

Margherita Vestoso\*

*Diritto e tecnologia: una riflessione critica sui contenuti  
di un rapporto in continua evoluzione\*\**

*Abstract:* The work reviews “Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali”, a book edited by Thomas Casadei and Stefano Pietropaoli, offering insights on how digital society has transformed the relationship between law and technology. Resulting from an interesting interdisciplinary reflection, the essays presented in the book try to shed light, in particular, on the numerous and complex issues that cross such a scenario which is partly still unexplored. Our work aims to sketch, in its essential features, the path traced by these reflections, taking into account the plurality of the themes dealt with, the different angles, and the numerous points of contact that put the same topics in close communication with one another.

*Keywords:* Legal informatics, Law, Open data, Algorithmic governance, Technoregulation

## 1. Introduzione

Da sempre, la narrazione sulle origini dell’Informatica giuridica è accompagnata dalla distinzione fra lo studio dei processi regolativi che hanno ad oggetto la tecnologia (ossia, il *diritto dell’informatica*) e l’approfondimento delle soluzioni informatiche che possono contribuire al miglioramento dell’attività pratica e di ricerca dei giuristi (ossia, l’*informatica del diritto*).

La rivoluzione digitale ha tuttavia reso la tecnologia il fulcro intorno al quale orbita gran parte della vita degli individui, trasformandola nella fonte di servizi, processi informativi e modelli di accesso alla conoscenza precedentemente inediti. Si tratta di fenomeni che hanno contribuito a modellare le dinamiche più profonde della società, ridefinendone valori, costumi e istituzioni. Il rigore di quel distinguo ha finito così per scontrarsi con l’impossibilità di separare in modo nitido lo studio propedeutico all’identificazione dei rischi e dei confini normativi della tecnologia dall’esplorazione dei vantaggi, offerti da quest’ultima, sul piano dei contenuti, degli strumenti conoscitivi e della disponibilità di nuovi modelli operativi.

\* Assegnista post-dottorato, Università degli studi di Napoli “Federico II”, Dipartimento di Giurisprudenza.

\*\* Recensione al volume Th. Casadei, S. Pietropaoli (a cura di) (2021), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Kluwer.

L'idea di una separazione netta fra le questioni di diritto dell'informatica e quelle di informatica del diritto è andata così in crisi, spingendo una parte della comunità giuridica a ricercare nuove letture del rapporto fra diritto e tecnologie, capaci di un inquadramento più ampio ed organico dei temi che ruotano intorno ad esso<sup>1</sup>.

Rivisitando in modo originale lo schema tradizionale del manuale universitario, il volume "Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali", a cura di Thomas Casadei e Stefano Pietropaoli, si confronta con questa sfida, provando ad attraversare in maniera trasversale lo spettro delle questioni riconducibili all'interazione fra diritto e tecnologie digitali.

Il volume, parte della Collana COMPLEX – Diritto, computazione, complessità, diretta dagli stessi Autori, si pone all'esito di un interessante percorso di riflessione interdisciplinare<sup>2</sup>.

Nelle prossime pagine si proverà a ricostruire, nei suoi tratti essenziali, il percorso tracciato da questa riflessione, tenendo conto della pluralità dei temi trattati ma anche dei numerosi punti di contatto che pongono gli stessi temi in stretta comunicazione gli uni con gli altri, delineando una visione comprensiva e d'insieme.

## 2. Il diritto nella società digitale: un quadro complesso

I contributi presentati all'interno del volume provano a raccontare le molteplici problematiche giuridiche cui lo sviluppo tecnologico ha esposto – e continua ad esporre – il diritto, nonché le sfide etico-sociali generate da questioni indubbiamente complesse.

Il pubblico di riferimento non è rappresentato, pertanto, dai soli giuristi in formazione, ma da tutti coloro che si relazionano con il mondo del diritto, dagli operatori agli studiosi ai privati cittadini, che potranno trovare nell'opera nozioni e spunti essenziali allo sviluppo di un'interazione consapevole con i fenomeni della società digitale.

Anche per questo, i contenuti del volume sono presentati secondo una struttura modulata su quattro macroaree di interesse.

La Parte I, che accoglie i contributi di Simone Scagliarini (pp. 3-12), Fernanda Faini (pp. 17-28), Noemi Miniscalco (pp. 31-42), Gianluigi Fioriglio (pp. 45-54) e Gianmarco Gomez (pp. 57-63), si occupa di tratteggiare le caratteristiche salienti dell'interazione fra tecnologia, diritti fondamentali e istituzioni, mettendo in ri-

1 Spunti in questa direzione possono essere tratti da letture diverse. A titolo puramente esemplificativo, si v. Faini & Pietropaoli 2021 [2017]; Taddei Elmi 2014; Sartor 2014; Fioriglio 2004. Per un approfondimento sulla riflessione giusfilosofica che ha accompagnato l'emergere dell'Informatica giuridica quale autonoma disciplina, si v., a titolo esemplificativo, Frosini 1975: 26-35; Losano 1971: 867-871.

2 I contenuti sono il frutto di elaborazioni maturate grazie alla collaborazione tra il Laboratorio "Hans Kelsen" dell'Università di Salerno, l'Officina informatica su "Diritto Etica Tecnologia – DET" del CRID – Centro di Ricerca su Discriminazioni e vulnerabilità dell'Università di Modena e Reggio Emilia e gli studiosi e le studiose che hanno preso parte a "Keywords. Le parole del nuovo diritto", una serie di incontri seminariali realizzato presso l'Università di Firenze.

salto il nuovo significato che all'interno di questa interazione assumono principi come quello di *eguaglianza, trasparenza amministrativa, riservatezza, tutela della salute, democrazia*.

