ORDINES
Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730
NUMERO 2 – DICEMBRE 2024

MICHELE BALBINOT

Le lenti del diritto nella metamorfosi digitale

T. CASADEI, S, PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, seconda edizione ampliata e aggiornata, Wolters Kluwer, Milano, 2024, pp. 1-336

ORDINES
Per un sapere interdisciplinare sulle istituzioni europee

2/2024

MICHELE BALBINOT*

Le lenti del diritto nella metamorfosi digitale

T. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, seconda edizione ampliata e aggiornata, Wolters Kluwer, Milano, 2024, pp. 1-336.

Accogliendo la rapidità della metamorfosi digitale, a distanza di tre anni dal volume che inaugurava la collana *Comp.Lex Diritto, Computazione, Complessità*, i curatori – della stessa[1], come del volume – Thomas Casadei e Stefano Pietropaoli procedono ad aggiornare ed ampliare il già importante lavoro di analisi delle tante questioni poste dalle trasformazioni legate all'evoluzione informatica.

L'opera mantiene la quadripartizione precedente, pur riorganizzando i ventitré contributi su direttrici che ancora meglio colgono le sfide sempre nuove del mondo digitale: la prima parte (pp. 3-74) rimane dedicata ai diritti fondamentali e al ruolo delle istituzioni; la seconda parte (pp. 75-144) introduce lo studio dei nuovi rischi, oltre che delle nuove tutele, offerti dalla digitalizzazione; la terza parte (pp. 145-258), invece, più di altre indaga gli aspetti applicativi delle tecnologie informatiche, in particolar modo nelle loro dimensioni privatistiche, penalistiche e internazionali, in termini sostanziali e processuali; infine, alle "trasformazioni sociali" già indagate nella prima edizione, si aggiungono alla quarta parte (pp. 259-336) le "scelte politiche" che l'evoluzione della tecnica rende oggi più che mai necessarie e di cui si occupano buona parte dei nuovi contributi al volume[2].

---

* Assegnista di ricerca, Dipartimento di Giurisprudenza, Università di Modena e Reggio Emilia

[1] La collana, edita da Wolters Kluwer, conta ad oggi otto volumi. Oltre alle due edizioni di "*Diritto e tecnologie*", sono stati pubblicati, in ordine cronologico, i seguenti testi: SERENA VANTIN, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, la Pubblica Amministrazione, le imprese*, 2021; ELISA ORRÙ, *Legittimità e digitalizzazione. Per una critica realistica delle politiche di sicurezza dell'Unione europea*, 2022; NOEMI MINISCALCO, *L'intelligenza artificiale in movimento. L'impatto sui diritti costituzionali della* smart mobility, 2024; SILVIA SALARDI, *Neurotecnologie tra potere e libertà. Medicina, etica, discriminazioni di genere*, 2024; ISABELLA FERRARI, *Protecting intellectual property in the age of artificial intelligence in the age of artificial intelligence*, 2024; ANGELA MENDOLA, *Diritto all'abitazione e credit scoring. Profili di diritto interno e comparato*, 2024.

[2] I contributi aggiunti in questa seconda edizione, che vede anche una riorganizzazione dei contributi già presenti nella prima edizione all'interno delle diverse parti, sono quelli di FEDERICO OLIVIERI (*Il "diritto a internet": ragioni e principi per democratizzare la rete*, pp. 43-58), di VALERIA GIORDANO (*Intelligenza artificiale e pratica dei diritti*, pp. 275-284), di VALERIA

Attraverso queste "lenti" e i relativi contributi, l'opera curata da Casadei e Pietropaoli riesce a offrire uno sguardo d'insieme sulle interazioni che la transizione digitale vive con il diritto e la società, con la sicurezza e la salute, con il potere e la democrazia. Lo sforzo dei curatori è teso, dichiaratamente, non tanto a delineare un quadro esaustivo della materia, quanto più a offrire un approccio analitico sempre multidisciplinare, ibrido, sia nella forma sia nella sostanza.

I primi cinque capitoli affrontano, come già suggerito, il rapporto tra le tecnologie digitali e i diritti fondamentali, indagando ulteriormente il ruolo delle istituzioni pubbliche nella difficile e delicata regolazione di tali interazioni.

