Norme e codici. La regolazione digitale tra architetture tecniche e soggettività fragili

Rules and Codes: Digital Regulation Between Technical Architectures and Vulnerable Subjectivities

Enrico Maestri[1], Giorgio Manfré[2]

Sommario[33]

Il saggio analizza, da una prospettiva sociologico-giuridica, la trasformazione della normatività nella società digitale, assumendo il codice informatico come vettore primario di regolazione sociale. L'indagine si colloca nel solco del *code-based approach* sviluppato da Lawrence Lessig, riformulandone criticamente i presupposti attraverso l'apporto della teoria dei sistemi di Niklas Luhmann e della teoria degli agenti *software* di Gunther Teubner, con particolare attenzione ai concetti di autopoiesi normativa, collisione tra razionalità parziali e attanti tecnici non umani.

Viene proposta una tassonomia dei modelli di regolazione tecno-digitale – *Lex Informatica, Lex Algorithmica, Lex ex Machina, Lex Cryptographica* – ed esaminate le ricadute normative di tale trasformazione, interrogando l'efficacia delle recenti risposte legislative europee (GDPR, DSA, DMA, AI Act), interpretate come tentativi di riappropriazione giuridica dello spazio digitale.

Nella parte conclusiva, l'attenzione si sposta verso il profilo soggettivo di *Code is Law*, concentrandosi sulla figura del minore, intesa come soggettività fragile, computazionalmente costruita e normata da dispositivi performativi. Il minore, in quanto *attante* esposto e *punto funzionale* di una normatività opaca, rappresenta dunque oggi il luogo critico in cui si misura la tenuta del diritto come istituzione capace di nominare, proteggere e riconoscere la persona.

---

1 Dipartimento di Giurisprudenza, Università degli Studi di Ferrara. enrico.maestri@unife.it

2 Dipartimento di Studi Umanistici, Università degli Studi di Urbino. giorgio.manfre@uniurb.it

3 [3] Ai soli fini dell'attribuzione formale della paternità scientifica, si precisa che i paragrafi 1, 2, 3 e 4 sono attribuibili a Enrico Maestri, mentre i paragrafi 5 e 6 a Giorgio Manfré. La suddivisione, tuttavia, non corrisponde alla reale dinamica di elaborazione del contributo, che è frutto di un confronto condiviso su contenuti, struttura e finalità teoriche. Il saggio va dunque considerato come esito unitario di una collaborazione sostanziale.

Data invio: 1 luglio 2025. Data accettazione: 26 agosto 2025.
DOI: https://doi.org/10.54103/1972-5760/30048

L'obiettivo è descrivere l'efficacia conformativa degli ambienti digitali nella formazione dell'identità minorile e nella riconfigurazione della tutela giuridica.

Parole chiave: normatività digitale; regolazione algoritmica; lex algorithmica; soggettività computazionale; minori vulnerabili negli ambienti digitali

Abstract

This essay examines, from a socio-legal perspective, the transformation of normativity in the digital society, considering computer code as the primary vector of social regulation. The analysis builds on the *code-based approach* developed by Lawrence Lessig, while critically reformulating its assumptions through the contributions of Niklas Luhmann's systems theory and Gunther Teubner's theory of software agents, with a particular focus on the concepts of normative autopoiesis, collision of partial rationalities, and non-human technical actants.

A taxonomy of techno-digital regulatory models— *Lex Informatica*, *Lex Algorithmica*, *Lex ex Machina*, and *Lex Cryptographica* — is proposed, and the normative implications of this transformation are explored, assessing the effectiveness of recent European legislative solutions (GDPR, DSA, DMA, AI Act) as attempts to reclaim legal authority within the digital space.

In the concluding section, the focus shifts to the subjective dimension of *Code is Law*, centering on the figure of the minor as a vulnerable subjectivity, computationally constructed and regulated by performative digital devices. The minor, as an exposed actant and functional node within an opaque normative system, emerges as the critical site for assessing the resilience of law as an institution capable of naming, protecting, and recognizing the person.

The aim is to describe the conformative power of digital environments in shaping minor's identity and in the reconfiguring legal protection.

Keywords: Digital normativity; Algorithmic regulation; Lex Algorithmica; Computational subjectivity; Vulnerable minors in digital environments

1. Introduzione

L'idea di norma, nel contesto dell'ambiente digitale, ha subito una trasformazione profonda che mette in discussione le categorie fondative del diritto e della teoria della normatività. Se, in origine, Internet fu concepito come uno spazio di libertà spontanea, anarchico e deterritorializzato (Johnson, Post 1996), in cui le regole emergevano da pratiche comunitarie e dinamiche cooperative (Rheingold 1993), l'evoluzione delle piattaforme, degli

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

algoritmi e delle infrastrutture digitali ha progressivamente reso evidente la presenza di forme di regolazione non giuridiche, ma efficacemente vincolanti, capaci di orientare e limitare i comportamenti in modo diretto e sistematico (Reidenberg 1998).

Questa transizione richiede una distinzione concettuale preliminare tra norme giuridiche – espressione di una volontà normativa formalizzata e riconosciuta da un ordinamento – e codici tecnici, intesi come regole operative scritte in linguaggio informatico, che strutturano *ex ante* le possibilità d'azione nello spazio digitale (Brownsword 2008; Yeung 2017b; De Filippi, Hassan 2016).

