesso ad Internet e coloro che non ne dispongono, tra chi ha accesso alla banda ultralarga e chi ne è privo, tra chi possiede un'adeguata alfabetizzazione informatica ed appropriate competenze digitali e chi ne è carente, implementando preesistenti criticità¹¹¹. Si può, dunque, ben comprendere come il *digital divide*, estendendosi oltre il possesso o meno di conoscenze e abilità tecnico-informatiche¹¹², declini un concetto sfaccettato e dinamico, tracciato, in

¹⁰⁸ S. VANTIN, *op. cit.*, 233-234. Basti pensare al divario sussistente tra Paesi industrializzati e Paesi in via di sviluppo per comprendere come le limitazioni all'accesso alle nuove tecnologie precludano molte possibilità di crescita economica di questi ultimi. Com'è noto, per comprendere l'intensità del divario digitale, sono utilizzati gli indicatori *HDI-Human Development Index* - con il quale viene considerato il livello di sviluppo di un Paese principalmente attraverso il tasso di istruzione, del PIL e delle aspettative di vita - e *TAI-Technological Achievement Index*, basato sulla creazione e diffusione delle nuove tecnologie, classificando gli Stati in leader, leader potenziali, utilizzatori dinamici e utilizzatori marginali.

¹⁰⁹ Cfr. P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in *Consulta online*, 2020, p. 287.

¹¹⁰ Cfr. S. VANTIN, *op. cit.*, p. 237.

¹¹¹ Cfr. *ivi*, pp. 291-297. In particolare, nel settore delle competenze digitali, il Covid-19 ha provocato un vero e proprio *shock* culturale digitale, legato all'«alfabetizzazione digitale forzata» originata dall'emergenza pandemica, cfr. *ivi*, p. 305.

¹¹² Cfr. *ivi*, p. 289.

primo luogo, dalla distanza tra coloro che dispongono di un sufficiente livello di consapevolezza per navigare in Rete, selezionandone opportunamente le fonti informative ed orientandosi tra sottili forme di profilazione¹¹³. Secondariamente, come si è potuto, ancora una volta, osservare nell'emergenza pandemica da Covid-19, ottenuto l'accesso, variabili strutturali quali, ad esempio, i mezzi tecnici a disposizione e la loro qualità, il sostegno di reti sociali, l'autonomia e la varietà di uso, appaiono tutt'altro che ininfluenti e, a tali fattori, possono aggiungersi ulteriori elementi di disuguaglianza riferibili a personali risorse motivazionali, culturali, cognitive ed economiche¹¹⁴.

I divari digitali, in definitiva, nel rafforzare pregresse disuguaglianze sociali, economiche e culturali, delineano inedite forme e pratiche di stratificazione quali discriminazioni reali e certamente non superabili attraverso una diffusione tecnologica che non implichi, altresì, l'adozione di mirate «politiche dell'uso»¹¹⁵ e di azioni di regolazione consapevole¹¹⁶. In ogni caso, e indipendentemente dal riconoscimento di un vero e proprio diritto costituzionale di accesso ad Internet¹¹⁷, sono da tempo presenti, nel nostro ordinamento, Dichiarazioni e norme di rango primario volte a favorire un'effettiva disponibilità di connessione e gli strumenti di base per la navigazione in Rete, nonché a stimolare una concreta fruizione dei diritti di cittadinanza digitale¹¹⁸. Tali concetti sono stati, in linea di principio,

¹¹³ Cfr. A. ALPINI, *Digital divide*, cit., p. 882. Per tali ragioni, è auspicato un mutamento della tradizionale concezione dello stato di bisogno e dello stato di pericolo estendendo il concetto di disuguaglianza all'incompetenza tecnologica, cfr. ad es. E. NAVARRETTA, *Principio di eguaglianza e diritto civile*, in *Questione Giustizia*, 2020, pp. 23-27.

¹¹⁴ Cfr. L. SARTORI, *Il divario digitale. Internet e le nuove disuguaglianze sociali*, il Mulino, Bologna, 2006, pp. 133-134.

¹¹⁵ Ivi, p. 168.