Nel primo contributo offerto dal volume, Simone Scagliarini (*I diritti costituzionali nell'era di internet: cittadinanza digitale, accesso alla rete e* net neutrality, pp. 1-16) analizza il rapporto tra i diritti fondamentali e l'era digitale, facendo specifico riferimento ora alle metamorfosi dei diritti preesistenti, che assumono nuove modalità di esercizio nella rete, ora a veri e propri nuovi interessi meritevoli di tutela. L'autore, quindi, suggerisce una nozione di "cittadinanza digitale" come insieme di diritti e doveri che presuppongono l'esistenza della rete e, quindi, la possibilità di connettervisi. In questo senso, la connessione ad internet assume le forme di "un elemento essenziale per dare effettività al rapporto di cittadinanza" (p. 6). Di qui, il contrasto tra le diverse tesi dottrinali che ricostruiscono l'idea di un "diritto ad internet" e la timidezza di una giurisprudenza ancora in difficoltà nel riconoscimento, pur di fronte ad un legislatore, nazionale e sovranazionale, impegnato nello sviluppo digitale del Paese.

Noemi Miniscalco apre il secondo contributo dell'opera (*La personalità in rete: protezione dei dati personali, identità digitale e diritto all'oblio*, pp. 17-30) con una riflessione sull'evoluzione dei diritti della personalità alla luce dei mutamenti contestuali storici, sociali e culturali. Il riferimento particolare, in questo capitolo, è al diritto alla riservatezza e alla sua evoluzione dal celebre "*right to be let alone*" di Samuel D. Warren II e Louis Brandeis, giunto oggi all'esplicitazione del suo più importante corollario: il diritto alla protezione dei dati personali. Principiando dalla legislazione nazionale ed eurounitaria, con particolare riferimento al regolamento 2016/679/UE, l'autrice quindi ricostruisce la nozione di "identità digitale": se l'identità personale si rapporta all'interesse del soggetto di essere rappresentato nella

---

BARONE (*La discriminazione ai tempi dell'intelligenza artificiale: la questione algoritmica*, pp. 285-296) e di ALFREDO D'ATTORRE (*La sovranità digitale. Poteri privati, intervento pubblico e diritti individuali nel cyberspazio*, pp. 313-324).

vita di relazione con la sua vera identità e a non vedere travisato il suo patrimonio di idee ed esperienze di vita (pp. 21-22), l'identità digitale altro non è che la trasposizione della medesima situazione giuridica nel modo online, cui si lega a doppio filo anche il cosiddetto "diritto all'oblio", cioè alla cancellazione o deindicizzazione dei dati e delle informazioni in rete relative ad una persona. Nonostante il riconoscimento degli sforzi di dottrina e legislatore, Miniscalco chiude il proprio contributo con un monito a rimanere attenti e vigili rispetto ai rischi che la rete cela, poiché le tracce che lasciamo sul web, i dati che condividiamo con le big tech, non sono facilmente rimovibili.

Gianmarco Gometz, nel terzo capitolo del volume (E-democracy. *Forme e problemi della partecipazione digitale*, pp. 31-42), indaga le forme di democrazia elettronica in ottica critica, cercando di tracciare una linea di demarcazione prima tra le diverse forme di partecipazione politica (diretta, rappresentativa, dimostrativa e deliberativa) e quindi tra ciò che può essere considerata effettiva "partecipazione democratica elettronica" e ciò che invece presenta importanti limiti. Su questo solco l'autore delinea gli aspetti chiave della partecipazione, perché si possa parlare puntualmente di "democrazia elettronica": essa deve prevedere l'uguaglianza di voto, la cogenza della decisione e la rappresentatività della consultazione.

Il quarto contributo del volume, che rientra tra quelli nuovi di questa seconda edizione, è quello che forse più di altri fornisce una chiave di lettura per tutta l'opera. Muovendo dall'analisi di quello che chiama "divario democratico digitale" quale asimmetria di potere tra chi controlla internet e chi lo utilizza, Federico Olivieri (*Il "diritto a internet": ragioni e principi per democratizzare la rete*, pp. 43-58) postula la necessità di un nuovo equilibrio, anche attraverso la formulazione di un "diritto a internet" specifico, pensato e materializzato non tanto per permettere il mero accesso alla rete, quanto più per mettere la popolazione "in condizione di controllare l'informazione, la comunicazione e la conoscenza prodotte *online* per recuperare potere sulla propria vita" (p. 46). In questo modo si potrebbe riconoscere un diritto a internet come precondizione per l'esercizio di altri diritti, nonché come garanzia di un "uso pieno della rete" (p. 53), cioè in termini di promozione di libero accesso alla conoscenza. Ciò, peraltro, si scontra con l'assenza di una adeguata formazione digitale di massa e di qualità e con le diverse frammentazioni della rete, che potrebbe altrimenti essere strumento foriero di democrazia e cittadinanza attiva globale.

