Journal of Ethics and Legal Technologies – Volume 7(1) – June 2025

Identità digitale e intelligenza artificiale: tra regolazione, poteri asimmetrici e sfide per il futuro

Maria Novella Campagnoli[*1], *Massimo Farina*[**2]

*Università degli Studi di Roma Tor Vergata
**Università degli Studi di Cagliari

Digital identity has become a key component of today's socio-digital landscape, shaping new power dynamics in systems governed by artificial intelligence. The growing reliance on technologies such as blockchain, biometrics, and facial recognition algorithms raises complex legal challenges, ranging from privacy protection to the risks of algorithmic discrimination. This study explores the role of legal and technical regulations in the construction of digital identity, examining how digital infrastructures influence the authentication process and an individual's inclusion within a virtual community. A particular focus is given to the power mechanisms embedded in AI systems, highlighting critical issues related to facial recognition, biometric data governance, and their implications for fundamental rights. Additionally, we assess potential regulatory frameworks aimed at mitigating power imbalances in digital identity management, with special attention to emerging European and international regulations. The approach adopted is interdisciplinary, combining legal analysis, philosophy of law, and computational sciences to outline both the challenges and opportunities for a fair and sustainable governance of digital identity.

Keywords: Artificial intelligence, Robotics, Hardware, Software, Privacy, Copyright Liability, Trust

[1] Maria Novella Campagnoli – Ricercatrice (RTD-b) presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tor Vergata – campagnoli@juris.uniroma2.it. (autrice dei paragrafi nn. 1, 2, 4).
[2] Massimo Farina – Professore associato presso il DIIE dell'Università degli Studi di Cagliari – m.farina@unica.it. (autore dei paragrafi nn. 3, 5, 6).

1. Una breve introduzione ai temi e ai percorsi della ricerca

Va detto subito che, rispetto a quanto accadeva in età classica e in epoca moderna[3], oggi, parlare di identità è diventato decisamente molto più complesso; non solo perché l'uso sempre più pervasivo delle nuove tecnologie – e l'immersione nella c.d. dimensione *on-life* – favorisce lo sviluppo di profili multipli (apocrifi e/o paralleli), ma anche perché, ormai, la nostra stessa identità non può non tener conto di tutte quelle informazioni pulviscolari e di quei dati che, in vario modo, raccontano (o provano a raccontare) qualcosa di noi. Si badi, non si tratta "solo" di misurarsi con un nuovo scenario, che riproporre "in chiave digitale" la felice intuizione letteraria che fu di Pirandello[4], ma si tratta di misurarsi con un autentico mutamento di paradigma: un contesto diverso nel quale – per così dire – l'*habeas corpus* sembra destinato ad essere soppiantato dall'*habeas data*[5].

Di qui, come è evidente, tutta una serie di questioni e di criticità che chiamano in causa il giurista e, in modo particolare, il filosofo del diritto e l'esperto di informatica giuridica, nella consapevolezza che, nel momento in cui si parla di identità, si discute, innanzitutto, della persona come soggetto di diritto e, ovviamente, dei suoi diritti fondamentali.

Entro questa cornice, il contributo si propone di riflettere sull'identità digitale, nella consapevolezza che, soprattutto oggi, la costruzione del tessuto e delle dinamiche socio-digitali scaturiscono dall'intreccio e dalla sovrapposizione di molteplici livelli normativi, che, talvolta, trascendono i confini formali del diritto "tradizionale". L'avvento di Internet alla fine degli anni Novanta – accompagnato dalla successiva (e sempre più pervasiva) diffusione delle tecnologie dell'informazione e della comunicazione (ICT) – non ha semplicemente ridefinito i rapporti tra individui[6], istituzioni e mercati, ma ha anche generato inediti spazi virtuali in cui le regole giuridiche, i codici tecnici e le consuetudini sociali si stratificano e si compenetrano in maniera ibrida[7], in una prospettiva sempre più orientata al c.d. *soft law*[8]. Se un tempo la normatività era associata principalmente all'autorità statuale e al diritto codificato[9], adesso le piattaforme digitali, le comunità *online* e gli algoritmi esercitano a loro modo una forma di "potere normativo" – e se vogliamo

[3] Sul concetto di identità in generale e, in modo particolare, relativamente alla sua evoluzione rinvio alle sempre attuali riflessioni di D'Agostino (2004, 109-119).
[4] Il richiamo va, ovviamente, a *Uno, Nessuno, Centomila* (Pirandello 2014).
[5] Riprendo, qui, le intuizioni di Amato Mangiameli (2015).
[6] Cfr. Turkle, 1995 e 2012.
[7] Lessig 1999; Castells 2009.
[8] Cfr. Amato Mangiameli, 2000 e 2004.
[9] *Ibidem.*

anche una nuova forma di sovranità digitale[10] – in grado di influenzare e in senso proprio di condizionare i comportamenti e le relazioni[11]. Tale evoluzione – che ha natura sociologica oltreché spaziale e sulla quale, fra i primi, si sono interrogati Lévy (1995), Virilio (1998) – interpella i fondamenti stessi del diritto e della filosofia del diritto, spingendo a domandarsi fino a che punto sia necessario riconsiderare e risemantizzare i concetti di sovranità, di soggettività e di responsabilità[12].

Ovviamente, il tema dell'identità digitale si colloca al centro di un complesso sistema di tensioni e di opportunità. Da un lato, la rete offre agli individui nuovi canali di auto-rappresentazione, di partecipazione politica[13] e di costruzione dei legami sociali[14] ; dall'altro, il nuovo contesto accentua le asimmetrie di potere e i rischi di discriminazione, poiché le pratiche di profilazione e le strategie di marketing propongono rinnovate forme di sorveglianza[15] o, meglio, di dataveglianza, che intensificano il controllo e la commercializzazione dei dati personali[16].

Siamo, così, di fronte a un ecosistema in cui l'identità – intesa come riconoscimento giuridico e sociale – non è attestata più unicamente dai documenti cartacei rilasciati dalle autorità pubbliche, ma è dettata anche da un insieme eterogeneo di protocolli crittografici, sistemi di reputazione, algoritmi di raccomandazione e politiche di contenuto stabilite da attori privati[17]. In pratica, non si registra semplicemente un passaggio dal contesto fisico a quello virtuale, bensì un processo circolare di continua stratificazione, contaminazione e sovrapposizione, in cui il diritto convenzionale interagisce con regole tecniche e consuetudini emergenti, che, a loro volta, producono situazioni bisognose di attenzione e di riconoscimento sul piano normativo[18].

Occorre, quindi, riflettere sul modo in cui i sistemi di intelligenza artificiale e le infrastrutture digitali contribuiscano a ridefinire i criteri di autenticità e di riconoscimento[19], e su come la nozione stessa di soggetto di diritto stia

[10] A proposito della nozione di sovranità digitale si veda Mangiameli, 2023, pp. 451-460.
[11] Imprescindibile il rinvio agli studi di Thaler e Sunstein (2009) che in argomento sono oramai ritenuti un classico.
[12] Floridi 2015; Rodotà 2007.
[13] Gometz 2023.
[14] Amato Mangiameli e Campagnoli, 2020.
[15] Non a caso, da tempo, si riflette sull'avvenuto passaggio dal Panopticon (Bentham [1791], 2002) al Synopticon.
[16] Zuboff 2019.
[17] Floridi, 2015 e 2023.
[18] De Hert e Papakonstantinou 2016; Amato Mangiameli 2017)
[19] Su tale versante, il Regolamento (UE) 2024/1689 (*AI Act*) fornisce un quadro normativo armonizzato che impone obblighi di trasparenza, responsabilità e verifica dell'impatto decisionale dei sistemi di IA utilizzati per supportare processi di validazione e attribuzione dell'identità digitale. Tali requisiti mirano a garantire che l'adozione di soluzioni basate

subendo un considerevole mutamento. Si badi: la costruzione dell'identità digitale non si limita a proiettare nel mondo *online* le caratteristiche dell'individuo, ma genera un insieme di attributi e di parametri che possono essere misurati, memorizzati e in senso proprio quantificati e monetizzati[20]. Le piattaforme agiscono come arbitri di questa produzione identitaria, stabilendo condizioni d'uso, configurando interfacce e decidendo le modalità di raccolta e di trattamento dei dati[21]. Il risultato è un ordine socio-digitale in costante evoluzione, in cui i normali meccanismi di imputazione e di responsabilità finiscono per frammentarsi in una pluralità di livelli: dal fornitore di servizi che gestisce le credenziali di accesso, all'ente che emette certificati digitali, passando per la rete di server che memorizzano e processano le informazioni.

Un ulteriore elemento di complessità è dato dalla natura transnazionale delle reti digitali (per loro natura de-territorializzate e de-centralizzate)[22], che erode i confini giuridici tradizionali, ponendo sfide notevoli, tanto al diritto statale quanto alle istituzioni sovranazionali. Se un tempo il legislatore poteva legittimamente regolare i rapporti tra i suoi cittadini e i soggetti presenti nel territorio di propria competenza, ora, al contrario, nell'universo socio-digitale i flussi di dati attraversano costantemente le frontiere, e i nuovi soggetti che esercitano potere (come le Big Tech) possono scegliere, di volta in volta, le giurisdizioni più favorevoli alle proprie attività[23] . Ne deriva un nuovo pluralismo normativo, in cui si intersecano norme pubbliche, regolamenti privati, standard tecnici e prassi sociali, senza che emerga un unico centro di potere in grado di coordinare efficacemente tutte le diverse dinamiche[24] . In questo scenario, diviene fondamentale provare a individuare dei criteri di legittimazione e di giustizia che possano valere all'interno di un ambiente in cui il rapporto tra norma e territorio risulta profondamente indebolito (Floridi, 2020b).

Il presente contributo nasce proprio dall'urgenza di ripensare le basi della normatività nelle more di uno spazio ibrido in cui il potere statale, le spinte del mercato e le relazioni digitali si incontrano e si scontrano, generando nuove forme di organizzazione socio-tecnica[25] . Non si tratta, quindi, solamente di limitarsi a constatare che i social network o le piattaforme di e-commerce emanano regole sotto forma di policy e di condizioni d'uso,

sull'IA non comprometta i diritti fondamentali e favorisca la fiducia nei processi digitali.

[20] Eubanks 2019; Tallia 2018; Mayer-Schönberger e Cukier 2013.

[21] Gillespie 2021.

[22] Concetti approfonditi anche in Amato Mangiameli e Campagnoli (2020).

[23] Lessig 1999.

[24] Castells 2009; Mangiameli 2023.

[25] Pollicino 2023b.

ma di comprendere come tali regole si pongano rispetto a principi etici e giuridici inderogabili, quali l'autonomia personale, la dignità, la privacy e, non da ultimo, l'uguaglianza. Parallelamente, è fondamentale interrogarsi su come queste piattaforme incidano sulla costruzione dell'identità digitale individuale: se, infatti, la persona fisica trovava un punto di riferimento certo negli atti ufficiali e nelle procedure statali, di contro, la persona digitale vede moltiplicarsi i canali di identificazione, con notevoli rischi di inconsapevolezza e di possibile manipolazione[26]. Il quadro che emerge è un insieme multi-sfaccettato, ricco di opportunità (pensiamo alle possibilità di partecipazione e di comunicazione), ma anche denso di criticità, soprattutto quando la regolazione algoritmica rischia di escludere i soggetti più deboli oppure di rafforzare stereotipi e discriminazioni[27].