La Parte II è invece dedicata all'impatto esercitato dal processo di digitalizzazione sulla sfera giuridica soggettiva dei privati. Filippo Murino (pp. 71-86), Iacopo Senatori (pp. 91-101), Federico Costantini (pp. 105-117), Sandro Luce (pp. 121-129) e Raffaella Brighi (pp. 135-144) affrontano il tema da angolazioni diverse, riflettendo, ciascuno in relazione ad un particolare aspetto, sulla natura dei diritti e sulle nuove forme tutela che vengono oggi configurandosi nel variegato scenario della società digitale. I temi trattati vanno dalle nuove espressioni della documentalità nel contesto giuridico (si pensi al documento informatico e agli smart contract) ai controversi profili dello smart working, dalla giustizia elettronica alle strategie informatiche idonee a garantire la sicurezza pubblica e privata dei dati.

La parte III, scandita dai contributi di Michele Ferrazzano (pp. 151-161), Francesco di Tano (pp. 165-176), Chiara Celesti e Stefano Dorigo (pp. 179-185), Diego Mauri (pp. 191-202), Elisa Orrù (pp. 203-212), guarda invece alla dimensione processuale dell'innovazione tecnologica, riflettendo sul tipo di supporto che quest'ultima può offrire all'attività dei magistrati, sulle recenti declinazioni del concetto di reato informatico e sui rischi che si annidano nel ricorso inconsapevole a strumenti algoritmici di sorveglianza.

La Parte IV, infine, offre una riflessione di taglio giusfilosofico e sociologico-giuridico sul progresso tecnologico e sulle profonde trasformazioni sociali da questo indotte. Con i loro contributi, Thomas Casadei e Stefano Pietropaoli (pp. 219-230), Serena Vantin (pp. 233-244), Barbara Giovanna Bello (pp. 247-260), Valeria Marzocco (pp. 263-272) e Rosaria Piroso (pp. 275-284) provano a far luce sul ruolo ambivalente che l'intelligenza artificiale può svolgere nel mondo del diritto e, più in generale, nella società, trasformarsi facilmente da mezzo di discriminazione in strumento di contrasto alle ingiustizie. Gli Autori e le Autrici estendono qui l'esplorazione del rapporto diritto e tecnologia alla dimensione culturale ed etica, concentrandosi sulle questioni poste da temi come il divario digitale, l'odio in rete ovvero la tutela giuridica del "corpo elettronico", emblemi di quel processo di virtualizzazione dell'esistenza sul quale sembra impernarsi il funzionamento della società algoritmica.

Nei paragrafi che seguono proveremo ad approfondire alcune delle questioni affrontate all'interno dell'opera, riproponendo, in un'ottica di continuità logica con le riflessioni offerte dai diversi Autori e Autrici, lo schema in quattro parti che ne caratterizza la struttura complessiva.

### 3. Diritti fondamentali e istituzioni nell'era della digitalizzazione

Nell'introdurre la prima parte del volume, Simone Scagliarini pone in evidenza un concetto tanto semplice quanto essenziale, quello secondo cui diritti costituzionali ed evoluzione della tecnica sono legati da un rapporto di reciproca evoluzione. Se i primi, infatti, pongono le condizioni perché la seconda si realizzi, quest'ultima, una

volta avveratasi, finisce per incidere sulla forma dei primi, partecipando al loro incessante mutamento. Un processo divenuto ancor più evidente nello scenario della società digitale, e che è andato accentuandosi durante l'emergenza pandemica, che ha portato con sé l'ineludibile bisogno di ricorrere agli strumenti informatici e alla rete.

Tutto ciò, precisa Scagliarini, ha contribuito ad ampliare il peso costituzionale di problemi, già esistenti, in vario modo collegati all'uso di questi strumenti. Il primo, è quello del *digital divide*, ossia dal diverso grado di accesso alla tecnologia che, per motivi di età, genere, scolarizzazione o disponibilità di risorse economiche, si registra tra le diverse fasce della popolazione. Il secondo è quello delle discriminazioni derivanti dalle deroghe al principio della *net neutrality*<sup>3</sup> che, ove esistenti, lasciano i provider dei servizi di rete liberi di operare delle differenziazioni sul piano dei contenuti accessibili agli utenti e delle modalità di accesso al servizio. Problemi che restano ancora oggi in attesa di risposte adeguate.

Occorre sottolineare, peraltro, che il bisogno di definire con maggiore chiarezza i confini costituzionali del legame fra i cittadini e la rete non è certamente nuovo. Già da qualche tempo si discute sull'opportunità o meno di una modifica alla Carta costituzionale volta all'introduzione di un autonomo diritto di accesso alla Rete, intesa come luogo virtuale di esercizio dei diritti di cittadinanza. Nel suo contributo, Fernanda Faini riflette su questo tema evidenziando come il riconoscimento di specifici diritti digitali ai cittadini – sia esso di natura costituzionale o meno – porti con sé la speculare esigenza di cogliere il ruolo che le istituzioni sono chiamate a svolgere in questo contesto.