Gianluigi Fioriglio (eHealth: *profili informatico-giuridici*, pp. 59-70) chiude la prima parte con un contributo sulle interazioni tra le nuove

tecnologie e l'ambito sanitario, per sua natura di particolare delicatezza. Quattro, in particolare, sono i profili applicativi della c.d. *eHealth* che l'autore indaga: l'intelligenza artificiale e la medicina algoritmica, che inseriscono nella già complessa dinamica paziente-medico un terzo attore – *sui generis* – qual è, appunto, l'algoritmo, il software (si pongono, in questo caso, importanti questioni in ordine alla responsabilità in caso di eventuali errori, che richiede necessariamente una forma di spiegabilità degli output di questi programmi informatici); lo sviluppo di sistemi informativi sanitari ha senz'altro migliorato la qualità e l'efficienza dell'assistenza sanitaria, ma questi devono rispettare precise condizioni sia di accessibilità che di protezione dei dati dei pazienti, specie quando prendono le forme dei c.d. "Fascicoli Sanitari Elettronici", grazie ai quali i pazienti possono tracciare e consultare la propria vita sanitaria; infine, l'autore analizza le questioni giuridiche che insistono sulla telemedicina, per cui è necessario individuare i dispositivi medici adatti e garantire, anche in questo caso, la tutela dei dati personali. Il rischio che Fioriglio evidenzia, in questi casi, è la sostituzione, in luogo dell'integrazione, del dispositivo elettronico nei confronti del medico professionista, il quale dovrebbe mantenere il compito di instaurare un rapporto di fiducia con l'assistito, prima ancora di formulare una terapia o suggerire l'utilizzo di tecnologie digitali.

La seconda parte dell'opera, dedicata a rischi e tutele del mondo digitale, si apre con una disamina sulla cybersecurity di Raffaella Brighi (Cybersecurity. *Scenari tecnologici e regolamentazione di un'area in espansione*, pp. 75-88). L'autrice tratteggia il passaggio dalla *computer security*, come protezione delle infrastrutture digitali, alla *information security* come tutela dei dati e delle informazioni contenute negli apparati informatici. In questo modo la questione della sicurezza trasla da un ambiente fortemente tecnico ad uno che tiene conto del fattore umano, in termini di analisi e controllo dei rischi. In questo senso si pongono le direttrici verso cui si orienta la sicurezza informatica: robustezza, resilienza e risposta dei sistemi, che devono garantire riservatezza, integrità e continua disponibilità – oltre che, oggi, anche veridicità, autenticità e non ripudio, come paradigma crittografico – dei dati ivi immagazzinati. A fronte di nuove minacce, su scala privata-commerciale e pubblica-internazionale, in considerazione anche dello sviluppo dei sistemi di intelligenza artificiale, l'autrice sottolinea la necessità di una risposta giuridica armonizzata a livello internazionale, principiata dapprima con la convenzione di Budapest del 2001 e proseguita, in modo particolare, nel sistema eurounitario attraverso

il regolamento GDPR e i meno celebri eIDAS e la direttiva PSD2, oltre alla *Cybersecurity Strategy* europea del 2013.

Il secondo contributo, nonché settimo dell'intero volume, firmato da Sandro Luce (*Dal* copyright *al* copyleft. *La diffusione della conoscenza ai tempi di internet*, pp. 89-102), analizza il diritto d'autore, o *copyright*, nella sua evoluzione storica, che inizia nell'Inghilterra del XVI secolo fino ad entrare in tutti gli ordinamenti nazionali in età contemporanea. Di qui il costante ampliamento dei campi di applicazione – alla musica, ai prodotti audiovisivi e finanche alle cc.dd. "opere derivate" – e della durata di protezione. Ciò, per l'autore, sembra fondare un forte disequilibrio tra la tutela degli interessi di pochi attori economici e la diffusione della conoscenza, la quale "assume sempre più le caratteristiche di una *fictious commodity*" (p. 93), specie a valle delle più importanti sentenze statunitensi e, più recentemente, europee[3]. Si formula dunque la possibilità di un paradigma alternativo, del c.d. *copyleft*, come permesso di utilizzare liberamente un'opera dell'ingegno o artistica, di diffonderla e persino di modificarla, mantenendo alcune regole che permettano il mantenimento di un sistema che comunque riconosca la paternità di un prodotto, pur non scadendo nella *commodification*.

Il contributo di Iacopo Senatori (*"Remoto", "multilocale" e "a distanza": l'impatto della trasformazione digitale nei mondi del lavoro*, pp. 103-116), dal canto suo, esplora l'impatto della trasformazione digitale sul mondo del lavoro, con particolare attenzione alle nuove modalità lavorative "a distanza": il lavoro agile, il telelavoro e, da ultimo, il c.d. *smart working*. Viene qui analizzata l'evoluzione dei modelli giuridici giuslavoristici nella quarta rivoluzione industriale, che cercano di adattarsi a un contesto caratterizzato da maggiore flessibilità, in cui il luogo, e sovente anche l'orario, di lavoro, perdono rilevanza. Di contro, si affronta il tema del "diritto alla disconnessione", fondamentale per garantire un equilibrio tra produttività e tutela della salute psicofisica del lavoratore e della lavoratrice; quindi, essenzialmente una soluzione di continuità tra tempo di vita e tempo di lavoro. Si analizza, parimenti, la questione della scelta del luogo di lavoro, che incide profondamente sulle dinamiche tra dipendente e datore in termini di controllo, sicurezza – anche informatica – e responsabilità. Infine, Senatori sottolinea il principio di volontarietà come elemento chiave per una regolamentazione equilibrata del lavoro a