Alcuni autori hanno evidenziato come la tensione tra *"Through Norms"* (norme giuridiche tradizionali) e *"Beyond Norms"* (pratiche informali, codici tecnici e dinamiche auto-organizzative) rifletta un mutamento strutturale del diritto e dell'ordine sociale[28]. Lungi dall'opporre in maniera netta il diritto statale ai meccanismi digitali, la prospettiva qui adottata punta a mostrare che la costruzione del socio-digitale è il frutto di una continua negoziazione tra poteri, diritti e forme di innovazione, in un processo di "co-costruzione" all'interno del quale nessuna fonte normativa conserva più un primato incontestato[29] . In altre parole, la sfera digitale non è meramente uno spazio virtuale o "derivato", ma si pone ormai come una dimensione costitutiva della realtà stessa, dove i soggetti agiscono in parte come cittadini tradizionali, in parte come consumatori o utenti di piattaforme, in parte come creatori di contenuti o operatori di reti algoritmiche[30].

Nelle more di questa trasformazione, il *focus* sull'identità digitale risponde all'esigenza di comprendere come la soggettività giuridica e sociale si stia riplasmando attraverso dispositivi, interfacce e canali di comunicazione che ridefiniscono le esperienze di autenticazione, relazione e appartenenza[31]. La riflessione filosofico-giuridica deve pertanto indagare i criteri di riconoscimento, la distribuzione della responsabilità, la conformazione dei diritti fondamentali e le modalità con cui l'innovazione tecnologica può essere orientata verso il perseguimento effettivo della giustizia e dell'eguaglianza[32]. Se da un lato la digitalizzazione dischiude scenari partecipativi inediti, dall'altro

[26] Boyd 2014; Tufekci 2018.
[27] Eubanks 2019; Bianchi 2021; Ziccardi 2016 e 2017.
[28] Rodotà 2007; Pagallo 2018.
[29] Floridi 2015; Amato Mangiameli 2017.
[30] Nissenbaum, 2009.
[31] Turkle, 1995; Bauman, 2010; Lovink, 2019.
[32] De Hert e Papakonstantinou 2016.

rafforza l'incidenza di meccanismi di controllo e di manipolazione su larga scala, evidenziando la necessità di un dibattito aperto sui limiti e sulle opportunità di questo mondo socio-digitale in divenire[33].

L'obiettivo di questo articolo è quello di offrire un contributo – al contempo teorico e pratico – in cui il tema dell'identità digitale funge da lente di ingrandimento privilegiata per leggere le tensioni tra le norme formali e quelle informali, tra i poteri centrali e la pervasività delle piattaforme, tra la libertà individuale e la possibile responsabilità condivisa. Nei paragrafi che seguono verranno messi a fuoco i principali snodi concettuali e le possibili evoluzioni normative, mantenendo sempre al centro l'idea che l'ecosistema digitale non si esaurisce in un apparato di *tools* tecnici, ma agisce come un non-luogo in cui comunque si gioca la definizione della soggettività e del patto sociale[34]. All'interno di questo spazio, le tensioni tra l'individuo e le strutture di potere assumono forme e modalità assolutamente inedite, generate dalla potenza analitica dei sistemi informativi, dalla scalabilità globale di alcuni *player* privati e alle quali concorre pure la vulnerabilità di alcune fasce di popolazione ancora prive di adeguata alfabetizzazione digitale[35].

L'idea è quella di prospettare un percorso che, attraverso l'analisi interdisciplinare, mira a mostrare come la costruzione socio-digitale del nostro tempo non possa prescindere da un'indagine critica sui meccanismi e sulle finalità che modellano l'identità *online*. Le norme "classiche" interagiscono, infatti, con altre "norme" che vanno "oltre il diritto", e che sono fatte di protocolli, linee guida di piattaforma, standard di design e prassi d'uso. Norme "altre" che, a loro modo, influenzano sensibilmente l'equilibrio tra tutela dei diritti fondamentali e le spinte commerciali o tecnologiche[36].

Vien da sé che – come ricordava Renato Borruso[37] – solo un dialogo aperto tra teorici e pratici, tra esponenti del settore pubblico e di quello privato, tra esperti di diritto positivo, filosofi del diritto, informatici giuridici e operatori tecnologici, può consentire di elaborare soluzioni efficaci e sostenibili, capaci di rispondere ai rapidi cambiamenti che caratterizzano la contemporaneità. In ossequio a quel vigoroso (e attualissimo) invito elevato da Sergio Cotta[38] nei confronti del giurista a farsi particolarmente *engagé* dinnanzi alle sfide poste dalla tecnologia.

[33] Zuboff 2019; Amato Mangiameli 2019; Casadei e Andronico 2021; Benasayag 2020; Cardon 2016; Domingos 2016.
[34] Castells 2009.
[35] Hargittai 2002.
[36] Lessig 1999.
[37] Borruso 1990.
[38] Cotta 1968.

È con questo spirito, che ci addentriamo nell'indagine dei molteplici volti di un mondo dove il digitale non è più un semplice canale di comunicazione, ma il tessuto connettivo su cui si articolano le relazioni umane, le dinamiche economiche e i processi di normazione.

2. Come cambia l'identità nella società digitale

La riflessione filosofico-giuridica sull'identità digitale emerge nel contesto di una trasformazione profonda dei rapporti sociali, economici e politici, che – come s'è già avuto modo di accennare – ha progressivamente ridisegnato i confini tradizionali della soggettività. Mentre l'idea classica di persona[39] in ambito giuridico si fondava, in larga parte, sull'iscrizione del singolo in un quadro istituzionale stabile, garantito da documenti ufficiali e da relazioni sociali prevalentemente materiali/fisiche, la dimensione digitale introduce variabili inedite, come la smaterializzazione dei supporti, la registrazione capillare delle tracce comportamentali e la possibilità di sperimentare una molteplicità di ruoli e identità attraverso piattaforme e reti globali[40]. In questa prospettiva, la costruzione dell'identità non è più riconducibile soltanto all'autocoscienza individuale o alla legittimazione da parte di un'autorità statale, ma si articola su più livelli di interazione e negoziazione[41], che si sviluppano in modo continuo e trasversale tra ambienti *online* e *offline* (Floridi, 2015; Iaselli, 2023).

Il carattere immateriale della rete solleva, anzitutto, una questione di fondo: in che modo la persona – intesa come soggetto di diritti e doveri – riesce a conservare e a riaffermare la propria autonomia e la propria dignità all'interno dello spazio virtuale? Alcuni autori, in particolare Rodotà[42] e Pagallo[43], hanno sottolineato che il fenomeno dell'identità digitale non può essere visto come una semplice proiezione di quella fisica, poiché la logica algoritmica e la dimensione globale della rete ne modificano profondamente i presupposti.

[39] Stolfi 1905; De Cupis 1949.
[40] Turkle 1995; Boyd 2014.
[41] In questo scenario, il quadro normativo europeo sta mostrando la sua capacità di adattamento e trasformazione. Si pensi, ad esempio, a come il Regolamento (UE) 2024/1183 (eIDAS 2) abbia ampliato la precedente disciplina, introducendo il cosiddetto *European Digital Identity Wallet* per permettere ai cittadini di gestire in modo sicuro e interoperabile i propri attributi digitali. Un'evoluzione normativa che, non solo conferma l'importanza di un'identità digitale riconosciuta legalmente, ma evidenzia anche come il processo identitario si stia progressivamente spostando da un ambito esclusivamente statale a una rete di interazioni dinamiche, in cui il cittadino acquisisce nuove forme di autonomia e controllo.
[42] Rodotà 2007.
[43] Pagallo 2018

Il soggetto digitale si trova così a subire – e nello stesso tempo a co-creare -normative e aspettative di condotta che non dipendono più soltanto dal diritto statuale, ma anche dalle *policy* delle piattaforme, dalla *governance* algoritmica e dalle dinamiche di mercato. Questa pluralità di fattori e di fonti normative – formali e informali – moltiplica e al contempo frammenta i riferimenti identitari, configurando una sorta di pluralismo giuridico all'interno del quale l'utente fatica a individuare le regole di riconoscimento, di responsabilità e di attribuzione alle quali deve attenersi e che ne devono orientare i comportamenti[44].

Un ulteriore aspetto, che si rivela cruciale, riguarda il nesso tra identità individuale digitale e partecipazione del soggetto al discorso pubblico. Mentre la visione classica vedeva l'individuo (il cittadino) inserito all'interno dell'*agorà* e lì partecipe del discorso pubblico[45] (secondo una lettura che sarà poi ampiamente ripresa e rivista in età moderna e contemporanea da illustri filosofi del calibro di Mill[46] e Habermas[47]), da par suo, la "società in rete"[48] sembra innescare logiche di polarizzazione e di personalizzazione dell'informazione, che, lungi dal realizzare il libero mercato delle idee, possono arrivare perfino ad alterare e a destabilizzare il concetto stesso di opinione pubblica; un fenomeno, questo, al quale, per certi versi, si è assistito anche nel 2016 in occasione delle elezioni politiche americane[49].

Diversamente dal passato, oggi l'individuo – in virtù della sua identità digitale e di quel costitutivo ribaltamento di piani (produttore/fruitore; autore/lettore) che contraddistingue il Cyberspace – si ritrova ad essere contemporaneamente consumatore e produttore di contenuti, ma soprattutto (più o meno consapevolmente) viene sottoposto a modelli di profilazione che in maniera larvata e pressoché invisibile ne influenzano le scelte e ne orientano le preferenze[50]. In questo scenario, si inscrivono fenomeni, che, per un verso, sono riconducibili all'effetto *filter bubble* o *echo chamber*[51]e, per un altro verso, sono espressione di sofisticate forme di ingegneria sociale e di tecno-regolazione[52] . Di qui, tutta una serie di problemi di *accountability* algoritmica e di trasparenza[53] , questioni che, a loro modo, mettono in discussione i fondamenti stessi della partecipazione democratica. Se, infatti, la persona è

[44] De Hert e Papakonstantinou 2016.
[45] Sul punto, imprescindibile il rinvio alle riflessioni di Foucault (2005).
[46] Cfr. Mill 1879, 36.
[47] Cfr. Habermas, 2005 e 2022.
[48] Castells 2009.
[49] Cfr. Woolley e Guilbeault 2017.
[50] Pasquale 2015.
[51] Pariser, 2012.
[52] Thaler e Sustein 2009.
[53] D'Acquisto 2022.

profilata in base ai dati e ai metadati, ecco che l'identità digitale non diventa soltanto uno strumento di auto-rappresentazione[54] , ma anche un oggetto/mezzo di manipolazione economica e/o politica, potenzialmente lesivo del principio di autodeterminazione[55]

La costruzione dell'identità digitale coinvolge, inoltre, i concetti di verità e di autenticità, capisaldi non solo della filosofia ma anche – e soprattutto – del diritto. Mentre l'identità fisica è a suo modo rigida, associata a un corpo univoco e a dei documenti ufficiali rilasciati dall'autorità (che, come sottolinea D'Agostino [2004], sono sì suscettibili di potenziali alterazioni, ma che, certo, sono meno esposti ai rischi del mondo *online*), la dimensione digitale concorre a estendere il numero dei canali e delle modalità di riconoscimento: dalle credenziali d'accesso agli avatar virtuali, dai sistemi di reputazione e di rating ai dati biometrici, sino ad arrivare alle firme elettroniche. Di qui, da un lato, la possibilità (alla quale si è fatto cenno nell'introduzione) di sperimentare e di ridefinire a piacimento e se stessi (in rete si può essere tanti sé diversi, giovani/vecchi, maschi/femmine/altro…)[56], dall'altro, il rischio che vengano irrimediabilmente minate la coerenza e la verificabilità delle informazioni, soprattutto quando l'intelligenza artificiale e le reti neurali producono deepfake o sistemi di autenticazione fallibili[57]. La persona giuridica – intesa come entità unitaria titolare di diritti – rischia così di frantumarsi in una serie di identità parziali, ciascuna regolata da algoritmi differenti, creando una sorta dissonanza ontologica tra l'essere (fisico) e l'apparire (digitale). Dal punto di vista normativo, ciò induce a riflettere su come garantire la continuità della soggettività e la certezza dei rapporti giuridici, in un contesto in cui la prova dell'identità e la validità degli atti dipendono dalla corretta funzionalità di piattaforme globali, spesso opache e centrate su interessi privati[58] .