Come sottolineato dall'Autrice, la rinnovata fisionomia della società contemporanea, innescata dalle tecnologie informatiche, ha determinato l'evoluzione di nuovi modelli di governo: il volto della pubblica amministrazione si è trasformato, nel tentativo di far fronte in maniera efficace alle esigenze poste dalle nuove espressioni della società. Queste evidenze legittimano, secondo Faini, una rivisitazione dello stesso concetto di amministrazione digitale, da intendersi sempre più come ripensamento delle logiche e dei processi che scandiscono l'azione pubblica. La digitalizzazione potrebbe infatti aprire le porte ad una semplificazione dei processi di accesso, consultazione e riutilizzo dei dati e degli strumenti su cui si fonda l'azione della pubblica amministrazione, rendendo l'operato di quest'ultima più visibile e insieme più consapevole<sup>4</sup>.

3 Il concetto di *net neutrality* è proposto dall'Unione Europea con il regolamento 2015/2120. L'articolo 3 di questo regolamento chiarisce che i fornitori di servizi di accesso a internet, nel fornire tali servizi, trattano tutto il traffico allo stesso modo, senza discriminazioni, restrizioni o interferenze, e a prescindere dalla fonte e dalla destinazione dei contenuti cui si è avuto accesso o che sono stati diffusi, dalle applicazioni o dai servizi utilizzati o forniti, o dalle apparecchiature terminali utilizzate.

4 Si segnala che alcune recenti riforme sembrano guardare in questa direzione. Accanto al già noto Codice dell'Amministrazione Digitale (CAD), che si occupa di definire il contenuto dei diritti digitali dei cittadini nei confronti delle pubbliche amministrazioni, un ruolo importante in questo senso va riconosciuto anche alla l. 124/2015, cd. *Legge Madia*, che nel riformare la PA ha provato a spostare la prospettiva della digitalizzazione dalle amministrazioni ai cittadini. Per un approfondimento sul tema, si v. Carloni 2019 :363-392.

Peraltro, come evidenzia Gianmarco Gomez con il suo contributo, a trarre beneficio da un processo di digitalizzazione della PA inteso in questi termini non è solo la trasparenza ma la stessa partecipazione alla vita democratica del Paese. La possibilità di leggere in chiaro le attività compiute dagli amministratori pubblici, a tutti i livelli, rende più semplice non solo il controllo sull'operato di questi ultimi ma anche il trasferimento in spazi virtuali condivisi della discussione che precede il processo decisionale. Seppur distinti, dunque, i concetti di *cittadinanza digitale*, *open-government* e *e-democracy* restano tra loro fortemente interconnessi e destinati a crescere secondo un modello sinergico.

Naturalmente, perché questo modello funzioni, è necessario che la persona resti al centro, con tutti i suoi interessi e bisogni. La ricerca dell'innovazione deve accompagnarsi ad una riflessione strutturata sui rischi che la tecnologia porta con sé, in termini di violazione della privacy o di discriminazioni. Interessanti spunti in questa direzione possono essere tratti dal contributo di Noemi Miniscalco che prova a far luce sulle declinazioni che la tutela della personalità assume nella società digitale. L'Autrice si concentra, in particolar modo, su tre declinazioni del concetto di personalità: *protezione dei dati personali*, *tutela dell'identità personale* e *diritto all'oblio*. Di queste declinazioni esamina, accanto alla storia e alle evoluzioni, l'interazione con lo spazio ambiguo della rete, alla luce dello stretto legame che ciascuno di essi presenta oggi con Internet e con le nuove modalità di produzione e utilizzazione della conoscenza da questo abilitate.

Il messaggio che emerge dalle parole dell'Autrice è che, al netto delle garanzie normative esistenti, i singoli devono sforzarsi di agire in maniera consapevole sul web, rappresentandosi le potenziali conseguenze delle proprie operazioni. Se il legislatore è il principale responsabile dell'evoluzione che i citati diritti possono subire nell'interazione con la rete, una parte di responsabilità resta pur sempre in capo ai cittadini, che sono chiamati a sfruttare i vantaggi di Internet senza mai smettere di essere vigili rispetto ai rischi che esso comporta.

L'invito a condividere informazioni in maniera oculata vale ancor più, peraltro, quando ci si muove in un'area particolarmente delicata com'è quella della salute. Al tema dà voce Gianluigi Fioriglio che illustra molto dettagliatamente l'emergente fenomeno dell'*e-health* evidenziandone sfumature tecnologiche e giuridiche. L'attenzione ricade, in particolare, sul diverso regime cui sono sottoposte le tecnologie che attraversano il mondo sanitario. Se con riguardo ai dispositivi medici, infatti, il legislatore si è premurato di fissare confini ben precisi, lo stesso non può dirsi per dispositivi e servizi di natura commerciale che, pur interagendo con dati relativi alla salute degli utenti, operano all'interno di una sorta di *zona grigia*.

La disparità di regime assume ancor più rilievo se combinata con la recente evoluzione algoritmica del settore sanitario, basata sull'impiego sempre più frequente di sistemi di *machine learning* capaci di sfruttare dati sensibili per effettuare ogni genere di inferenza<sup>5</sup>. I pericoli che si pongono in questo senso, secondo Fioriglio,

5 Per un approfondimento sui fattori che spingono a mettere in discussione l'affidabilità

vanno in due direzioni: da un lato, c'è il timore che questo genere di strumenti possa essere utilizzato per finalità non legate al mondo sanitario e addirittura illecite; dall'altro, il rischio di fare eccessivo affidamento sulla neutralità e qualità delle risposte fornite da tali sistemi, anche quando usati a supporto di decisioni di natura medica.