[3] L'autore cita nel dettaglio le sent. A&M Records v. Napster del 2001, MGM v. Grokster e la sentenza della Corte di Giustizia dell'UE C/610/15 relativa al caso "*The Pirate Bay*".

distanza, evitando imposizioni e rispettando le esigenze delle parti coinvolte.

Fernanda Faini, nel quarto capitolo della seconda parte, esamina il ruolo dell'amministrazione pubblica nella società tecnologica e la sua connessione con i diritti digitali, evidenziando l'impatto della trasformazione digitale sulle istituzioni e sui cittadini (*L'amministrazione pubblica nella società tecnologica e i diritti digitali*, pp. 117-130). A partire dal Codice dell'amministrazione digitale (d.lgs. n. 82/2005), l'autrice analizza come la tecnologia stia ridefinendo i processi amministrativi, dando centralità al paradigma della cittadinanza digitale (p. 119) e indirizzandosi verso un modello di "governo aperto", caratterizzato da maggiore trasparenza e apertura – attraverso, ad esempio, il diritto di accesso, e garantendo la protezione dei dati personali dei cittadini *by design* e *by default*. Viene quindi approfondita l'evoluzione dell'amministrazione digitale, passando dal principio del *digital first* verso un approccio di esclusività digitale, dove i servizi pubblici sono progettati prioritariamente in tale forma. Al centro del capitolo ci sono le sfide legate alla tutela dei diritti digitali e all'equilibrio tra innovazione tecnologica, accessibilità e inclusione, in un contesto in cui la digitalizzazione diventa sempre più pervasiva e necessaria.

La seconda parte si chiude con il contributo di Valeria Marzocco (*Vita e morte digitali. Il* corpo elettronico *e la sua tutela giuridica*, pp. 131-141) che esplora il concetto di corpo elettronico e la sua tutela giuridica, analizzando le implicazioni della trasformazione digitale sulla costruzione e gestione dell'identità in rete, oltre che sulla memoria digitale dopo la morte. L'autrice parte dall'idea di impronta digitale e di dato informatico come "segmento del corpo elettronico" (p. 132), per affrontare il rapporto tra identità personale e identità digitale, evidenziando le sfide legate alla rappresentazione del sé nei contesti digitali. In questo senso Marzocco contrappone le due questioni più interessanti e opposte che si pongono nella frammentazione dell'identità personale in forma digitale: da un lato, il diritto ad essere dimenticati, dall'altro, quello a mantenere la memoria di sé, entrambe peraltro attinenti ad una più ampia riflessione sulla vita e la morte nella "duplicazione artificiale" del corpo elettronico. Per questo particolare attenzione è dedicata alla *digital death* e alla gestione dei dati e delle identità digitali *post mortem*, un tema che solleva questioni etiche e giuridiche relative alla conservazione, all'accesso e alla cancellazione dei dati, considerati veri e propri "beni digitali" in capo al *de cuius* e per cui si può parlare di *digital inheritance*.

La terza parte del volume indaga le dimensioni applicative delle tecnologie digitali in diverse materie giuridiche. Il primo capitolo, di Filippo Murino (*Dalla firma elettronica agli* smart contract, pp. 145-166), analizza l'evoluzione della "documentalità" nell'era digitale prendendo le mosse dallo spostamento dalla firma autografa tradizionale alla firma elettronica, spostando poi l'attenzione, in particolare, sull'impatto delle tecnologie digitali sulla certezza giuridica e sull'efficacia probatoria dei documenti. L'analisi di Murino include poi le tecnologie basate su registri distribuiti, come la *blockchain*, che introduce nuovi paradigmi di sicurezza e trasparenza grazie alla crittografia asimmetrica e all'uso della chiave privata in sostituzione della firma autografa, ma fa parallelamente emergere delle criticità. Il capitolo si conclude con un focus sui cc.dd. *smart contracts*, contratti auto-eseguibili basati sulla *blockchain*, che vedono un'evoluzione significativa nel campo della certezza contrattuale, nonché numerose possibili applicazioni, pur rappresentando problematicità in ordine alla traduzione in linguaggio informatico delle clausole generali (p. 164) o degli standard e, più in generale, alla legge applicabile agli stessi.