Da questa premessa discende la necessità di elaborare una filosofia dei diritti digitali che non si limiti a proteggere la privacy o il diritto all'oblio, ma che ponga al centro la dignità della persona come criterio regolativo dell'ecosistema *online*[59]Tale prospettiva riconosce che l'identità digitale non è un oggetto statico[60] , bensì un processo di continuo riassetto di ruoli, relazioni e narrazioni[61], che si svolge su piattaforme controllate da soggetti privati capaci di plasmare, per mezzo delle loro *policies* e dei loro algoritmi,

[54] Lovink 2019.
[55] Benanti 2020, 2022.
[56] Turkle, 1995.
[57] Eubanks, 2019.
[58] Gillespie 2021.
[59] Rodotà 2007; Benanti 2024.
[60] Tiribelli 2023.
[61] Riva 2025.

intere aree della vita sociale[62]. In linea con l'impostazione *"Through Norms, beyond Norms"* – e richiamandosi anche alle ben note osservazioni di Martin Heidegger[63] a proposito della tecnica – occorre evidenziare come l'innovazione tecnologica non sia di per sé stessa mai neutrale[64]: le scelte di *design*, i modelli di business e i criteri di moderazione dei contenuti rappresentano vere e proprie norme tecniche che interagiscono con il diritto statale e con le pratiche sociali, trasformando la costruzione dell'identità in un fenomeno multidimensionale[65].

La filosofia del diritto, pertanto, si trova di fronte al duplice compito: da un lato, quello di analizzare criticamente le nuove dinamiche di potere[66] (non già coercitive quanto piuttosto seducenti e persuasive[67] che agiscono nello spazio digitale, spesso anche in contrasto con l'ideale di emancipazione individuale) e, dall'altro, quello di elaborare categorie giuridiche adeguate a un soggetto sempre più ibrido (con riferimento al quale il discrimine tra l'utente-consumatore e il titolare di diritti fondamentali tende a farsi sempre più evanescente sino a sfumare [68]). La cosiddetta etichettatura digitale[69] può presentarsi in forme mascherate di normalizzazione, in cui le piattaforme esercitano un potere quasi sovrano, definendo i criteri di accesso e di riconoscimento. Parallelamente, i meccanismi di sorveglianza e di profilazione rischiano di esacerbare le disuguaglianze e di andare a colpire proprio i soggetti più vulnerabili[70].

[62] Couldry e Mejias, 2019.
[63] trad. it. 2017.
[64] Così si esprimeva sul punto il celebre filosofo: "[…] l'essenza della tecnica non è affatto qualcosa di tecnico. Non possiamo quindi esperire veramente il nostro rapporto con l'essenza della tecnica finché ci limitiamo a rappresentarci la tecnicità e a praticarla, a rassegnarci ad essa o a fuggirla. Restiamo sempre prigionieri della tecnica e incatenati ad essa, sia che la accettiamo con entusiasmo, sia che la neghiamo con veemenza. Ma siamo ancora più gravemente in suo potere quando la consideriamo qualcosa di neutrale […] questa rappresentazione, che oggi si tende ad accettare con particolare favore, ci rende completamente ciechi di fronte all'essenza della tecnica".
[65] Floridi 2015; Amato Mangiameli 2017.
[66] Impossibile non ricordare quanto osservava – fra i primi – Castells (2013): "[…] i rapporti di potere, fondamento delle istituzioni che organizzano la società, vengono in larga misura costruiti nella mente degli individui attraverso determinati processi comunicativi. I meccanismi che consentono di plasmare le menti rappresentano un sistema di dominio più potente e duraturo della sottomissione dei corpi per mezzo dell'intimidazione o della violenza".
[67] Pressoché immediato, qui, il richiamo a Orwel (dove, con riguardo al potere del Partito, si legge: *"Orthodoxy means not thinking not needing to think. Orthodoxy is unconsciousness"*). Inoltre, fra i classici, imprescindibile il richiamo agli studi di Durkheim (1894).
[68] Bauman 2000.
[69] Rodotà 2007.
[70] Eubanks 2019; Tommasi 2020; Morondo Taramundi 2022.

Anche il tema della memoria digitale[71] assume una valenza peculiare: non si tratta soltanto di consentire all'utente di rimuovere le informazioni obsolete o dannose, ma di riconoscere che la dimensione storica della persona, in rete, è conservata e riplasmata da soggetti terzi, spesso a scopo di profitto [72]. La perdita del controllo sui propri dati può condurre a vere e proprie forme di espropriazione identitaria, in cui la narrazione personale è filtrata e reindirizzata dagli algoritmi di indicizzazione e dai motori di ricerca[73]. Qui, il contrasto tra la volontà individuale di autodeterminazione e il potere dei gestori di piattaforma diviene palese, richiamando la necessità di un intervento regolativo che coniughi il diritto statale con le norme di *design* e con la responsabilità sociale delle imprese[74].

Dal quadro sin qui delineato emerge come l'identità digitale rappresenti un aspetto nodale per comprendere la complessità della dimensione socio-digitale. A regolamentare (e soprattutto a garantire) l'identità nel contesto digitale non bastano le norme giuridiche tradizionali: la costruzione dell'identità, infatti, implica una negoziazione continua tra attori diversi, ciascuno portatore di valori e interessi specifici. La rete non è più soltanto un canale di comunicazione, ma un vero e proprio ecosistema normativo in cui si assegnano valore, credibilità e fiducia ai diversi soggetti[75] . Per interpretare e orientare questo fenomeno, ci si deve confrontare con l'estrema rapidità dei cambiamenti tecnologici e con l'emergere di pratiche sociali e culturali che sfuggono ai confini della singola giurisdizione[76] . Comprendere le forme di *governance*, le responsabilità degli attori e le implicazioni etiche delle soluzioni tecniche diviene fondamentale per elaborare modelli di regolazione in grado di assicurare spazi di libertà e di giustizia compatibili con la dimensione algoritmica del potere (o, meglio, e dei nuovi poteri)[77].

3. Intelligenza Artificiale e gestione dell'identità digitale

La presenza sempre più pervasiva dell'intelligenza artificiale (IA) all'interno degli ecosistemi digitali ha profondamente trasformato le dinamiche di gestione dell'identità, influenzando sia le forme di riconoscimento personale sia i modelli di relazione sociale. Se, per un verso, le tecnologie di IA consentono, in linea di principio, una maggiore precisione nell'autenticazione (ad

[71] Ziccardi, 2017.
[72] Norris, Inglehart 2019; Riva 2016; Riva, Gaggioli 2019.
[73] Pasquale 2015.
[74] Tufekci 2018.
[75] De Hert e Papakonstantinou 2016; Fabris 2018; Pascuzzi 2020; Finocchiaro 2024)
[76] Moro e Sarra 2017; Amato Mangiameli 2015, 2017, 2020; Floridi 2020°.
[77] Vespignani 2019; Mangiameli 2023; Pollicino, Dunn 2024

esempio, tramite sistemi di riconoscimento facciale o di analisi biometrica), per un altro verso, esse introducono al contempo rischi di discriminazione, sorveglianza estesa e manipolazione. Come si è accennato, in una prospettiva filosofico-giuridica, l'incontro tra IA e identità digitale solleva numerose questioni in merito alla distribuzione del potere, all'*accountability* dei processi decisionali automatizzati e alla tenuta dei diritti fondamentali[78].

i) Un primo aspetto critico riguarda la capacità dell'IA di effettuare classificazioni e profilazioni degli utenti sulla base di enormi quantità di dati, generando identità algoritmiche che possono risultare divergenti dalla percezione di sé o dalle qualifiche giuridiche ufficiali[79] . Algoritmi di machine learning, infatti, non si limitano a riconoscere i tratti biometrici, ma elaborano correlazioni statistiche su comportamenti, preferenze[80] e reti relazionali, creando una vera e propria "mappa digitale" della persona[81] .

Un aspetto particolarmente controverso, in questa prospettiva, è dato dal fatto che l'utente spesso ignora i criteri di analisi e i parametri di valutazione che di volta in volta vengono adottati, trovandosi in una posizione di sostanziale asimmetria rispetto alle piattaforme che gestiscono l'infrastruttura tecnologica[82]. Di qui, come è evidente, non solo la percezione di trovarsi dinnanzi ad una nuova dittatura dell'algoritmo[83] (*rectius* degli algoritmi), ma anche tutta una serie di potenziali – e assai preoccupanti – violazioni della privacy e della dignità, laddove l'IA associ l'individuo a categorie "sensibili" (etnia, orientamenti politici o religiosi, ecc.) o ne pregiudichi l'accesso a servizi essenziali (assicurazioni, prestiti bancari, opportunità lavorative) sulla base di punteggi o *rating* opachi[84].

ii) Secondariamente, non si può non sottolineare che l'intelligenza artificiale a suo modo suggerisce un ripensamento e una ricodifica del concetto stesso di responsabilità, poiché i processi decisionali automatizzati si reggo-

[78] Eubanks 2019; Pasquale 2015.

[79] Boyd, 2014.

[80] Sul punto, è interessante ricordare quanto osservato – con il consueto acume e già diversi anni fa – da Bauman relativamente alla conoscenza dettagliata (di inclinazioni, gusti e preferenze), sviluppata da Amazon nei confronti dei diversi utenti: "ogni volta che entro nel sito di Amazon vengo accolto da una serie di titoli 'selezionati appositamente per te, Zygmunt'. Dati i miei precedenti acquisti di libri, c'è un'ottima probabilità che quei consigli siano una tentazione… e di solito è così! Ovviamente, grazie alla mia inavvertita ma ubbidiente collaborazione, i server di Amazon conoscono ormai meglio di me le mie preferenze e i miei hobby. Questi suggerimenti non mi appaiono più come pubblicità, ma come un aiuto amichevole nel muovermi nella giungla del mercato librario. Ringrazio, e ogni volta che acquisto un libro pago per aggiornare le mie preferenze negli archivi di Amazon e orientare così in modo infallibile i miei acquisti […]" (Bauman, Lyon 2015, 115-116).

[81] Tufekci 2018.

[82] Gillespie 2021.

[83] Fra gli altri, cfr. Benanti 2018; Benasayag 2020.

[84] Eubanks 2018.

no su algoritmi spesso non trasparenti e su *dataset* che possono contenere *bias*. Tale caratteristica fa emergere ulteriori interrogativi. Fra tutti: se l'identità digitale di un individuo viene ridisegnata e/o filtrata da un sistema di IA che sbaglia la classificazione o che perpetua stereotipi discriminatori, chi dovrebbe risponderne[85]? Il progettista dell'algoritmo, l'azienda che lo commercializza o l'ente che lo implementa? Vien da sé che la filosofia del diritto sia in prima linea fra le discipline che sono chiamate a elaborare nuovi schemi di imputazione, in grado di tenere conto dei molteplici soggetti coinvolti nella catena di sviluppo, addestramento e utilizzo dei modelli di IA[86] e, soprattutto, di muoversi fra lo *jus conditum* e lo *jus condendum*. Il tutto, con l'intento primario di rispondere agli orizzonti d'attesa della società digitale[87]. La proposta di estendere la soggettività giuridica a sistemi autonomi avanzati ha suscitato ampi e controversi dibattiti, evidenziando la tensione tra l'esigenza di individuare un responsabile e la natura distribuita e complessa dei processi algoritmici[88]. A creare non poche difficoltà sul punto è, infatti, il sempre maggiore grado di indipendenza e di imprevedibilità acquisito dai nuovi *attanti*[89] artificiali, che – grazie e a causa dei sempre più sofisticati meccanismi auto-evolutivi di machine e di deep learning[90] – sono in condizione di prospettare risposte e di tenere comportamenti, che i loro stessi programmatori non sono quasi più in condizione di calcolare, né di pronosticare. Nasce qui, la *querelle* circa l'eventuale necessità/possibilità di abbandonare il tradizionale modello vicario di responsabilità[91] che – in ossequio al dogma secondo il quale *machina delinquere (et puniri) non potest*[92] – in caso di agente macchinico implica il rinvio alla responsabilità dell'uomo.