L'esigenza che emerge, con tutta evidenza, è quella di una più attenta ed organica regolazione di questo complesso scenario, che sappia bilanciare la spinta verso lo sviluppo di strumenti utili e innovativi con l'irrinunciabile bisogno di tutelare la persona e la sua dignità.

#### 4. Diritti dei privati e nuove tutele nella società digitale

La Parte II del volume, come anticipato, guarda al mondo dei diritti dei privati e alle nuove forme di tutela che vengono oggi configurandosi per effetto della loro interazione con la tecnologia.

Il contributo di Filippo Murino, che apre questa seconda parte, si concentra in particolare sul rapporto fra tecnologia e "documentalità". Nel ripercorrere le principali fasi evolutive del concetto di documento informatico, l'Autore pone in evidenza le questioni che nascono dall'incontro fra i meccanismi già noti di autenticazione e conservazione dei documenti informatici e la tecnologia *blockchain*, con un occhio particolare ai rischi che si annidano nel connesso fenomeno degli *smart contract*.

Il modello tradizionale, che chiedeva di affidare ad un ente terzo autorevole (un pubblico ufficiale o un privato accreditato) il processo di gestione e certificazione dei documenti, è stato in effetti messo in crisi dal sistema decentralizzato della *blockchain*, che suddivide il peso computazionale del processo di gestione in pacchetti distribuiti lungo una rete di computer (i nodi) capaci, in quanto connessi a internet, di scambiare informazioni in maniera autonoma, senza alcuna autorità di vigilanza centrale. La logica *peer-to-peer* e il peculiare sistema di marcatura temporale che caratterizzano questa tecnologia offrono, senza dubbio, dei vantaggi sul piano dell'affidabilità del processo e della riduzione del rischio di corruzione. Tuttavia, come ricorda Murino, le criticità non mancano. Emblematico è il caso degli *smart contract*, dove la *blockchain*, da un lato, semplifica la fase di esecuzione e conferisce maggiore trasparenza alle obbligazioni, dall'altro, conferisce estrema complessità al contratto, rendendone difficile l'analisi in sede giudiziaria.

Occorre precisare, peraltro, che lo sviluppo di tecniche informatiche di ottimizzazione sempre più raffinate ha indirizzato verso una logica "smart" non solo la contrattazione, ma anche il mondo del lavoro. Come racconta Iacopo Senatori nel suo contributo, la trasformazione digitale ha esercitato un impatto importante su forma, contenuti e modelli di gestione del rapporto di lavoro, con conseguenze spesso contraddittorie. Nel delineare le caratteristiche dello *smart working*, l'Auto-

re sottolinea infatti come questo modello, che pure consente una maggiore flessibilità e un miglioramento dei processi di organizzazione e produzione, apra le porte a rischi significativi sul piano della tutela dei lavoratori e delle lavoratrici.

Uno di questi è senza dubbio l'*iperconnettività*. La disponibilità di tecnologie che consentono al lavoratore di prestare la propria attività rimanendo connesso in modo potenzialmente illimitato con colleghi e superiori rischia di far sfumare il confine tra i tempi del lavoro e quelli della vita privata. A questo rischio, in parte arginato dall'introduzione di previsioni normative ad hoc, se ne aggiungono altri. Le modalità delocalizzate di svolgimento della prestazione, su cui si fonda lo *smart working*, potrebbero infatti favorire un'alterazione dell'equilibrio dei poteri fra datore e prestatore di lavoro, o compromettere l'integrità psicofisica dei lavoratori o, ancora, aprire le porte a vulnus di tipo informatico e rendere possibile la violazione di dati sensibili dei lavoratori.

Quest'ultimo profilo problematico si collega alla riflessione presentata da Raffaella Brighi in tema di sicurezza informatica, ove si evidenzia il ruolo centrale rivestito in questo senso dalla predisposizione di misure organizzative e tecniche orientate al controllo del rischio. Nel suo discorso, Brighi opera una differenziazione sul piano dei vulnus informatici che possono mettere a rischio la sicurezza di un sistema, cui si ricollegano conseguenze spesso molto diverse. Un'attenzione particolare è dedicata, in questo senso, ad alcune forme recenti di cyber minacce, come le guerre di informazioni (*information warfare*), capaci di modificare in maniera silente i rapporti fra gli stati, o le evoluzioni del crimine informatico ispirate al modello del *Crime as a service*, basate sull'offerta di software che consentono di sferrare attacchi informatici senza il bisogno di particolari competenze tecniche nel settore.

Lo scenario descritto conferma l'idea che la tecnologia tenda oggi a produrre sempre più spesso cambiamenti sostanziali, generando nuovi fenomeni collettivi, nuove fattispecie di interesse giuridico, e non semplici aggiornamenti formali delle attività che scandiscono il vivere sociale. Il discorso, come si è già avuto modo di osservare, è trasversale, interessando contesti molto diversi fra loro, dall'amministrazione pubblica al mondo del lavoro, dalla partecipazione democratica alla criminalità.

In alcuni settori, la natura sostanziale del cambiamento è probabilmente anche più visibile che in altri.

È così, ad esempio, per il diritto d'autore, istituto giuridico che, come segnalato da Sandro Luce nel suo intervento, molto ha risentito dell'avvento della rivoluzione digitale. Il modo di articolarsi della creatività intellettuale e delle relative tutele è infatti fortemente mutato per effetto di Internet e dello sviluppo di modalità alternative di diffusione della conoscenza, che hanno reso possibili nuove forme di creazione, distribuzione e acquisizione di opere letterarie e artistiche.