Il contributo di Federico Costantini (*Giustizia elettronica e digitalizzazione giudiziale: contesto europeo ed esperienza italiana*, pp. 167-182) offre una disamina sul contesto europeo e italiano in materia di digitalizzazione della giustizia. Il processo di digitalizzazione prevede, potenzialmente, tre fasi: la dematerializzazione dei supporti documentali, la delocalizzazione degli accessi e l'automazione dei processi. Se queste sono astrattamente facili da perseguire, meno percorribile è il cambiamento di paradigma necessario per "accedere ad una visione in cui il processo è un ecosistema in cui diversi agenti – il giudice, le parti, *in primis* – interagiscono tra loro in funzione di un risultato che […] idealmente si risolve nella Giustizia" (p. 170). Costantini, quindi, analizza le origini della giustizia elettronica, esaminando gli sviluppi nel Consiglio d'Europa e nell'Unione Europea, con un *focus* rispettivamente sul CEPEJ (Commissione per l'efficienza della Giustizia del Consiglio d'Europa) e sui piani strategici d'azione dell'UE. Particolare attenzione viene in questo senso dedicata al Piano d'azione 2024-2028 e alla piattaforma e-CODEX, che facilita la cooperazione giuridica transfrontaliera. Il capitolo prosegue con un'analisi dell'esperienza italiana nella digitalizzazione dei procedimenti giudiziari, con riguardo al Processo Civile Telematico (PCT), al Processo Amministrativo Telematico (PAT), al Processo Tributario Telematico (PTT) e al Processo Penale Telematico (PPT), alla luce della celebre riforma c.d. "Cartabia". Si riflette dunque sull'evoluzione verso una vera "Giustizia

elettronica", postulando una necessaria collaborazione tra le diverse figure professionali coinvolte.

Michele Ferrazzano, nel suo contributo, esplora l'informatica forense, esaminando sia gli aspetti giuridici sia tecnici legati al trattamento delle prove digitali (*L'informatica forense: profili giuridici e tecnici nel trattamento della* digital evidence, pp. 183-196). A partire da una breve panoramica sul ruolo della stessa e sulle sue criticità, l'autore evidenzia l'importanza di garantire l'affidabilità e l'integrità, quindi l'attendibilità, dei dati durante le indagini. L'informatica forense viene qui presentata come una disciplina scientifica, che si occupa di ammettere, assumere, analizzare e conservare prove digitali in modo da poterle utilizzare in sede giudiziaria, seguendo protocolli operativi e norme giuridiche stringenti. Di qui l'approfondimento del concetto di *digital evidence* nei suoi caratteri principali: immaterialità, alterabilità, volatilità e riproducibilità *ad infinitum*, e quindi i requisiti che la prova digitale deve corrispondentemente avere. Ferrazzano, quindi, rivede le linee guida e gli *standard* previsti in materia e descrive le fasi del trattamento del reperto informatico, dalla raccolta alla conservazione, sottolineando l'importanza di seguire procedure rigorose per garantire la validità giuridica delle prove. Infine, affronta il profilo professionale dell'informatico forense, evidenziando le competenze tecniche e legali richieste per operare in questo campo.

Il contributo di Francesco Di Tano analizza i reati informatici e i fenomeni emergenti legati all'uso delle tecnologie digitali, focalizzandosi in maniera particolare su *cyberstalking*, cyberbullismo e sul c.d. *revenge porn* (*I reati informatici e i fenomeni del* cyberstalking, *del cyberbullismo e del* revenge porn, pp. 197-212). Il capitolo illustra le modifiche legislative che sin dagli anni Settanta del Novecento il legislatore italiano ha introdotto per far fronte all'evoluzione digitale della criminalità, continuando poi con una panoramica sui principali reati informatici, definendone le caratteristiche essenziali e le implicazioni legali. Viene poi esplorato l'odio in rete, un fenomeno che alimenta diverse forme di violenza digitale nei confronti di minoranze, esponenti politici ma anche singoli individui, e quindi le più recenti manifestazioni della cybercriminalità, che traducono comportamenti devianti tradizionali, come *stalking* e bullismo, nelle forme digitali, ampliandone i profili dannosi. L'autore si dedica quindi al c.d. *revenge porn*, ossia la diffusione non consensuale di immagini intime con l'intento di danneggiare la reputazione della vittima. Ogni fenomeno, in questo senso, viene esaminato sotto il profilo giuridico, evidenziando le normative esistenti e le difficoltà nell'affrontare questi crimini nel contesto

digitale, dove l'anonimato e la rapidità di diffusione delle informazioni complicano le indagini e le punizioni.