[85] Pagallo 2018; Amato Mangiameli 2019.
[86] Bassini e Pollicino 2018.
[87] Cotta 1968.
[88] Rodotà 2007.
[89] Neologismo, a cui già molti studiosi ricorrono, per non equipararli agli attori – in quanto non sono soggetti – e per riuscire comunque a distinguerli dai meri oggetti. Relativamente alla perdita di confine fra soggetti ed oggetti generata connessa all'avanzare della tecnologia, impossibile non richiamare i pionieristici e fondamentali studi di: Lévy 1990, 157; Latour 1999, 122 e 2005, 54; Teubner 2006.
[90] Per un approfondimento in ordine a tali meccanismi, cfr. Beck 2016; Surden 2014; Desai 2016; Stilgoe 2018.
[91] Fra i maggiori sostenitori della necessità di introdurre una qualche forma di responsabilità diretta in capo a questi particolari dispositivi, Hallevy 2010a, 2010b, 2010c e 2018.
[92] Formula, questa, che riprende e adatta quella classica, rivolta alle *societas* e usata per negare loro lo *status* di agente delittuoso. È interessante ricordare che – come spiega dettagliatamente Cappellini (2019) – la "storia di tale 'principio' ha radici sorprendentemente antiche. Già sul finire dell'Ottocento, la dottrina tedesca si era espressamente interrogata sulla sua validità: sebbene intelligenze artificiali e robot fossero ancora ben lungi dal venire a esistenza. Neppure il clima positivistico e scientista di quegli anni, che pure forse spiega il precoce interesse per tali tematiche, poteva tuttavia condurre a risposte al quesito che non fossero graniticamente negative."

iii) Altro snodo problematico è rappresentato dall'espansione dell'IA nel campo della sorveglianza biometrica e del riconoscimento facciale. In diversi paesi sono già attive reti di videocamere intelligenti, capaci di tracciare i movimenti delle persone e di identificarle in tempo reale attraverso algoritmi di *computer vision*. Tali sistemi, potenzialmente, consentono un monitoraggio capillare della vita quotidiana, generando basi di dati enormi su spostamenti, abitudini e relazioni interpersonali. La costruzione dell'identità digitale, in questa prospettiva, rischia di diventare una versione "controllata dall'alto" della persona, in cui l'utente non esercita alcun potere di scelta o di correzione[93]. Questo scenario pone interrogativi assai complessi su come bilanciare le esigenze di sicurezza pubblica o di efficienza amministrativa con il diritto all'autonomia, alla privacy e all'autodeterminazione informativa[94] . Ancora una volta, l'architettura stessa dei sistemi di IA si configura come una "norma tecnica"[95], che dispone di ciò che è visibile, riconosciuto e tracciato.

iv) Da non trascurare, poi, è il fenomeno delle cosiddette *deepfake*, ossia dei contenuti audiovisivi generati o manipolati attraverso tecniche di intelligenza artificiale, che possono distorcere profondamente la reputazione e l'immagine pubblica di un individuo. La possibilità di creare video o registrazioni audio perfettamente verosimili, ma completamente falsi, mette a dura prova i criteri di autenticità e la tenuta dell'identità digitale, favorendo fenomeni di disinformazione e di calunnia su larga scala[96] . Anche in questo caso, le conseguenze possono essere varie e ampiamente lesive dei diritti dell'individuo (si pensi, semplicemente a titolo d'esempio, alle connessioni con fattispecie particolarmente odiose come il *revenge porn*)[97]. In assenza di strumenti idonei a rilevare e a neutralizzare queste manipolazioni, la persona colpita si trova a dover gestire gravi ripercussioni sulla reputazione, senza che vi sia un quadro normativo robusto per richiedere la rimozione del contenuto o il risarcimento del danno. Tale scenario dimostra come l'IA, pur offrendo straordinarie opportunità creative, amplifichi le criticità relative all'integrità e al controllo dell'identità *online*.

Fortunatamente, le prospettive non si declinano solo in chiave negativa, al contrario, aprono anche a un livello decisamente promettente. L'IA, difatti, può fungere persino da volano per una migliore gestione dell'identità digitale, qualora i progetti siano sviluppati con finalità di inclusione e di tutela dei diritti. Ad esempio, gli algoritmi di analisi del linguaggio naturale potrebbero facilitare la moderazione dei contenuti offensivi o discriminatori, offrendo

[93] Zuboff 2019.
[94] Norris, Inglehart 2019.
[95] Floridi 2015.
[96] Pasquale 2015.
[97] Cfr. Lo Monte 2021; Paladino 2020.

una protezione più tempestiva alle vittime di *hate speech* [98]. Sistemi di IA *explainable* – cioè in grado di fornire ragioni e logiche delle proprie decisioni – potrebbero migliorare la trasparenza nella valutazione delle identità algoritmiche, scongiurando il rischio di arbitrarietà[99]. Inoltre, la ricerca su modelli di IA decentralizzati o *privacy-preserving* (come *federated learning* o tecniche crittografiche avanzate) potrebbe consentire una gestione più responsabile e sicura delle informazioni personali, restituendo all'utente un maggiore controllo sulla propria identità[100].

In definitiva, l'incrocio tra IA e identità digitale evidenzia la complessità del paradigma "*Through norms, beyond norms*": se, da un lato, le classiche normative statali (privacy, diritto all'oblio, responsabilità civile) cercano di arginare gli abusi, dall'altro si assiste all'emergere di regole tecniche e pratiche di progettazione che, nel bene e nel male, definiscono i contorni dell'identità *online*.

Si è detto che i modelli di responsabilità e gli strumenti di regolazione tradizionali devono necessariamente essere ripensati[101] alla luce della crescente complessità degli ecosistemi digitali e dell'urgenza di prospettare soluzioni e riforme capaci di coniugare l'innovazione tecnologica, la tutela dei diritti fondamentali del cittadino digitale e le esigenze di mercato[102].

Un primo settore di intervento riguarda la definizione di standard di trasparenza e *accountability* algoritmica, volti a rendere verificabili e comprensibili le logiche che guidano la raccolta, l'elaborazione e l'uso dei dati personali. L'Unione Europea – attraverso strumenti come il GDPR, il *Digital Services Act* e le nuove proposte di regolamentazione dell'IA – sta cercando di imporre obblighi di spiegabilità e di valutazione del rischio[103] , con l'obiettivo di scongiurare il pericolo di un potere invisibile[104] esercitato dai colossi del web e dalle piattaforme globali. Parallelamente, l'idea di certificazioni o marchi di qualità algoritmica, rilasciati da enti terzi indipendenti, ha iniziato a prendere sempre più piede nella discussione internazionale: in modo analogo ai controlli di sicurezza alimentare o ambientale, si ipotizza che un software o un sistema di IA possa essere sottoposto a verifiche circa l'assenza di bias discriminatori, la correttezza del trattamento dei dati e la robustezza delle sue decisioni[105] . Sebbene queste proposte siano ancora in fase di definizione,

[98] Tufekci 2018. Cfr. Di Rosa 2020; Pitruzzella e Pollicino 2020.
[99] Yeung 2018.
[100] Lessig, 1999
[101] Amato Mangiameli 2019; Perri 2020.
[102] Rodotà 2007.
[103] Yeung 2018.
[104] Che si nutre della nuova sorveglianza. Cfr. Calenda e Fonio 2010; Foucault 2014; Lyon 1997 e 2002.
[105] Pasquale 2015.

esse lasciano intravedere un percorso di regolazione collaborativa, in cui le istituzioni pubbliche, la società civile e gli operatori tecnologici condividano responsabilità e competenze.

Un secondo filone di sperimentazione riguarda le forme di *governance* partecipata, che mirano a coinvolgere gli utenti, le comunità e gli sviluppatori nei processi decisionali che plasmano l'architettura e le regole delle piattaforme. La centralità del consenso informato e della partecipazione democratica sono indiscussi ma applicare tali principi nel dominio digitale significa ripensare le modalità di consultazione e le sedi di discussione: forum aperti, assemblee virtuali, meccanismi di voto basati su blockchain, comitati etici indipendenti e trasparenti[106]. Alcuni progetti di *software* libero e *open source* forniscono un esempio di come la collaborazione distribuita possa produrre soluzioni tecniche e normative condivise, anche se non mancano criticità legate all'effettiva inclusività e alla disomogeneità di risorse tra i partecipanti[107]. In tal senso, la *governance* algoritmica potrebbe non essere soltanto subita dall'utente finale, ma divenire oggetto di una co-regolamentazione, dove il controllo su *policy* e standard di funzionamento sia esercitato, almeno in parte, dal basso.

Connessa a questa dimensione partecipativa è la proposta di sviluppare "piattaforme etiche" o "consorzi di fiducia", in cui i principi di equità, trasparenza e rispetto dei diritti fondamentali siano integrati nel design stesso delle soluzioni digitali. L'idea, mutuata dal filone di ricerca della cosiddetta *Ethical by Design*[108] , consiste nell'adottare un approccio proattivo, volto a prevenire discriminazioni e abusi fin dalla fase di progettazione dei sistemi. Tale modello, però, richiede un alto livello di consapevolezza e formazione sia da parte dei progettisti di *software* e algoritmi, sia da parte dei decisori politici e delle autorità regolatrici, che dovrebbero saper valutare l'impatto sociale e morale delle innovazioni proposte[109]. Senza un adeguato supporto istituzionale, il rischio è che le iniziative etiche restino confinate a nicchie sperimentali, mentre i colossi tecnologici continuano a imporre logiche di mercato incentrate sulla massimizzazione del profitto e sulla monetizzazione dei dati[110] . La sfida, dunque, consiste nel trovare meccanismi di incentivo (o di obbligo) per diffondere pratiche progettuali che tengano conto dell'interesse collettivo.

Sul piano strettamente giuridico, uno degli snodi più delicati resta la definizione della responsabilità in caso di danni causati da sistemi automatizzati

[106] Finck 2018.
[107] Lessig 1999.
[108] Floridi, Josh 2022.
[109] Gillespie 2021.
[110] Zuboff 2019.

o da dinamiche tipiche della sfera digitale, come la disinformazione o la violazione massiva di dati. Le esperienze di alcuni ordinamenti[111], ad esempio, hanno introdotto fattispecie specifiche per il danno digitale, estendendo la responsabilità anche a chi detiene il controllo effettivo degli strumenti tecnici[112] . Ciononostante, il passaggio a sistemi di intelligenza artificiale in grado di agire in modo autonomo o semi-autonomo – e la diffusione di architetture decentralizzate come la blockchain – alimentano interrogativi: è ipotizzabile attribuire personalità giuridica a un'IA particolarmente avanzata[113]? E come conciliare tale opzione con la necessità di garantire un'adeguata tutela per le vittime di errori o discriminazioni algoritmiche? La filosofia del diritto, in questa sede, può fornire categorie e principi di coerenza sistematica, ma la prassi regolativa dovrà inevitabilmente confrontarsi con un panorama tecnologico in costante evoluzione.

Un ulteriore versante di riforma concerne l'impostazione dei diritti fondamentali nell'ambiente digitale, toccando aspetti come la privacy, la libertà di espressione, il diritto all'identità e alla non discriminazione. Se i primi tentativi legislativi – dal GDPR alle normative nazionali su *cyberbullismo* e *hate speech* – hanno cercato di arginare i fenomeni più evidenti di abuso, permane una "terra di nessuno" riguardo a questioni più sottili, quali la manipolazione psicologica tramite *micro-targeting*, l'uso di dati comportamentali a fini di controllo sociale o la costruzione di bolle informative che limitano la pluralità di visioni[114]. La filosofia del diritto è chiamata a contribuire a una sistematizzazione di tali sfide, chiarendo che la persona digitale necessita di garanzie aggiuntive affinché anche nella dimensione virtuale possa essere garantita la sua autodeterminazione e la sua dignità, in un contesto dove i confini tra pubblico e privato sono costantemente ridefiniti dalle tecnologie.