Il problema è, secondo l'Autore, nell'inadeguatezza della risposta giuridica a questo mutamento. Gli Stati Uniti, ad esempio, hanno reagito rafforzando le garanzie delle grandi compagnie di produzione. La stessa tecnologia è stata impiegata in questo senso, con i sistemi di *Digital Rights Management* che sfruttano misure crittografiche di protezione per amplificare la dimensione delle limitazioni. Una soluzione che ha finito sostanzialmente per ampliare le ipotesi di violazione del

diritto d'autore, mancando peraltro di cogliere lo spirito con cui Lawrence Lessig suggeriva di ibridare tecnologia e tutela dell'autorialità<sup>6</sup>. I mutamenti normativi non sono stati in grado di cogliere le reali potenzialità di questa transizione. Necessario sarebbe stato, come suggeriva Lessig, orientarsi verso un *framework* giuridico di più ampio respiro, capace di tutelare la dimensione collettiva della creazione artistica, più che quella delle singole compagnie di produzione. Una condizione che il carattere generalizzante ed escludente del copyright continua a lasciare disattesa.

La riflessione sull'impatto esercitato dal processo di digitalizzazione sulla sfera giuridica soggettiva dei privati si chiude con il contributo di Federico Costantini che offre spunti interessanti sull'informatizzazione del mondo giudiziario e sugli effetti da questa prodotti sul piano delle condizioni logistiche e organizzative dell'attività processuale. L'idea qui suggerita è che l'evoluzione in senso digitale del processo non possa essere letta solo come un modo per semplificare l'attività documentale collegata al giudizio. Essa costituisce, piuttosto, l'occasione per rivedere, secondo uno schema più in linea con le esigenze poste dalla realtà, l'interazione fra i diversi soggetti dell'attività processuale, dai magistrati alle parti. Il rischio, in caso contrario, è che la tecnologia accentui la distanza fra di essi, deformando la natura dialettica del processo e neutralizzando il significato degli atti che all'interno di questo si producono.

## 5. Risvolti processuali, tributari, penali, internazionali delle nuove tecnologie

La Parte III del volume espande la riflessione sui risvolti processuali dell'innovazione tecnologica, ponendo l'attenzione sulla natura del supporto che quest'ultima può offrire ai diversi attori del mondo giudiziario ovvero sulle nuove forme di tutela processuale nate per contrastare e controllare fenomeni propri della società digitale, come le criptovalute, il cybercrime o i sistemi *mass surveillance*.

Quanto al primo profilo, è opportuno considerare che le nuove tecnologie hanno innovato l'operato non solo di magistrati e avvocati ma anche di altre figure coinvolte nell'attività processuale, collaterali al mondo del diritto. Una fra queste, come suggerito da Michele Ferrazzano, è quella dell'esperto di *computer forensic*. Con l'avvento della società digitale, in effetti, il numero di casi processuali improntati su prove contenute in dispositivi tecnologici è andato crescendo, assegnando agli informatici forensi un valore sempre più strategico. Il nuovo ruolo ha richiesto a questi ultimi, allo stesso tempo, di ampliare il proprio bagaglio di conoscenze, acquisendo non solo necessarie competenze informatiche e giuridiche ma anche schemi comunicativi idonei a rendere facilmente comprensibili i risultati di un'attività analitica sempre più specializzata. Si tratta di un percorso formativo la cui complessità tenderà sicuramente a crescere nei prossimi anni, se si tiene conto

6 Spunti interessanti in questa direzione possono essere rinvenuti in Lessig 2003: 1. Le tesi di Lessig, introdotte nel dibattito italiano da Vittorio Colomba (cfr. Lessig 2005: 17-76; il saggio è stato ristampato in Colomba 2016: 38-75), sono oggi al centro di riflessioni diverse: per un inquadramento si v. la nota Vantin 2017: 95-98.



della rapidità con cui si allarga il numero di fenomeni giuridicamente rilevanti che sono oggi mediati dalla tecnologia.

Un sintomo di questa sorta di “deriva tecnologica” della realtà è rappresentato dalla crescita subita dal catalogo dei reati informatici nel corso di questi anni. Il fenomeno è ben fotografato da Francesco Di Tano, che ne riporta le evoluzioni specificando, peraltro, i limiti che il consolidato distingue tra reati informatici propri (reati commessi direttamente a mezzo o a danno di dispositivi informatici) e impropri (reati comuni che possono prevedere per la loro integrazione – senza che questo ne costituiscono requisito necessario- l'utilizzo di mezzi informatici) incontra nello scenario della società digitale, le cui manifestazioni, pur non rappresentando assolute novità sul piano criminale, non possono comunque essere ricondotte *in toto* a fattispecie di reato già esistenti.

È questo il caso, ad esempio, dell'odio in rete, fenomeno che nasce dalla possibilità di riversare su Internet condotte discriminatorie ai danni di gruppi e minoranze etniche o religiose, di esponenti politici e di altre categorie di individui di volta in volta scelti come bersaglio. Non molto diverso è il caso del *cyberstalking*, che viene fuori dall'estensione del già noto reato di *stalking*, caratterizzato dall'intromissione minacciosa e indesiderata nella vita altrui, al mondo dei social network e, in generale, della comunicazione online.