Barbara Giovanna Bello (*I discorsi d'odio* in rete, pp. 213-230) prosegue inquadrando in maniera sistematica uno dei temi trattati da Di Tano: i discorsi di odio in rete. A partire da una riflessione sul concetto di *hate speech*, evoluto da forme di espressione nel mondo reale a discorsi *online*, quindi con un impatto potenzialmente maggiore a causa della diffusione rapida e dell'anonimato che internet offre, l'autrice analizza poi le diverse declinazioni che questo assume e in cui si manifesta, sempre in ottica intersezionale. Il capitolo prosegue quindi affrontando la regolamentazione della rete e le difficoltà nel contrastare i discorsi d'odio, evidenziando le principali pratiche adottate dai *service provider*, le iniziative delle istituzioni internazionali e portando alcuni esempi di legislazione nazionale nel contesto eurounitario. Infine, Bello analizza le pratiche di contrasto, facendo specifico riferimento alla cooperazione e al ruolo delle organizzazioni della c.d. società civile.

Il capitolo di Elisa Orrù (*Verso un nuovo Panottico? La sorveglianza digitale*, pp. 231-244) esplora il tema della sorveglianza digitale, analizzando come le tecnologie moderne stiano cambiando la relazione tra potere e controllo nella società. Partendo dall'analisi foucaultiana sulla disciplina, Orrù distingue le tre forme in cui si esprime oggi la sorveglianza digitale: il "capitalismo della sorveglianza", che descrive il modello economico che sfrutta i dati degli utenti per fini commerciali; i metodi di controllo della criminalità e della mobilità, che evidenziano come la tecnologia venga utilizzata per monitorare il comportamento delle persone in vari ambiti della vita quotidiana e in termini sempre più di interoperabilità come opposta ad un approccio più settoriale e specifico; e infine la convergenza tra pubblico e privato nella sorveglianza digitale, dove le pratiche di monitoraggio da parte degli enti pubblici si intrecciano con quelle delle aziende private, creando nuove dinamiche di controllo. La parte conclusiva del contributo è dedicata alle implicazioni e ai rischi derivanti da un eccessivo controllo digitale, come la violazione della privacy e la creazione di una società di sorveglianza, suggerendo possibili rimedi – giuridici e tecnologici – per bilanciare la sicurezza con la protezione dei diritti individuali.

L'ultimo contributo della parte prettamente applicativa del volume è affidato a Diego Mauri, che ragiona sull'uso della forza legato alle nuove tecnologie, in ottica internazionale (*"Aggiornamento disponibile": nuove tecnologie, uso della forza e diritto internazionale*, pp. 245-256). A partire

dall'analisi del diritto internazionale tradizionale, l'autore esamina l'utilizzo di droni e di robot, nonché il panorama sempre più evidente di c.d. *cyberwarfare*. Se nei primi si pongono problemi di accumulo di dati e di qualificazione "giuridica" dei *drone strikes* come "legittima difesa preventiva" (una contraddizione in termini), che quindi richiedono l'applicazione dei principi in materia di diritti umani, i robot si sono dimostrati poco precisi e quindi inaffidabili nella gestione autonoma delle funzioni critiche, cioè, in questo caso, la decisione sul *target* di un attacco, oltre a sollevare dubbi sulla responsabilità di eventuali errori. Il capitolo si concentra quindi sui cyberattacchi e la cybersecurity, esplorando come la crescente digitalizzazione delle guerre abbia portato all'emergere di vere e proprie *cyberweapons* e di nuove forme di conflitto (si parla, in tal senso, di "quinta dimensione" della conflittualità), per le quali il diritto internazionale deve ancora adattarsi. Di qui, la riflessione finale sul futuro del diritto internazionale, che dovrà tenere conto delle sfide poste dall'uso delle nuove tecnologie.

La quarta, e ultima, parte, dedicata alle trasformazioni sociali e alle scelte politiche in materia di diritto e tecnologia, si apre con il contributo dei curatori del volume, Casadei e Pietropaoli (*Intelligenza artificiale: l'ultima sfida per il diritto?*, pp. 259-274). Esso esamina l'"intelligenza artificiale" come una delle sfide più rilevanti per il diritto, esplorando il suo sviluppo, le sue implicazioni e le possibili evoluzioni normative. Prendendo le mosse dall'origine e dal significato del termine, coniato negli anni Cinquanta del Novecento, gli autori chiariscono come "Intelligenza Artificiale" faccia riferimento ad una "costellazione estremamente complessa di tecnologie, anche diversissime tra loro, che perseguono obiettivi pratici diversi" (p. 260), restando accomunate dallo scopo di eseguire compiti che tipicamente richiedono l'intelligenza di esseri umani. Si mettono quindi in evidenza il "test di Turing" e la "stanza cinese di Searle", due concezioni fondamentali per comprendere la relazione tra IA e intelligenza umana, sollevando questioni su cosa significhi "pensare" per una macchina (e per una persona) e se sia possibile attribuire una forma di coscienza a un'intelligenza artificiale. In questo contesto d'analisi si esplorano le "stagioni" dell'IA, analizzando l'evoluzione della tecnologia e il suo impatto sull'attuale scenario tecnologico e sociale, dai "sistemi esperti" alle reti neurali. Di qui scaturisce la riflessione in ordine al "diritto computazionale", un sistema legale che si occupa di "computabilizzare" il ragionamento giuridico, rendendolo "comprensibile" da una macchina, e finanche di concepire e riconoscerle una forma di personalità e di *moral agency*. Gli autori