[111] Si vedano, tra le altre, la *Loi* n° 2016-1321 *du 7 octobre 2016 pour une République numérique* (Francia), che inserisce nell'art. L311-3-1 del *Code des relations entre le public et l'administration* l'obbligo per la PA di spiegare ai cittadini i "principali parametri di trattamento" usati dagli algoritmi decisionali, prevedendo tutela risarcitoria in caso di malfunzionamento; la *Ley Orgánica 3/2018* spagnola, artt. 80-82, sancisce un diritto al risarcimento per i danni – anche immateriali – causati da decisioni automatizzate; mentre il *Netzwerkdurchsetzungsgesetz* (NetzDG) tedesco estende la responsabilità dei gestori di piattaforma, prevedendo sanzioni fino a 50 milioni € per mancata rimozione algoritmica di contenuti illeciti. A livello europeo l'art. 82 del Regolamento (UE) 2016/679 (GDPR) riconosce il diritto al risarcimento di danni materiali e immateriali derivanti da trattamenti illeciti; la Direttiva (UE) 2019/770 sui contratti di fornitura di contenuti e servizi digitali – recepita in Italia con d.lgs. 173/2021 – estende la responsabilità per difformità anche al *software* e agli algoritmi; la Proposta di Direttiva sulla responsabilità civile per l'IA (COM(2022) 496 final) introduce una presunzione di nesso causale quando il danno digitale deriva da sistemi ad alto rischio, ampliando l'ambito dei soggetti responsabili a chi "controlla" o "addestra" l'algoritmo.

[112] Rodotà 2007.

[113] Pagallo 2018.

[114] Tufekci 2018.

L'eventuale riconoscimento di "nuovi diritti" digitali – o l'adeguamento delle garanzie costituzionali classiche al contesto *online* – rappresenta il banco di prova su cui i poteri pubblici dovranno misurarsi, potenzialmente attraverso la codificazione di vere e proprie *Carte dei diritti digitali*[115].

Non meno importante è la dimensione internazionale e sovranazionale: le reti globali e la presenza di piattaforme transcontinentali rendono spesso inefficaci le iniziative normative limitate a singoli Stati[116]. Si va delineando, dunque, l'esigenza di accordi multilaterali o quantomeno di cornici giuridiche comuni, capaci di fornire standard minimi di protezione e di tutela. È in questo snodo che potrebbe giocare un ruolo cruciale la cooperazione tra istituzioni europee e altre realtà giuridiche avanzate (ad esempio, alcuni Stati americani o asiatici con normative evolute in tema di privacy e IA), allo scopo di evitare un "forum shopping" in cui le multinazionali scelgono le giurisdizioni più permissive e i cittadini si trovano privi di strumenti di difesa[117] .

In sintesi, le prospettive di riforma e le soluzioni sperimentali[118] nel panorama digitale si muovono verso la ricerca di un equilibrio tra la promozione dell'autonomia individuale e collettiva – attraverso strumenti come la *governance* partecipata, il *design* etico e la responsabilità algoritmica – e il rischio del consolidamento di asimmetrie di potere, in cui l'identità e i dati personali divengono la materia prima di un mercato globale sfuggente a regole chiare[119].

La filosofia del diritto, in dialogo con le altre discipline, può contribuire ad elaborare nuovi modelli di cittadinanza digitale e di responsabilità distribu-

[115] De Pasquale 2022.

[116] Mangiameli 2023.

[117] De Hert, Papakonstantinou 2016.

[118] Fra le iniziative più significative si annoverano: le *AI Regulatory Sandboxes* previste dall'art. 57 del Regolamento (UE) 2024/1689 (*AI Act*), che obbliga ogni Stato membro a istituire ambienti controllati in cui testare sistemi ad alto rischio sotto la supervisione dell'autorità competente; la *Regulatory Sandbox* dell'*Information Commissioner's Office* (ICO) del Regno Unito, avviata nella fase-beta nell'agosto 2021 e descritta nel *Regulatory Sandbox Insights Report 2024* (luglio 2024), che documenta quattordici progetti assistiti nell'applicazione della *data protection by design;* i quattro *Large-Scale Pilot Projects* dell'*EU Digital Identity Wallet* (POTENTIAL, EWC, NOBID, DC4EU), lanciati nell'aprile 2023 con il finanziamento del *Digital Europe Programme*: oltre 350 enti pubblici e privati di 26 Stati membri, Norvegia, Islanda e Ucraina stanno testando undici casi d'uso quotidiani prima del *roll-out* definitivo del *wallet* europeo.

[119] In questa cornice, il Regolamento Generale sulla Protezione dei Dati (GDPR, Reg. (UE) 2016/679) gioca un ruolo cardine, introducendo meccanismi di *data protection by design* e *data protection by default*, essenziali anche per le nuove forme di identità decentralizzata e per la tutela dai bias algoritmici.

ita[120], promuovendo una visione dell'innovazione non solo il più possibile inclusiva, ma anche – e soprattutto – conforme ai principi di giustizia[121].

4. Asimmetrie e nuovi poteri

Le tecnologie digitali e i meccanismi di intelligenza artificiale non soltanto ridefiniscono l'identità individuale, ma – come è evidente – incidono sensibilmente sui rapporti di potere che si creano all'interno della società in rete. Le forze[122] che agiscono sull'utente (sulle sue scelte e sulle sue decisioni) sono suadenti e fortemente condizionanti, un po' come ci ricorda efficacemente la favoletta della tartaruga e della volpe ripresa dall'analista militare russo Sergej P. Rastorguev:

C'era una volta una volpe che voleva mangiare una tartaruga, ma ogni volta che la volpe ci provava, la tartaruga si ritirava nel suo guscio proteggendosi. La volpe provò a mordere la tartaruga, provò a scuoterla, ma nulla. Un giorno la volpe ebbe un'idea: disse alla tartaruga che voleva comprare il suo guscio e le promise in cambio una lauta ricompensa. Ma la tartaruga, che era intelligente e che sapeva che senza il guscio a proteggerla sarebbe stata mangiata, rifiutò l'offerta. Il tempo passò, fino a quando un giorno apparve un televisore appeso a un albero, che mostrava immagini di stormi di tartarughe felici e nude. 'Volano!' – esclamò la tartaruga era stupita – 'Possono volare! E, anche io potrei farlo!' Ma, poi, pensò: 'non sarebbe pericoloso rinunciare al guscio?' Nel frattempo, Hark (la voce in televisione) annunciò che la volpe era diventata vegetariana. A quel punto, la tartaruga pensò: 'Se solo potessi togliermi il guscio, la mia vita sarebbe molto più semplice'. E, da par suo, la

[120] Sulla cittadinanza digitale si veda la *Recommendation CM/Rec(2019)10* del Consiglio d'Europa su *Developing and promoting digital citizenship education*, che delinea le competenze necessarie per partecipare attivamente alla società in rete e invita gli Stati membri a farne una priorità di policy. In ambito UE, la *European Declaration on Digital Rights and Principles for the Digital Decade* (firmata da Parlamento, Consiglio e Commissione il 15 dicembre 2022) fissa i valori di riferimento — dignità, inclusione, partecipazione democratica — che dovranno orientare la futura "cittadinanza digitale europea". Per la responsabilità distribuita nelle interazioni uomo-macchina, cfr. A. Strasser, che propone criteri per ripartire la responsabilità morale fra agenti umani e artificiali. Sul versante giuridico-costituzionale, Oreste Pollicino (2023b) elabora un modello di *digital constitutionalism* fondato su procedure di *accountability* condivisa tra Stato, piattaforme e utenti

[121] Benasayag 2020; Benanti 2020, 2022, 2024)

[122] Il riferimento è al ruolo delle piattaforme digitali, che è oggetto di crescente attenzione normativa attraverso misure che mirano a contrastare la concentrazione di potere, garantendo che le regole del gioco siano più equilibrate e che gli utenti possano esercitare un controllo effettivo sulle informazioni e sulle decisioni che li riguardano. In tal senso, il *Digital Services Act* (Regolamento (UE) 2022/2065) e il *Digital Markets Act* (Regolamento (UE) 2022/1925) sono strumenti normativi volti a imporre maggiori obblighi di trasparenza e a limitare le pratiche abusive dei cosiddetti *gatekeeper* digitali.

volpe pensò: 'Se la tartaruga rinunciasse solo al suo guscio, sarebbe molto più facile mangiarla'. Quindi la volpe pagò perché venissero trasmesse altre trasmissioni che pubblicizzavano tartarughe volanti. Alla fine, una mattina, quando il cielo sembrava più grande e più luminoso del solito, la tartaruga rimosse il suo guscio. 'Cosa non ha capito la nostra tartaruga?' – si chiede Rastorguev – 'Che lo scopo della guerra [...] è indurre un avversario a abbassare la guardia'[123].

Mutatis mutandis, l'aneddoto della volpe e della tartaruga ci dice qualcosa della nostra contemporaneità: fatta di poteri larvati, che – come si è già avuto modo di accennare – hanno sostituito la modalità-strategia coercitiva con quella persuasiva[124]. Da un lato, le piattaforme – forti di un immenso bacino di utenti e di dati – assumono il ruolo di arbitri nella gestione delle informazioni, stabilendo chi può accedere a cosa, con quali modalità e per quale finalità[125]. Dall'altro, i singoli utenti si trovano spesso in una posizione di dipendenza, poiché non dispongono di un controllo effettivo sulle infrastrutture e sui codici che "governano" le loro identità digitali[126] . Si crea, così, uno squilibrio che può tradursi in vere e proprie forme di dominio: la capacità di decidere le regole del gioco si concentra nelle mani di poche aziende o soggetti, mentre la maggioranza degli utenti subisce passivamente tali regole, con scarsa possibilità di negoziazione.

Un esempio emblematico di questo fenomeno è la gestione dei dati personali, che rappresentano la "materia prima" su cui si basa gran parte dell'economia digitale[127]. Piattaforme e servizi *online* raccolgono, analizzano e monetizzano dati di ogni tipo. Mentre gli utenti, incentivati da modelli "freemium" o da promesse di convenienza – in ossequio a una novella servitù volontaria – cedono i propri dati in cambio di servizi apparentemente gratuiti, le aziende ricavano un vantaggio competitivo enorme, costruendo modelli predittivi e profili dettagliati che possono essere venduti o utilizzati per orientare pubblicità e contenuti (Eubanks, 2019). In tale contesto, l'asimmetria informativa si somma all'asimmetria di potere[128], poiché chi possiede la capacità di elaborare i dati influenza non solo le scelte di mercato, ma anche la percezione della realtà e la definizione del discorso pubblico[129].

Le conseguenze di queste asimmetrie si manifestano su più livelli. Da un punto di vista sociale, la profilazione algoritmica può perpetuare stereotipi e

[123] Riprendo l'aneddoto da Campagnoli 2020, 39-40.
[124] Cfr. Cialdini 2022.
[125] Gillespie 2021.
[126] Lessig 1999.
[127] Zuboff 2019; Tallia 2018; Benanti 2022.
[128] Cfr. Colombo 2013.
[129] Castells 2009, 2013.

discriminazioni, se i dataset di addestramento riflettono pregiudizi storici o culturali[130] . In ambito politico, il micro-targeting e la personalizzazione spinta dei contenuti informativi possono polarizzare le opinioni e restringere la sfera del dibattito pubblico, creando bolle informative dove ciascuno vede soltanto ciò che conferma le proprie idee[131] . Sul piano personale, l'identità digitale dell'utente diventa oggetto di manipolazioni e stratificazioni cui è difficile opporre resistenza, poiché le pratiche di raccolta dati e di raccomandazione algoritmica operano con logiche opache, difficilmente ricostruibili dall'esterno[132]. In questa prospettiva, l'identità digitale non è più un semplice riflesso dell'identità fisica, bensì un insieme di etichette e/o la risultanza di punteggi assegnati da sistemi su cui la persona non esercita alcun controllo.