Peraltro, come messo in evidenza da Chiara Celesti e Stefano Dorigo nel loro contributo, problemi di inquadramento giuridico si presentano non solo in queste ipotesi squisitamente criminose, ma anche in occasione di altri fenomeni mediati dalla tecnologia. L'attenzione dei due Autori ricade, in particolare, sul mondo delle criptovalute o, per dirla con loro, delle “criptoattività”: strumenti finanziari, spesso utilizzati per concludere transazioni fra privati, che presentano natura immateriale e assenza di un contesto regolatorio di tipo pubblico.

Le caratteristiche proprie di questi sistemi contribuiscono in effetti a conferire una certa opacità giuridica alle operazioni che si svolgono per mezzo di essi, rendendo difficile non solo l'inquadramento delle fattispecie di reato ad esse collegate (si pensi al *cyberlaundering*<sup>7</sup>) ma anche la tassazione e il monitoraggio fiscale di queste operazioni.

Vale la pena sottolineare che la tecnologia *blockchain*, su cui poggia l'intero impianto delle criptoattività, è nata per offrire una risposta concreta a un sentimento libertario diffusosi all'interno della comunità informatica intorno agli anni '80. L'idea, estremizzata da esponenti del movimento cyberpunk, era quella di rendere il più possibile sicura la comunicazione virtuale così da incoraggiare gli individui a ricorrervi in maniera quasi esclusiva e ridurre il rischio di scontri fisici fra le persone<sup>8</sup>.

7 L'espressione è utilizzata per indicare la trasposizione in chiave informatica dei delitti di cui agli artt. 648-bis c.p. e 648-ter.1 c.p., riferendosi, in termini ampi, alle ipotesi di riciclaggio realizzate sfruttando internet e tecnologie digitali. Per un inquadramento del tema v. Plantamura 2019: 859 ss.

8 Per un approfondimento sulle radici filosofiche della *blockchain*, si v. Swan & De Filippi 2017: 603-619; Karlström 2014: 23-36.

Le manifestazioni concrete di questa filosofia hanno tuttavia finito per tradirne gli ideali di fondo.

Il “cyberspazio” che questa tecnologia ha contribuito a modellare può essere definito oggi, prendendo in prestito le parole usate da Diego Mauri nel suo contributo, la “quinta dimensione” della conflittualità, un dominio attraverso il quale può essere impiegata la forza, con effetti distruttivi che possono manifestarsi anche su larga scala. Emblematico è il caso dei *cyberattacchi*: attacchi informatici capaci di mettere a rischio la stabilità e la sicurezza di interi Stati mandando in tilt sistemi strumentali al funzionamento di servizi essenziali, come quelli bancari o sanitari.

I pericoli collegati al cyberspazio o, più in generale, alla raccolta, modifica e scambio di informazioni attraverso la rete non presentano sempre effetti così immediati ed eclatanti. Alcuni assumono, al contrario, forme sottili, meno evidenti, ma non per questo meno dannose. La riflessione di Elisa Orrù sulle nuove forme di “panottismo digitale”, aiuta a far chiarezza sul tema. La studiosa si interroga in particolare sulle conseguenze del ricorso sempre più frequente a strumenti di web intelligence, sorveglianza delle comunicazioni digitali, controllo informatico della mobilità e *predictive policing*, evidenziando l’impatto negativo esercitato da tali sistemi su valori centrali delle società democratiche e dello stato di diritto, come l’autonomia, la libertà di pensiero e di espressione, il principio di non discriminazione, la tutela della vita privata e dei dati personali.

Alcuni di questi pericoli sono in parte arginati dall’attuazione di meccanismi di auto-censura e da interventi di tipo giuridico e tecnologico. Molto resta ancora da fare, tuttavia. Come sottolinea Orrù, la protezione di valori costitutivi dello stato di diritto non può passare solo per le scelte dei singoli. È necessario, perché i singoli siano posti in condizione di effettuare scelte consapevoli, che il contesto normativo, sociale ed economico si aggiorni, offrendo risposte più puntuali.

## 6. Intelligenza artificiale e trasformazioni sociali

I contributi finora esaminati offrono senza dubbio una interessante ricostruzione delle numerose dimensioni che oggi assume il rapporto fra diritto e tecnologia, tratteggiando opportunità e criticità da questo generate in contesti diversi, dal mondo del lavoro alla pubblica amministrazione, dal cyberspazio alle aule giudiziarie. L’immagine che ne emerge è quella di una relazione che si trova continuamente di fronte alla sfida di ricercare nuovi punti di equilibrio, nuovi criteri di interazione.

D’altra parte, gli sviluppi della *computer science* hanno finito negli ultimi decenni per condizionare ogni aspetto della vita dell’uomo, come singolo e come membro della collettività. La disponibilità di un numero crescente di dati – frutto anche del progressivo trasferimento in rete di gran parte delle interazioni sociali<sup>9</sup> – e l’evoluzione di modelli sempre più sofisticati di intelligenza artificiale

9 Per una dettagliata ricostruzione dello scenario, si v. Mayer-Schönberger & Cukier 2013. Spunti interessanti sul ruolo svolto dalla rete e dai big data nella ridefinizione del concetto

hanno conferito nuova forma alla realtà quotidiana, modificando il modo di pensare e di essere della società.