¹¹⁶ Cfr. ivi, pp. 20-21.

¹¹⁷ Sul diritto di accesso ad Internet come diritto sociale o a prestazione, si veda T.E. FROSINI, *Il diritto costituzionale di accesso ad Internet*, in ITTIG-CNR, «Studi e documenti», 9/2011, Edizioni Scientifiche Italiane, Napoli, pp. 32-35. Sul dibattito italiano intorno al riconoscimento costituzionale del diritto di accesso, cfr. M. OLIVETTI, *Diritti fondamentali e nuove tecnologie: una mappa del dibattito italiano*, in *Journal of Institutional Studies*, 2/2020, pp. 395-430.

¹¹⁸ Cfr. S. SCAGLIARINI, *I diritti costituzionali nell'era di internet: cittadinanza digitale, accesso alla rete e net quality*, in T. CASADEI, S. PIETROPAOLI, *Diritto e tecnologie informatiche*, cit., pp. 6-10. Possiamo qui ricordare una prima risposta offerta dal *Piano strategico nazionale per lo sviluppo della banda ultralarga e la crescita digitale* - approvato dal Governo il 3 marzo 2015 ed accompagnato da un accordo quadro con le Regioni siglato l'11 febbraio 2016 – così come, più in generale, le norme in materia contenute nel Codice dell'amministrazione digitale (CAD), nonché il *Decreto Cura Italia*, dl. 17 marzo 2020 n. 18, contenente norme rivolte, tra

espressi dalla *Carta dei Diritti di Internet*, resa pubblica il 13 ottobre 2015 presso la Sala della Regina di Palazzo Montecitorio, un documento che, pur risultando privo di forza vincolante e prescrittiva, svolge, tuttavia, una significativa funzione di *moral suasion*¹¹⁹, rappresentando una guida nella promozione di norme sul digitale e, prima ancora, nella valorizzazione di una società della dignità, dell'uguaglianza e della partecipazione¹²⁰. La Carta delinea l'accesso a Internet come diritto fondamentale e come condizione del pieno sviluppo individuale e sociale, indicando le pubbliche istituzioni come i soggetti deputati ai necessari interventi di superamento di ogni forma di dislivello digitale determinata dal genere, dalle condizioni economiche e da situazioni di vulnerabilità e disabilità¹²¹, tematiche parzialmente sviluppate, in tempi più recenti, dal PNRR nel valorizzare la connettività dei cittadini e delle PA, la loro interazione e prevedendo interventi nel sistema produttivo, nel turismo e nella settore della cultura¹²².

In prospettiva, la rapidità di innovazione tecnologica sembra richiedere un forte impegno di educazione e di formazione continua rivolto non solo ai soggetti direttamente coinvolti nella gestione delle tecnologie digitali, ma esteso ad ogni cittadino¹²³, valorizzando l'inclusione dei più fragili sin dalla fase di progettazione delle soluzioni tecnologiche, in modo tale da conseguire "non solo un generico riconoscimento della libertà in rete, ma la concreta possibilità di esercitare 'virtù civiche', dando corpo a una cittadinanza attiva"¹²⁴.

gli altri obiettivi, a ridurre il *digital divide* sia sotto il profilo tecnologico sia in una più ampia direzione di superamento delle disparità culturali, economiche e sociali, cfr. P. ZUDDAS, *Covid-19 e digital divide*, cit., pp. 290-299.

¹¹⁹ Cfr. F. FAINI, *op cit*, p. 51.

¹²⁰ Cfr. S. RODOTÀ, *L'uomo nuovo di Internet*, cit.

¹²¹ https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf

¹²² Cfr. F. SCIAUDONE, *Digitalizzazione, innovazione, competitività, cultura e turismo*, in: *Guida al PNRR. Opportunità, procedure e adempimenti per imprese, professionisti e pubblica amministrazione*, il Sole 24 ORE, pp. 29-38.

¹²³ Cfr. P. ZUDDAS, *Covid-19 e digital divide*, cit., p. 305.

¹²⁴ S. RODOTÀ, *Il mondo nella rete*, cit., p. 71.