Un ulteriore fattore di squilibrio risiede nella capacità delle piattaforme di modulare – spesso in modo unilaterale – le *policy* e le condizioni d'uso, determinando così i confini di ciò che è consentito o vietato nello spazio digitale[133]. Se, in teoria, gli utenti potrebbero abbandonare il servizio in caso di dissenso, nella pratica la concentrazione di mercato e il *lock-in* tecnologico rendono questa opzione poco realistica. Al punto che, con riguardo ai contratti di questo tipo, più che di consenso sarebbe forse più appropriato parlare di assenso da parte dell'utente.

Il potere quasi "normativo" delle piattaforme si manifesta, ad esempio, nelle controversie sulla moderazione dei contenuti: la rimozione di post, account o gruppi di discussione può impattare significativamente sulla libertà di espressione e sulla partecipazione politica, senza che esista un meccanismo chiaro di tutela o di contraddittorio[134]. Tale discrezionalità, che a volte risponde a interessi commerciali o pressioni esterne, mette in crisi i principi dello Stato di diritto, poiché la sanzione e la censura avvengono in un contesto privatistico, senza un sistema istituzionale di checks and balances[135].

Le asimmetrie di potere si estendono anche alla sfera lavorativa, dove l'identità digitale funge da "biglietto da visita" per accedere a opportunità professionali o per gestire relazioni di lavoro. Le piattaforme di *gig economy*, ad esempio, assegnano rating ai lavoratori in base a *feedback* dei clienti o a parametri di produttività, creando una forma di "classifica permanente" che può favorire alcuni e marginalizzarne altri[136] . In assenza di un quadro normativo che disciplini queste dinamiche, la reputazione digitale si tramuta in

[130] Eubanks 2019.
[131] Castells 2013; Tufekci 2018.
[132] Pasquale 2015.
[133] Pollicino 2023°.
[134] Gillespie 2021.
[135] Rodotà 2007.
[136] Bauman 2000.

una fonte di disuguaglianza, esponendo i lavoratori a valutazioni arbitrarie e consolidando rapporti di dipendenza[137]. L'utente-lavoratore, privo di un contratto stabile e vincolato al punteggio, subisce il potere dell'algoritmo e la flessibilità illimitata richiesta dalla piattaforma, senza una reale possibilità di contrattazione collettiva o di tutela sindacale.

Da un punto di vista filosofico-giuridico, queste asimmetrie sollevano anche il problema della legittimità: in base a quale autorità le piattaforme, gli algoritmi o i gestori di infrastrutture digitali si arrogano l'autorità di fissare regole e punteggi? Se la teoria classica fondava la validità della norma sul patto sociale o sulla sovranità popolare, nell'era digitale osserviamo la legittimazione "per contratto" (i termini di servizio) o "per egemonia di mercato", e un uso crescente di metriche e protocolli tecnici come fonti di normatività[138] . La "norma" non è più emanata soltanto dal potere legislativo, ma promana anche dal codice di funzionamento delle piattaforme[139]. Questa compenetrazione tra norme giuridiche, regole tecniche e meccanismi di mercato genera una forma di pluralismo regolativo[140] in cui gli utenti, spesso inconsapevoli, si ritrovano a doversi destreggiare a fatica fra gli obblighi giuridici formali e quelli che, invece, sono imposti con strumenti privati.

A tutto ciò si aggiunge il fatto che spesso i vuoti di disciplina e le sovrapposizioni tra giurisdizioni consentono alle grandi imprese tecnologiche di aggirare agevolmente persino le normative più restrittive, ricorrendo alla logica del "forum shopping"[141] Ciò rende difficile, se non impossibile, un controllo effettivo sull'uso dei dati e sulle pratiche algoritmiche potenzialmente lesive di diritti fondamentali[142]. Fra l'altro, la stessa rapidità con cui si evolvono le tecnologie digitali e l'intelligenza artificiale fa apparire decisamente obsoleto l'approccio giuridico tradizionale, basato su leggi elaborate in tempi lunghi, che spesso arrivano in ritardo rispetto alle innovazioni. Il risultato è uno scenario di incertezza e imprevedibilità, in cui le piattaforme agiscono come poteri normativi *de facto*, mentre gli Stati li "rincorrono", tentando di correggere *ex post* distorsioni e soprusi[143].

Ora, se è vero che queste forme di potere (alternative e sommerse), se incontrollate, possono restituirci una realtà digitale in cui l'autonomia personale e i diritti fondamentali rischiano di essere sottomessi a logiche privatistiche (orientate al profitto o alla massimizzazione del controllo), è altrettanto vero

[137] Eubanks 2019.
[138] Floridi 2015.
[139] Lessig 1999.
[140] De Hert e Papakonstantinou 2016.
[141] Amato Mangiameli 2015, 2020; Ferrari 2013).
[142] Rodotà 2007.
[143] Pasquale 2015.

che via via si fanno strada possibili soluzioni sperimentali atte a ridurre le disuguaglianze, in un equilibrio tra libertà individuale, protezione dei dati e responsabilità collettiva. In quest'ottica, l'approccio multi-stakeholder, unito ad alcune iniziative di *governance* partecipata e alle nuove frontiere dell'etica del design, possono rivelarsi utili a offrire meccanismi di regolazione più flessibili e inclusivi, in sintonia con i principi di giustizia e autonomia tipici della riflessione filosofico-giuridica.

5. Tra prospettive normative e soluzioni sperimentali

S'è detto, la tutela dell'identità digitale – e in generale dei diritti fondamentali – richiede interventi mirati, capaci di armonizzare le esigenze dei diversi attori coinvolti. Da un lato, gli Stati e le istituzioni sovranazionali tentano di aggiornare i propri strumenti legislativi, al fine di contrastare gli abusi e di garantire maggiore trasparenza nel trattamento dei dati personali[144] . Dall'altro, le piattaforme e le comunità di utenti sperimentano forme di *governance* partecipata, in cui la definizione delle regole e dei parametri di interazione avviene con un certo grado di coinvolgimento dal basso[145] . In questo quadro, assumono rilievo tanto gli approcci multi-stakeholder, che vedono la collaborazione di governi, imprese e società civile, quanto le soluzioni tecniche ispirate ai principi di *design etico* e *accountability by design*[146]

Uno dei filoni più interessanti riguarda l'idea di *governance* partecipativa. Alcuni progetti, soprattutto in ambito *open source* e *blockchain*, mirano a includere gli utenti nella fase di stesura delle policy e nella verifica dei meccanismi di moderazione, ricorrendo a strumenti come votazioni elettroniche, assemblee virtuali o comitati etici[147] . Sebbene tali iniziative siano ancora limitate a contesti sperimentali, esse mostrano come la regolazione possa essere "co-costruita" dai diversi stakeholder, evitando di relegare l'utente al ruolo di semplice destinatario passivo di norme imposte dall'alto. La stessa logica *multi-stakeholder* è stata adottata in alcuni consessi sovranazionali – si pensi, ad esempio, agli Internet *Governance* Forum (IGF) – dove governi, imprese e organizzazioni non governative discutono le linee guida per la gestione delle risorse critiche di Internet. Queste esperienze, però, scontano la difficoltà di rendere vincolanti gli accordi raggiunti e l'eterogeneità degli interessi rappresentati[148].

[144] De Hert e Papakonstantinou 2016.
[145] Gillespie 2021.
[146] Floridi 2020b.
[147] Lessig 1999.
[148] Abba, Alù 2020

Sul piano legislativo, alcune riforme puntano a integrare o rafforzare gli strumenti di tutela esistenti. Il GDPR (Regolamento Generale sulla Protezione dei Dati) nell'Unione Europea rappresenta un esempio di normativa volta a restituire un maggiore controllo ai cittadini, imponendo obblighi di informativa, consenso[149] e portabilità dei dati[150]. Tuttavia, permangono dubbi sulla reale efficacia del regolamento di fronte alla capacità delle grandi piattaforme di aggirare o negoziare le sanzioni[151].

Più di recente, proposte legislative riguardanti l'intelligenza artificiale – è il caso dell'*AI Act* – hanno mirato a introdurre principi di *risk-based approach* individuando settori ad alto rischio (ad esempio la sanità o il credito) per cui sarebbe necessaria una supervisione più stringente[152] . Tali iniziative – senza alcun dubbio apprezzabili dal punto di vista della tutela dei diritti – suscitano al contempo il timore di ostacolare l'innovazione. È dunque evidente una certa tensione tra la volontà di regolare *ex ante* i possibili abusi e la necessità di non soffocare la ricerca e lo sviluppo.

[149] Degno di nota, in tal senso, è sicuramente l'articolo 7, che disciplina le Condizioni per il consenso. Qui, si legge "1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. 2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante. 3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato. 4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".

[150] Così, l'articolo 30 del GDPR: "1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati. 2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. 3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui".

[151] Rodotà, 2006

[152] Yeung 2018.

Un approccio intermedio si rintraccia nelle soluzioni tecniche basate su principi di *privacy by design* e di *accountability by design*. Invece di affidarsi unicamente a norme legislative, tale prospettiva suggerisce che i sistemi informativi e le piattaforme debbano incorporare, fin dalla fase di progettazione, meccanismi di tutela dei dati personali, di trasparenza algoritmica e di equità decisionale. Ad esempio, l'uso di protocolli crittografici *end-to-end*, sistemi di anonimizzazione o architetture decentralizzate può ridurre la concentrazione del potere e prevenire abusi nella gestione dell'identità digitale[153]. Analogamente, la creazione di interfacce che rendano comprensibili i criteri di classificazione e i parametri dei rating algoritmici potrebbe promuovere un controllo più consapevole da parte degli utenti[154]. Tuttavia, l'adozione su larga scala di questi standard richiede incentivi adeguati e la volontà politica di imporre requisiti tecnici anche a soggetti che detengono posizioni dominanti sul mercato[155].

Un altro ambito di sperimentazione è dato dalle identità digitali *self-sovereign*[156], in cui la persona conserva la piena titolarità dei propri attributi e decide in modo granulare quali informazioni condividere e con chi. Grazie a infrastrutture decentralizzate (spesso basate su *blockchain*) e a protocolli di verifica crittografica, questi modelli mirano a sottrarre la gestione dell'identità dalle mani dei gestori di piattaforma, restituendo all'individuo il potere di controllare i propri dati[157].

Sebbene si tratti ancora di progetti sperimentali, il potenziale di queste soluzioni risiede nel fatto che la fiducia è ripartita tra più nodi della rete, riducendo il rischio di abuso o censura da parte di un unico ente centralizzato. Rimane, tuttavia, la sfida di combinare la flessibilità dell'autogestione con la sicurezza giuridica, dal momento che lo Stato e le istituzioni conservano un ruolo cruciale nel riconoscimento formale della personalità giuridica[158].

[153] Finck 2018.
[154] Eubanks 2019.
[155] Pasquale 2015.
[156] Il dibattito sulle identità self-sovereign si è intensificato soprattutto dopo l'approvazione della nuova versione del regolamento eIDAS 2.0 (Reg. UE 2024/1183), che introduce il *European Digital Identity Wallet*: un portafoglio d'identità digitale, interoperabile a livello unionale, destinato a contenere attributi certificati e a consentire la condivisione selettiva dei dati grazie a meccanismi di "*attribute-based disclosure*" e di crittografia omomorfica. Sul piano degli standard, la raccomandazione W3C sui Decentralized Identifiers (DID) v 1.0 fornisce la sintassi degli identificativi gestiti direttamente dall'utente, mentre la versione 2.0 del *Verifiable Credentials Data Model* descrive la struttura crittografica delle attestazioni che possono essere rilasciate da autorità pubbliche e verificate "*on-chain*" senza passare per database centralizzati
[157] Finck 2018.
[158] De Hert, Papakonstantinou 2016.