Non è un caso che parole come *big data*, IA o *machine learning* siano ormai entrate nel lessico comune, ricorrendo con una certa frequenza nei discorsi del quotidiano. Appare ragionevole domandarsi, tuttavia, quale sia la consapevolezza che noi tutti abbiamo di simili fenomeni, protagonisti delle trasformazioni sociali in atto? Sui risvolti di questo interrogativo si soffermano i curatori del Manuale, Thomas Casadei e Stefano Pietropaoli, nell'ultima parte del volume. Il loro contributo ripercorre le fasi che hanno segnato l'evoluzione del paradigma dell'Intelligenza Artificiale, riflettendo non solo sulle opportunità ma anche sulle controverse questioni etiche, sociali e giuridiche dischiuse dallo stesso.

Gli autori ragionano, fra le altre cose, sui vantaggi e sui pericoli riconducibili al verificarsi di scenari normativi "sintetici", facendo riferimento, con questa espressione, all'eventualità – non così remota – che le interazioni umane si svolgano all'interno di ambienti governati prevalentemente da regole scritte in linguaggio formale, ossia in un linguaggio accessibile e processabile solo ad opera di una macchina. Il pericolo, segnalato da Casadei e Pietropaoli, è che l'interazione fra mondo digitale e agire umano finisca col produrre non tanto o non solo benefici per la società ma forme di governo del primo sul secondo.

Come sottolineato, peraltro, il timore in questione si ricollega a molti degli scenari tecnologici attuali. Si pensi, solo per fare un esempio, ai vincoli materiali – iscritti nel codice informatico – che condizionano l'operato di chiunque interagisca con la rete. Un profilo critico che assume manifestazione più complessa nel contesto dell'altro fenomeno segnalato all'interno del capitolo, ossia l'intelligenza aumentata, intesa come diffusione di modelli che si propongono non di sostituire ma di potenziare l'intelligenza umana attraverso l'integrazione – anche nella forma dell'innesto fisico – con specifici strumenti hardware e software.

L'obiettivo che sembra animare il discorso dei due Autori è soprattutto quello di porre i lettori a confronto con questioni sì di frontiera ma destinate a materializzarsi sempre più rapidamente nel vivere quotidiano, con effetti che il diritto non potrà certo permettersi di ignorare. La sensazione è che, nell'interagire con i nuovi scenari tecnologici, la scienza giuridica sia sempre più spesso costretta a ridefinire i suoi confini, pressata dalla comparsa di fenomeni che insistono non su aspetti formali ma sullo stesso tessuto valoriale che orienta la funzione ordinatrice del diritto.

La riflessione offre una buona introduzione ai successivi contributi della Parte IV, tesi a fotografare alcuni degli effetti già concretamente prodotti dal descritto processo di trasformazione tecnologica della società.

Un primo interessante contributo in questo senso è offerto da Serena Vantin che si sofferma sull'annoso problema del *digital divide*, ossia del divario fra chi ha la possibilità effettiva di accedere alle tecnologie dell'informazione e chi ne è parzialmente

o totalmente escluso. Le parole dell'Autrice delineano in modo puntuale i confini e le diverse declinazioni del fenomeno. L'attenzione è posta soprattutto sui rischi, in termini di discriminazioni e nuove vulnerabilità personali, che da esso sembrano scaturire e sulla conseguente urgenza di immaginare azioni di contrasto mirate, che sappiano dialogare con la realtà socio-culturale al cui interno il fenomeno si inserisce.

L'idea che le tecnologie digitali possano alimentare nuove e più pervasive forme di discriminazione ritorna anche nel contributo di Barbara Giovanna Bello, che approfondisce il tema dei discorsi d'odio diffusi attraverso internet. Dopo una disamina dei profili che rendono giuridicamente rilevante il fenomeno sociale dell'odio, l'Autrice si sofferma sulle caratteristiche proprie degli *hate speech online*<sup>10</sup>, ossia sul problema della diffusione sulla rete di espressioni, termini, messaggi volti a veicolare un contenuto discriminatorio e offensivo nei confronti di categorie specifiche di soggetti. La riflessione offerta si sofferma sulle diverse forme che un problema antico come l'odio può assumere se combinato con i modelli comunicativi della rete, estendendosi poi alle possibili strategie di regolazione e contrasto attuabili in questa direzione.

D'altra parte, come precisato da diversi Autori all'interno del Manuale, il cyberspazio può essere sede di grandi libertà ma anche di profondi pericoli per la dignità della persona. Pericoli che, come sottolinea Valeria Marzocco nel ripercorrere i problemi etico-giuridici collegati al tema della *morte digitale*<sup>11</sup>, impongono al diritto di evolvere, di ripensare le proprie categorie. Un passaggio che si presenta strumentale e necessario all'elaborazione di strategie di contenimento adeguate o, in alcuni casi, di vera e propria fuga dal mondo digitale.

Anche in questo si sostanzia l'idea, articolata da Rosaria Piroso nel contributo che chiude il volume, di un approccio *critico* allo studio del rapporto fra diritto e tecnologia. Mettendo a confronto la prospettiva dei *Critical Legal Studies* con alcune recenti letture ispirate al movimento dei *Critical Data Studies*<sup>12</sup>, la studiosa suggerisce di ridisegnare il quadro concettuale di cui il diritto si serve per rispondere ai problemi posti dalla tecnologia e, in modo particolare, dalle nuove forme di *algorithmic governance*<sup>13</sup>.

Problemi come quello delle discriminazioni digitali, ad esempio, potrebbero essere affrontati utilizzando categorie giuridiche nuove, che non puntano alla gerarchizzazione tra individui e gruppi, e sono in grado di integrarsi con approcci regolativi non convenzionali, ispirati al paradigma della tecnoregolazione.