analizzano anche l'impatto dell'IA nelle sfere del diritto e nelle professioni legali, con particolare attenzione al concetto di "autonomia" e alla trasformazione dei settori legali attraverso l'automazione e l'uso di algoritmi intelligenti. Il capitolo si conclude dunque con un'analisi dell'IA generativa, evidenziando le differenze tra l'americano ChatGPT ed Ernie-Bot, sviluppato dall'azienda cinese Baidu e che ha necessitato dell'approvazione del governo di Pechino, subendo delle censure e delle limitazioni nelle risposte fornite e fornibili.

Il contributo di Valeria Giordano (*Intelligenza artificiale e pratica dei diritti*, pp. 275-284) prosegue sul solco del precedente, esplorando le implicazioni dell'intelligenza artificiale nella pratica dei diritti, concentrandosi su come essa stia modificando la loro soggettività e gestione e analizzando, in particolare, la questione del soggetto e lo scarto esistente tra la fisicità della persona e l'invenzione della figura astratta funzionale al discorso giuridico. L'autrice approccia l'uso delle tecnologie all'interno del mondo giuridico, e in particolare nella funzione decisoria sulle controversie, riprendendo il carattere conflittuale dei diritti e la necessità di porli sempre all'interno di un costante bilanciamento, esercizio che un algoritmo inferenziale potrebbe non essere in grado di operare. Le medesime perplessità si espandono al campo della giustizia predittiva, che ha evidenziato anche nei suoi profili applicativi degli importanti limiti di *bias* e condizionamenti. Di qui è chiaro il riferimento alle espressioni di *soft law* relativamente all'intelligenza artificiale, che hanno richiesto maggiore trasparenza nella programmazione e il rispetto dei diritti fondamentali.

Valeria Barone (*La discriminazione ai tempi dell'intelligenza artificiale: la questione algoritmica*, pp. 285-296), dal canto suo, esplora la discriminazione nell'era dell'intelligenza artificiale, focalizzandosi sulla sua forma "algoritmica". A partire da una riflessione sulla terminologia, evidenziando l'ambiguità e le difficoltà nell'applicazione di una definizione univoca, soprattutto quando si tratta di nuove tecnologie, l'autrice prosegue con un'analisi del diritto antidiscriminatorio nazionale e sovranazionale, riprendendo inoltre la distinzione tra discriminazione diretta e indiretta già presente nella l. n. 125/1991 per suggerire come la discriminazione algoritmica sfuggirebbe ad entrambe le categorie.

Il capitolo approfondisce quindi la discriminazione algoritmica, cioè come gli algoritmi possano perpetuare o amplificare pregiudizi preesistenti, portando a risultati discriminatori non intenzionali. Si esaminano in questo senso i diversi tipi di algoritmi: deterministici, non deterministici e i modelli di apprendimento automatico, che possono essere

costruiti attraverso forme di addestramento più o meno supervisionato. Di qui, l'analisi dei *bias* algoritmici, cioè dei pregiudizi incorporati negli algoritmi a causa dei dati utilizzati per addestrarli, delle diverse tipologie (di selezione, di misurazione, temporale, di rilevamento, di pubblicazione e di conferma) e delle fasi in cui possono manifestarsi.

Infine, il capitolo si concentra sulle discriminazioni di precisione, un fenomeno in cui gli algoritmi sono creati sulla base di analisi di dati personali dettagliati, che permettono di prendere decisioni altamente mirate che possono dunque determinare un trattamento specifico in determinati campi commerciali come quelli assicurativi, finanziari o di marketing.