A livello istituzionale, alcune iniziative[159] guardano alla creazione di autorità indipendenti con poteri di supervisione sugli algoritmi e sulle pratiche di profilazione, in modo da garantire un audit esterno e imparziale. Questi organismi potrebbero collaborare con le autorità garanti della protezione dei dati, dando seguito alle istanze dei cittadini e svolgendo verifiche periodiche sui sistemi automatizzati di maggiore impatto[160]. Tale proposta mira a ricreare, almeno in parte, quel sistema di *checks and balances* che caratterizza le democrazie costituzionali, ma appare complesso da attuare su scala globale, a causa delle differenze tra i vari ordinamenti nazionali e del potere contrattuale delle grandi piattaforme transnazionali.

Nel complesso, le prospettive normative e le soluzioni sperimentali che emergono dall'odierna discussione ruotano attorno a un equilibrio delicato: da un lato, l'esigenza di arginare gli effetti perversi della concentrazione di potere e delle asimmetrie informative; dall'altro, la volontà di non soffocare le opportunità offerte dalle tecnologie digitali, che possono favorire l'innovazione, la trasparenza e la partecipazione. La sfida consiste nel delineare una *governance* della sfera socio-digitale in cui i principi di democrazia, eguaglianza e dignità della persona[161] non siano messi in secondo piano rispetto alle logiche commerciali o all'efficienza tecnologica[162].

In tal senso, la pluralità degli attori coinvolti – legislatori, giudici, imprese, comunità di sviluppatori, organizzazioni internazionali e singoli utenti – potrebbe rappresentare una risorsa, qualora si prevedessero meccanismi di consultazione e co-decisione partecipativi e inclusivi. D'altro canto, la mancanza di un'effettiva volontà politica o di un quadro istituzionale condiviso (il più possibile omogeneo e convergente) rischia di ridurre tali esperimenti a semplici buone intenzioni, incapaci di scalfire il potere consolidato delle grandi piattaforme[163] . La filosofia del diritto e l'informatica giuridica, in questo contesto, hanno il compito di offrire un contributo critico e propositivo,

[159] Esempi recenti di autorità o standard dedicati alla supervisione algoritmica sono: il *Digital Services Act* (Reg. UE 2022/2065), che impone a ogni Stato membro di designare un Digital Services Coordinator con poteri di indagine, ingiunzione e sanzione sulle piattaforme online; il nuovo *AI Act* (Reg. UE 2024/1689), che istituisce presso la Commissione l'European AI Office e affida a specifiche autorità nazionali la vigilanza sui sistemi ad alto rischio e sui modelli di IA generali; la *CNIL* francese, che dal 2017 ospita la missione "Algorithmes et IA" e ha pubblicato il rapporto *Comment permettre à l'homme de garder la main?* per promuovere audit etici e tecnici sugli algoritmi pubblici; nel Regno Unito, la *Algorithmic Transparency Recording Standard* (GDS/Digital Service, 2023) e il *Centre for Data Ethics and Innovation* (CDEI), che forniscono linee guida e valutazioni indipendenti dei sistemi automatizzati impiegati nel settore pubblico.

[160] Simoncini 2021.

[161] Benanti 2020, 2022, 2024.

[162] Rodotà 2007.

[163] Tufekci 2018.

elaborando concetti e categorie che permettano di connettere la sfera del diritto positivo con le regole emergenti dai codici tecnici e dalle prassi sociali, nella cornice di un'etica pubblica sensibile ai mutamenti dell'era digitale[164].

Solo attraverso un confronto costruttivo tra i diversi approcci – giuridici, tecnici, etici, politici – sarà possibile elaborare una regolazione polifonica, in grado di attenuare gli squilibri e di valorizzare la dimensione democratica del mondo socio-digitale. L'identità, in questo orizzonte, non è un dato acquisito, bensì il risultato di un processo collettivo che coinvolge libertà e diritti, mercato e tecnologie, tradizione giuridica e innovazione istituzionale.

6. Traiettorie di ricerca

La ricognizione sulle asimmetrie di potere e sui vuoti normativi, nonché sulle possibili soluzioni di *governance* e di sperimentazione strategica, delinea un quadro in cui l'identità digitale è la cartina di tornasole delle sfide dell'odierna realtà socio-tecnologica[165]. Lungi dall'essere un semplice riflesso della soggettività fisica, l'identità in rete rappresenta la sintesi dinamica di processi di profilazione, *policy* di piattaforma e regimi di responsabilità che sfuggono ai confini del diritto codificato. In questo scenario, le tensioni tra norme formali e norme "oltre il diritto" – ovvero, gli standard tecnici e le prassi sociali – rendono palese l'urgenza di elaborare meccanismi di regolazione capaci di connettere l'agire degli Stati, delle imprese e degli individui in un orizzonte di giustizia e dignità[166]

Per un verso, le istituzioni pubbliche devono aggiornare i propri strumenti legislativi e giurisprudenziali, tenendo il passo con l'innovazione e tutelando i diritti fondamentali. Per un altro verso, le piattaforme globali, nella veste di nuovi poteri privati, devono sviluppare forme di autodisciplina e *governance* partecipata, se vogliono evitare un futuro di sempre maggior diffidenza e conflitto con gli utenti [167]. Le sperimentazioni in ambito blockchain, open source e identità *self-sovereign* prospettano modelli di decentralizzazione che potrebbero restituire controllo e responsabilità ai singoli, ma sollevano an-

[164] Amato Mangiameli 2019, 2020.

[165] Le più recenti normative europee – come il Regolamento (UE) 2024/1183 (eIDAS 2) e il Regolamento (UE) 2024/1689 (Artificial Intelligence Act) – rappresentano strumenti fondamentali per garantire un'identità digitale sicura e interoperabile, nonché per regolamentare l'uso dell'intelligenza artificiale in modo da tutelare i diritti fondamentali, Tuttavia, va evidenziato, che il successo di questo quadro normativo dipende in larga misura dalla capacità di implementazione e dall'aggiornamento continuo in risposta all'evoluzione tecnologica e, per questo, impone un impegno costante da parte di istituzioni, imprese e cittadini per tradurre in pratica i principi di trasparenza, inclusività e responsabilità.

[166] Rodotà 2007; Floridi 2015.

[167] Gillespie 2021.

che interrogativi sulla loro concreta implementabilità su larga scala e sulla compatibilità con gli istituti giuridici esistenti[168]

Sul piano filosofico-giuridico, questa "costruzione socio-digitale" impone di ripensare la soggettività, la responsabilità e la legittimità in un contesto che non segue più le logiche tradizionali della sovranità territoriale. Il potere di emanare regole e di condizionare comportamenti è oggi distribuito tra piattaforme, standard tecnici e comunità d'uso, dando luogo a un pluralismo di fonti normative in cui l'utente rischia di perdere la consapevolezza dei propri diritti e dei doveri[169] . Il compito del giurista (e in modo particolare del filosofo del diritto e dell'esperto di informatica giuridica) – in ossequio a quelle che furono le intuizioni di Cotta e di Borruso – è quello di definire i principi etici e giuridici che dovrebbero ispirare la progettazione di tecnologie e architetture digitali, dall'equità algoritmica alla proporzionalità delle misure di sorveglianza[170].

Le prospettive future di ricerca e di intervento richiedono un approccio interdisciplinare e aperto al dialogo con le scienze sociali, l'ingegneria informatica e l'etica applicata. In primo luogo, appare indispensabile promuovere studi empirici sulle pratiche reali di *governance* digitale, per capire come le varie forme di regolazione – legislative, private, collaborative – interagiscano e quali effetti producano sui diritti e sulle opportunità dei cittadini[171] . In secondo luogo, si rende necessario un confronto internazionale più incisivo, da realizzarsi attraverso accordi e linee guida sovranazionali, capaci di affrontare la complessità di un mercato globale e di piattaforme che sfuggono al controllo territoriale[172] . Infine, la formazione di professionisti e decisori, consapevoli tanto degli aspetti tecnici quanto di quelli etici e giuridici, costituisce un pilastro per la costruzione di una cittadinanza digitale critica e ben informata[173] .

In definitiva, il percorso tracciato da questo contributo – pur concentrandosi in modo specifico sulla tensione tra "*through norms*" e "*beyond norms*" – mira a dimostrare come la regolazione della dimensione socio-digitale non possa più essere relegata su un unico livello di azione, ma richieda un impegno collettivo nel quale Stato, mercato e società civile riconoscano la posta in gioco: la definizione dell'identità, i confini della libertà, la tutela dell'autonomia e la qualità della vita democratica. Coniugare innovazione e giustizia, tecnica e diritto, è la sfida fondamentale del nostro tempo. Si tratta di una

[168] Finck 2018; De Hert, Papakonstantinou 2016.
[169] Lessig 1999.
[170] Eubanks 2019; Yeung 2018.
[171] Tufekci 2018.
[172] Pollicino 2016b.
[173] Rodotà 2007.

sfida in cui la filosofia del diritto si pone in prima linea. Lungi dal rappresentare una disciplina astratta, essa riscopre il proprio ruolo di sapere critico e progettuale, di "bussola" orientata a forgiare nuovi istituti e pratiche capaci di dare forma a un mondo digitale equo, inclusivo e giusto.

Riferimenti bibliografici

Abba, Laura, e Angelo Alù. "Internet Governance Forum: l'evoluzione del modello multi-stakeholder tra criticità e prospettive future." *Rivista italiana di informatica e diritto* 2 (1): 79-86.

Amato Mangiameli, Agata C. 2000. *Diritto e Cyberspace*. Giappichelli.

Amato Mangiameli, Agata C. 2004. *Stati Post-moderni e diritto dei popoli*. Giappichelli.

Amato Mangiameli, Agata C. 2015. *Informatica giuridica*. Giappichelli.

Amato Mangiameli, Agata C. 2017. "Tecno-regolazione e diritto. Brevi note su limiti e differenze." *Diritto dell'informazione e dell'informatica* 2: 147-167.

Amato Mangiameli, Agata C. 2019. "Algoritmi e big data. Dalla carta sulla robotica." *Rivista di Filosofia del diritto* 1: 107-124.

Amato Mangiameli, Agata C., e Campagnoli, Maria Novella. 2020. *Strategie digitali. #diritto_educazione_tecnologie*. Giappichelli.

Bassini, Marco, Laura Liguori, e Oreste Pollicino. "Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?." *Intelligenza artificiale, protezione dei dati personali e regolazione*, F. Pizzetti (a cura di), 333-369. Giappichelli.

Bauman, Zygmunt. 2000. *Liquid Modernity*. Polity Press.

Bauman, Zygmunt. 2010. *La società individualizzata. Come cambia la nostra esperienza*. Il Mulino.

Bauman, Zygmunt, e David Lyon. 2015. *Sesto potere. La sorveglianza nella modernità liquida*. Laterza.

Beck, Susanne. 2016. "Intelligent agents, and criminal law. Negligence, diffusion of liability and electronic personhood." *Robotics and Autonomous Systems* 86 (4): 138-143.

Benanti, Paolo. 2018. *Le macchine sapienti. Intelligenze artificiali e decisioni umane*. Marietti.

Benanti, Paolo. 2020. *Digital age. Teoria del cambio d' epoca. Persona, famiglia e società*. San Paolo.

Benanti, Paolo. 2022. *Human in the loop. Decisioni umane e intelligenze artificiali*. Mondadori.

Benanti, Paolo. 2024. *Noi e la macchina. Un' etica per l'era digitale*. Luiss University Press.