10 Formula usata per descrivere le manifestazioni di odio che hanno luogo sulla rete.

11 L'espressione si riferisce, per usare le parole della stessa Marzocco, a quella "porzione dell'esistenza, consegnata alla rete attraverso dati e informazioni personali, che sopravvive al decesso naturale dell'individuo".

12 In questo senso, si v. Lettieri 2020.

13 Per una disamina sui vari effetti della regolazione algoritmica, con particolare riguardo all'ambito giuridico, si veda da ultimo il fascicolo monografico, a cura di A. Andronico e Th. Casadei, della rivista *Ars interpretandi*, 26(1), 2021 dedicato a *Algoritmi ed esperienza giuridica*.

## 7. Conclusioni

La panoramica fin qui proposta suggerisce, ancora una volta, l'idea che il volume *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali* vada oltre la funzione didascalica tipica di una manuale.

Ai contributi presentati, che gettano luce su questioni nuove, complesse e spesso sottovalutate dalla comunità giuridica, può senza dubbio essere riconosciuto il merito di aver provato a far chiarezza sulle molteplici dimensioni che il rapporto fra diritto e evoluzione tecnologica va oggi assumendo.

La società digitale in cui viviamo non offre solo strumenti o categorie di servizi innovativi. Essa pone cittadini e regolatori di fronte a interrogativi e sfide inediti, per affrontare i quali occorre acquisire nuove competenze e sviluppare nuove categorie concettuali. Il Manuale in commento guarda esattamente in questa direzione, proponendo delle chiavi di lettura con cui interpretare i nuovi fenomeni della realtà.

Il giurista in formazione, lo studioso di diritto o anche semplicemente il privato cittadino sono così accompagnati in una delicata operazione di decifrazione utile a identificare la dimensione tecnologica, etica e giuridica di questi fenomeni e a relazionarsi consapevolmente con essi.

Un processo che aiuta a governare l'incertezza che si annida nello scenario della società digitale e ad evitare di essere brutalmente travolti da essa.

## Bibliografia

- Andronico, A – Casadei, Th., 2021, “Algoritmi ed esperienza giuridica”, *Ars interpretandi*, 26(1).
- Carloni, E., 2019, “Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni”, *Diritto pubblico*, 25(2), 363-392.
- Faini, F., 2019, *Data society: governo dei dati e tutela dei diritti nell'era digitale*, Milano: Giuffrè Francis Lefebvre.
- Faini, F., 2017, “Social open government: l'utilizzo dei social media nell'amministrazione digitale e aperta”, *Informatica e diritto*, 26, n. 1, 319-345
- Faini, F. – Palmirani, M., 2016, September. *Italian Open and Big Data Strategy. International Conference on Electronic Government and the Information Systems Perspective*, Springer, 105-120.
- Faini, F. – Pietropaoli S., 2021 [2017], *Scienza giuridica e tecnologie informatiche*, Torino: Giappichelli.
- Fioriglio, G., 2004, *Temi di informatica giuridica*, Roma: Aracne
- Frosini, V., 1975, “La giuritecnica: problemi e proposte”, *Informatica e diritto*, 1, n. 1, 26-35.
- Karlström, H., 2014, *Do libertarians dream of electric coins? The material embeddedness of Bitcoin*, *Distinktion: Scandinavian Journal of Social Theory*, 15, n. 1, 23-36.
- Lessig, L., 2003, “Law regulating code regulating law”, *Loy. U. Chi, LJ*, 35, 1.
- Lessig, L., 2016 [2005], “Il diritto del cavallo: la lezione del cyberdiritto”, in Colomba, V., (a cura di), *I diritti nel cyberspazio: architetture e modelli di regolamentazione*, Parma: Diabasis, 38-75.

- Lettieri, N., 2021, "Contro la previsione. Tre argomenti per una critica del calcolo predittivo e del suo uso in ambito giuridico", *Ars Interpretandi*, n. 1, 83-96.
- Lettieri, N., 2020, *Antigone e gli algoritmi. Appunti per un approccio giusfilosofico*, Modena: Mucchi.
- Losano, M.G., 1971, "Lo stato attuale dell'Informatica giuridica in Europa", *Giornale degli Economisti e Annali di Economia*, 867-871.
- Mayer-Schönberger, V. – Cukier, K., 2013, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano: Garzanti.
- Plantamura V., 2019, "Il Cybericiclaggio", in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Torino: Utet, 859-890.
- Sartor, G., 2014, "Nozione e settori dell'informatica giuridica", *L'informatica giuridica in Italia: cinquant'anni di studi, ricerche ed esperienze*, in Ginevra Peruginelli e Mario Ragona (a cura di), Napoli: ESI, 59-74.
- Swan, M. – De Filippi, P., 2017, "Toward a philosophy of blockchain: A symposium: Introduction", *Metaphilosophy*, 48, n. 5, 603-619.
- Taddei Elmi, G., 2014, "Informatica e Diritto. Presupposti, storia, disciplina, insegnamento, ius condendum", *Informatica e diritto*, 23, n. 2, pp. 85-123.
- Vantin, S., Colomba, V., 2017, "I diritti nel cyberspazio. Architetture e modelli di regolamentazione, con un saggio di Lawrence Lessig, Diabasis, Parma 2015", *Ars interpretandi*, 22, n. 1, 95-98.