Il quarto contributo della parte in esame, di Serena Vantin (*I divari digitali nell'epoca della rete globale*, pp. 297-312), offre una disamina dei divari digitali, analizzando come le disuguaglianze nell'accesso e nell'uso delle tecnologie digitali influenzino diversi gruppi sociali e geografici. In questo senso, i soggetti e i gruppi maggiormente esposti al rischio di esclusione digitale sarebbero le persone anziane, quelle disoccupate, quelle con un *background* migratorio, quelle con disabilità, quelle che vivono nelle aree rurali o, più in generale, i gruppi socio-economicamente svantaggiati. Fattori che, peraltro, si aggravano per le donne e nei confronti delle quali va riservata una speciale attenzione. Vengono quindi esplorate le differenti tipologie di divario, che non riguardano solo l'accesso alla tecnologia, ma anche le competenze digitali necessarie per utilizzarla efficacemente. L'autrice si concentra dunque sull'inquadramento giuridico, analizzando le politiche e le normative, italiane ed eurounitarie, per contrastare l'esclusione digitale. Particolare attenzione viene data, entro questo scenario, agli strumenti di *soft law* comunitari che promuovono la formazione permanente e progressiva come strumento fondamentale per ridurre le disuguaglianze e per contrastare le possibili discriminazioni algoritmiche e tecnologiche, specie dove l'accesso alle competenze digitali è cruciale per l'integrazione sociale e professionale.

Il contributo di Alfredo D'Attorre, (*La sovranità digitale. Poteri privati, intervento pubblico e diritti individuali nel cyberspazio*, pp. 313-324) esplora l'evoluzione della sovranità nel mondo digitale, analizzando le dinamiche tra poteri privati, intervento pubblico e diritti individuali. Nonostante una visione di Internet più storicamente datata lo indichi come strumento nato in ambito militare, esso è sovente rappresentato come "dimensione integralmente orizzontale" (p. 314), in termini ideologici: l'autore riconosce questi ultimi come esacerbati nel mondo iper-globalizzato odierno, in cui il

ciberspazio si è emancipato dal controllo della sovranità statale in favore dell'auto-normatività dei soggetti privati. Il capitolo, in questo senso, esplora l'evoluzione di Internet, sottolineando l'emersione di un oligopolio delle grandi piattaforme che agisce indisturbato un controllo pervasivo sulle comunicazioni. In opposizione, viene approfondita la questione del controllo statale dello spazio digitale, in particolare attraverso il confronto tra diversi modelli di sovranità digitale applicati da paesi come gli Stati Uniti, la Cina e l'Unione Europea. Si esaminano anche qui i diritti individuali in un contesto di crescente controllo pubblico e di un "capitalismo della sorveglianza", in cui i diritti fondamentali degli individui sono messi in discussione dall'uso dei dati personali da parte di attori sia pubblici, spesso in ottica di protezione dagli attacchi informatici, sia privati. La chiave di lettura è fornita quindi sulla difficoltà a sviluppare una sovranità digitale soggetta a legittimazione democratica senza che si ponga un esteso controllo pubblico delle grandi piattaforme digitali, a maggior ragione quando, nello scacchiere geopolitico, entrano in gioco anche le "intelligenze artificiali".

La chiusura del volume è affidata a Rosaria Pirosa (*I dilemmi della tecnoregolazione: uno sguardo critico*, pp. 325-336), che offre uno sguardo critico sul rapporto tra il diritto e le nuove tecnologie digitali. La riflessione parte dalla prospettiva pluralista dei c.d. *Critical Legal Studies*, la quale mette in discussione l'idea di un diritto neutrale, suggerendo invece che esso sia influenzato da poteri economici, sociali e politici; l'autrice suggerisce parimenti che tale concezione ha ignorato il portato contemporaneamente tutelante e potenzialmente discriminatorio dell'evoluzione tecnologica. Di qui la possibilità di applicare l'approccio teorico-critico alla tecnoregolazione, prendendo in considerazione come gli algoritmi operano con riguardo ai soggetti e alle relazioni sociali (p. 330). In questo senso vengono esplorati i *Critical Data Studies* e gli *Algorithm Studies*, che richiamano un approccio interdisciplinare e di interazione tra diverse prospettive critiche, cosa che permette, e forse rende necessaria, una relazione tra i due ambiti, di tecnoregolazione e di normazione giuridica, per tracciare "un campo di osservazione che implica uno sguardo proteso verso più fronti" (p. 335).

Ed è proprio "uno sguardo proteso verso più fronti" che il volume curato da Casadei e Pietropaoli complessivamente offre, non limitandosi mai ad una prospettiva, ad un ambito applicativo, bensì integrando profili teorici e pratici, critici e applicativi, delle più recenti tecnologie e del diritto, sempre più lento della tecnica ma oggi più che mai necessario a limitarne i

risvolti rischiosi e dannosi. Attraverso i contributi di esperti ed esperte nei settori più diversi, l'opera garantisce una visione di insieme, ampliata in questa versione da importanti sguardi critici: siffatta metodologia assicura una feconda apertura verso i mondi giuridici che hanno interagito, interagiscono e senz'altro interagiranno con l'evoluzione e lo sviluppo tecnologico.