Benasayag, Miguel. 2020. *La tirannia dell'algoritmo*. Vita e Pensiero.

Bentham, Jeremy. 2002. *Panopticon ovvero la casa d'ispezione*. Feltrinelli.

Bianchi, Claudia. 2021. *Hate speech. Il lato oscuro del linguaggio*. Laterza.

Borruso, Roberto. 1990. *L'informatica per il giurista*. Giuffré.

Boyd, Danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.

Calenda, Davide, e Cristina Fonio. 2010. *Sorveglianza e società*. Bonanno.

Campagnoli Maria Novella. 2020. *Informazione, Social Network e Diritto. Dalle fake news all'hate speech online. Risvolti sociologici, profili giuridici, interventi normativi*. Key editore.

Cappellini, Alberto. 2019. "Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale." *Criminalia*, 2018: 499-520.

Cardon, Dominique. 2016. *Cosa sognano gli algoritmi. Le nostre vite ai tempi dei big data*. Mondadori.

Casadei, Thomas, e Andrea Andronico. 2021. "Algoritmi ed esperienza giuridica." *Ars interpretandi* 26 (1).

Castells, Manuel. 2009. *The Rise of the Network Society*. Wiley-Blackwell.

Castells, Manuel. 2013. *Communication Power*. Oxford University Press.

Cialdini, B. Robert. 2022. *Le armi della persuasione. Come e perché si finisce col dire di sì*. Giunti.

Colombo, Fausto. 2013. *Il potere socievole. Storia e critica dei social media*. Mondadori.

Cotta, Sergio. 1968. *La sfida tecnologica*. Il Mulino.

Couldry, Nick, e Ulises A. Mejias. 2019. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

D'Acquisto, Giuseppe. 2022. *Decisioni algoritmiche. Equità, causalità, trasparenza*. Giappichelli.

D'Agostino, Francesco. 2004. "Identità." *Parole di bioetica*, 109-119. Giappichelli.

De Cupis, Adriano. 1949. *Il diritto all' identità personale*. Giuffrè.

De Hert, Paul, e Vagelis Papakonstantinou. 2016. "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" *Computer Law & Security Review* 32 (2): 179-194.

De Pasquale, Patrizia. 2022. "Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?." *Il Diritto Dell'unione Europea*: 1-15.

Desai, R. Deven. 2016. "Exploration and Exploitation. An Essay on (Machine) Learning, Algorithms, and Information Provision." *Loyola University Chicago Law Journal* 47 (2): 541-581.

Di Rosa, Andrea. 2020. *Hate speech e discriminazione. Un'analisi performativa tra diritti umani e teorie di libertà*. Mucchi.

Domingos, Pedro. 2016. *L'algoritmo definitivo. La macchina che impara da sola e il futuro del nostro mondo*. Bollati Boringhieri.

Durkheim, Émile. 1894. *Règles de la méthode sociologique*. Félix Alcan.

Eubanks, Virginia. 2019. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. Picador, St. Martin's Press.

Fabris, Adriano. 2018. *Etica per le tecnologie dell'informazione e della comunicazione*. Carocci.

Ferrari, Franco. 2013. "Forum Shopping: A Plea for a Broad and Value-Neutral Definition." *NYU Lectures on Transnational Litigation, Arbitration and Commercial Law,* Vol. 1, Public Law Research Paper No. 14-39

Finck, Michèle. 2018. *Blockchain Regulation and Governance in Europe*. Cambridge University Press.

Finocchiaro, Giusella. 2024. *Intelligenza artificiale. Quali regole?* Il Mulino.

Floridi, Luciano. 2015. *The Onlife Manifesto: Being Human in a Hyperconnected Era*. Springer.

Floridi, Luciano. 2020a. *Il verde e il blu: Idee ingenue per migliorare la politica*. Raffaello Cortina.

Floridi, Luciano. 2020b. *Pensare l'infosfera: La filosofia come design concettuale*. Raffaello Cortina.

Floridi, Luciano. 2023. *The Ethics of Artificial Intelligence. Principles, Challenges, and Opportunities*. Oxford University Press.

Floridi, Luciano, e Josh Cowls. 2022. "A unified framework of five principles for AI in society." *Machine learning and the city: Applications in architecture and urban design*: 535-545.

Foucault, Michel. 2005. *Discorso e verità nella Grecia antica*. Donzelli

Foucault, Michel. 2014. *Sorvegliare e punire. Nascita della prigione*. Einaudi.

Gillespie, Tarleton. 2021. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

Gometz, Gianmarco. 2023. "E-democracy." *Cento e una voce di Informatica giuridica*, (a cura di) Amato Mangiameli, Agata C., e Guido Saraceni, 196-200. Giappichelli.

Habermas, Jürgen. 2005. *Storia e critica dell'opinione pubblica*. Laterza.

Habermas, Jürgen. 2022. *Teoria dell'agire comunicativo*. Il Mulino.

Hallevy, Gabriel. 2010a. "'I, Robot. I, Criminal' – When Science Fiction Becomes Reality: Legal Liability of AI Robots committing Criminal Offences." *Syracuse Science & Technology Law Reporter* 22: 1-37.

Hallevy, Gabriel. 2010b. "The Criminal Liability of Artificial Intelligence Entities. From Science Fiction to Legal Social Control." *Akron Intellectual Property Journal* 4 (2): 171-201.

Hallevy, Gabriel. 2010c. "Virtual criminal responsibility." *Original Law Review* 6 (1): 6-27.

Hallevy, Gabriel. 2018. "Dangerous Robots. Artificial Intelligence vs. Human Intelligence" *SSRN*: 1-44.

Hargittai, Eszter. 2002. "Second-Level Digital Divide: Differences in People's Online Skills." *First Monday* 7 (4).

Heidegger, Martin. 2017. *La questione della tecnica*. GoWare.

Iaselli, Michele. 2023. "Identità digitale nel Metaverso." *Democrazia e Diritti Sociali* 1: 33-46

Latour, Bruno. 1999. *Pandora's hope. Essays on the reality of science studies*. Harvard University Press.

Latour, Bruno. 2005. *Reassembling the Social. An Introduction to Actor-Network-Theory*. Oxford University Press.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. Basic Books.

Lévy, Pierre. 1990. *Les technologies de l'intelligence. L'avenir de la pensée à l'ère Informatique*. La Découverte.

Lévy, Pierre. 1995. *Qu'est-ce que le virtuel?*. La Découverte.

Lo Monte, Emanuela. 2021. *L'art. 612-ter c.p. Diffusione illecita di immagini o video sessualmente espliciti*. Giappichelli.

Lovink, Geert. 2019. *Nichilismo digitale. L'altra faccia delle piattaforme*. Bocconi.

Lyon, David. 1997. *L'occhio elettronico. Privacy e filosofia della sorveglianza*. Feltrinelli.

Lyon, David. 2002. *La società sorvegliata. Tecnologie di controllo della vita quotidiana*. Feltrinelli.

Mangiameli, Stelio. 2023. "Sovranità digitale." *Cento e una voce di Informatica giuridica*, (a cura di) Amato Mangiameli, Agata C., e Guido Saraceni, 451-460. Giappichelli.

Mayer-Schönberger, Viktor, e Kenneth Cukier. 2013. *Big data. Una rivoluzione che trasformerà il nostro modo di vivere – e già minaccia la nostra libertà*. Garzanti.

Mill, J. Stuart. 1879. *On Liberty and The Subjection of Women*. Henry Holt and Co.

Morondo Taramundi, Dolores. 2022. *Le sfide della discriminazione algoritmica*. In *GenIus* 1: 1-13.

Moro, Paolo, e Carlo Sarra. 2017. *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*. Franco Angeli.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Norris, Pippa, e Ronald Inglehart. 2019. *Cultural Backlash: Trump, Brexit, and Authoritarian Populism*. Cambridge University Press.

Orwel, George. 1949. *Nineteen Eighty-Four*. Secker & Warburg.

Pagallo, Ugo. 2018. "Vital, Sophia, and Co.–The Quest for the Legal Personhood of Robots." *Information* 9 (9): 230.

Paladino, Alessandra. 2020. *Revenge porn e cyberbullismo*. Alpes.

Pariser, Eli. 2012. *The filter bubble: what the internet is hiding from you*. Penguin Books.

Pascuzzi, Giovanni. 2020. *Il diritto dell'era digitale*. Il Mulino.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

Perri, Paolo. 2020. *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*. Giuffrè.

Pirandello, Luigi. 2014. *Uno, Nessuno, Centomila*. Einaudi.

Pitruzzella, Giovanni, e Oreste Pollicino. 2020. *Disinformation and hate speech. A European Constitutional*. Bocconi University Press.

Pollicino, Oreste, Valerio Lubello, e Marco Bassini. 2016a. *Identità ed eredità digitali*. Aracne.

Pollicino, Oreste. 2016b. *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe*. Routledge.

Pollicino, Oreste. 2023a. Voce "Potere digitale." *Enciclopedia del diritto: i tematici*. Giuffrè: 410-446.

Pollicino, Oreste. 2023b. "The quadrangular shape of the geometry of digital power (s) and the move towards a procedural digital constitutionalism." *European Law Journal* 29 (1-2): 10-30.

Pollicino, Oreste, e Paul Dunn. 2024. *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*. Bocconi University Press.

Riva, Giuseppe, e Andrea Gaggioli. 2019. *Realtà virtuali: Gli aspetti psicologici delle tecnologie simulative e il loro impatto sull'esperienza umana*. Giunti.

Riva, Giuseppe. 2016. *Selfie. Narcisismo e identità*. Il Mulino.

Riva, Giuseppe. 2025. *Io, noi, loro. Le relazioni nell'era dei social e dell'IA*. Il Mulino.

Rodotà, Stefano. 2007. *La vita e le regole: Tra diritto e non diritto*. Feltrinelli.

Simoncini, Andrea. 2021. "Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di Stato e forma di Governo." *Osservatorio sulle fonti* 2: 723-732.

Stilgoe, Jack. 2018. "Machine learning, social learning and the governance of self-driving cars." *Social Studies of Science* 48 (1): 25-56.

Stolfi, Nicola. 1905. *I segni di distinzione personali*. Salvatore Romano.

Strasser, Anna. 2022 "Distributed responsibility in human–machine interactions". AI & Ethics, vol. 2: 523-532.

Surden, Harry. 2014. "Machine Learning and Law." *Washington Law Review* 89 (1): 87-115.

Tallia, Domenico. 2018. *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*. Rubettino.

Teubner, Gunther. 2006. "Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law." *Journal of Law and Society* 33 (4): 497-521.

Thaler, Richard H., e Cass R. Sunstein. 2009. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Penguin Books.

Tiribelli, Stefano. 2023. *Identità personale e algoritmi. Una questione di filosofia morale*. Carocci.

Tommasi, Sara. 2020. "Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo." *Revista de Direito Brasileira* 27 (10): 112-129.

Tufekci, Zeynep. 2018. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

Turkle, Sherry. 1995. *Life on the Screen: Identity in the Age of the Internet*. Simon & Schuster.

Turkle, Sherry. 2012. *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books.

Vespignani, Alessandro. 2019. *L'algoritmo e l'oracolo: Come la scienza predice il futuro e ci aiuta a cambiarlo*. Il Saggiatore.

Virilio, Paul. 1998. *La bombe informatique*. Editions Galilée.

Yeung, Karen. 2018. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12 (4): 505-523.

Woolley, Samuel C. e Guilbeault, Douglas R. 2017. *Computational Propaganda in the United States of America: Manufacturing Consensus Online*. Working Paper No. 2017.5. Oxford Internet Institute.

Ziccardi, Giovanni. 2016. *L'odio online. Violenza verbale e ossessioni in rete*. Raffaello Cortina.

Ziccardi, Giovanni. 2017. *Il libro digitale dei morti. Memoria, lutto, eternità e oblio nell'era dei social network*. Utet.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.