L'affermazione di Lawrence Lessig (1999), secondo cui "Code is Law", segna un punto di svolta teorico nella comprensione della normatività digitale (Goldoni 2015), pur essendo stata a lungo criticata da parte della dottrina giuridica tradizionale, talvolta ridotta al paradigma del cosiddetto "diritto del cavallo" (Easterbrook 1996)[4].

Il codice informatico agisce come dispositivo performativo: non si limita a prescrivere comportamenti, ma costruisce i contesti e i valori entro i quali tali comportamenti diventano possibili o impossibili. In questo senso, il codice si presenta non solo come linguaggio tecnico, ma come vero e proprio ambiente digitale, dotato di efficacia vincolante indipendente da processi di deliberazione giuridica.

Con l'introduzione degli algoritmi e dell'intelligenza artificiale, il paradigma "Code is Law" non solo si conferma, ma si intensifica, adattandosi modularmente alle nuove forme di normatività algoritmica. Come osserva Håkan Hydén (2020), il problema non è più tanto quello di disciplinare la nuova tecnologia, quanto quello di comprendere in che modo la tecnologia, attraverso le proprie regole implicite, assuma progressivamente il controllo dei processi regolativi.

Un approccio sociologico-giuridico consente, a questo punto, di spostare l'attenzione dalla forma alla funzione della regola (Ferrari 1992): ciò che rileva non è tanto la fonte della norma, quanto l'efficacia regolativa che essa esercita sui comportamenti sociali, siano essi veicolati da dispositivi giuridici o tecnici. Seguendo la lezione di Niklas Luhmann (1982), se si considera il

4 Fatte salve alcune eccezioni di rilievo (si vedano, tra gli altri, Finocchiaro 2008; Goldoni 2007; Ziccardi 2006; Colomba 2005; Rossato 2006), la dottrina giuridica italiana ha a lungo trascurato — quando non liquidato con superficialità — il paradigma "Code is Law" proposto da Lawrence Lessig. Spesso ridotta a una visione ingenua o confutata tramite argomentazioni di stampo essenzialista (del tipo: "è sempre l'essere umano a decidere in ultima istanza", senza cogliere che l'architettura può esercitare un vincolo anche in assenza di soggettività), tale impostazione è rimasta ai margini del dibattito teorico-giuridico per almeno due decenni. Solo recentemente, anche grazie alla ricezione di riflessioni come quelle di Antoine Garapon (2021), si è iniziato a riconoscere l'elevato potenziale euristico della proposta lessighiana, in particolare per comprendere le trasformazioni normative indotte dalla regolazione algoritmica.

diritto come un sistema funzionalmente differenziato, che produce norme attraverso operazioni comunicative codificate secondo il codice binario lecito/illecito, allora anche la tecnologia digitale può essere ricondotta a una logica analoga. Essa si fonda sull'opposizione binaria "0/1", classificando ogni fenomeno all'interno di una struttura dicotomica. In questo modo, diventa possibile catturare ogni aspetto del mondo, riducendolo alle sue proprietà misurabili e traducendolo in dati digitali (Accoto 2017). Pur non esplicitandolo pienamente, Nassehi (2024) suggerisce che la digitalizzazione costituisce una prospettiva di riduzione tecnica, che raddoppia il mondo in forma di dato. Essa funziona in maniera analoga ai codici dei sistemi funzionali: opera una riduzione binaria a partire dalla quale si possono costruire modelli regolativi di elevata complessità. Con la digitalizzazione, dunque, oltre alle riduzioni sistemiche, il mondo sperimenta un'ulteriore duplicazione sotto forma di rappresentazione informazionale.

I sistemi di moderazione algoritmica, ad esempio, non si limitano a eseguire istruzioni: essi configurano le possibilità d'azione degli individui, stabilendo ciò che è permesso, proibito o obbligatorio all'interno del sistema tecnologico. Questa capacità normativa trasforma la tecnologia in un attore regolativo autonomo, inserito in reti di comunicazione e regolazione sociale.

La digitalità, infatti, genera nuovi sistemi regolativi: i codici, concepiti originariamente come strumenti autoesecutivi (Lessig 1999), tendono a configurarsi oggi come pseudo-soggetti normativi autonomi – o *attanti*, secondo la terminologia di Teubner – fondati su architetture diverse, capaci di produrre forme di normatività alternative. Gunther Teubner (2015) ha individuato in tali dispositivi (algoritmi, architetture digitali, sistemi di automazione) una nuova forma di *agentività normativa*, capace di esercitare effetti regolativi efficaci al di fuori dei circuiti della deliberazione giuridica.

L'ambiente digitale si configura, in tal modo, come un campo normativo ibrido e asimmetrico attraversato da un pluralismo regolativo de facto in cui coesistono norme statuali e sovranazionali, regole di piattaforma, automatismi computazionali, standard tecnici e dispositivi di governance privata. In questo contesto, il diritto non solo perde centralità simbolica e strutturale, ma si confronta con una forma inedita di normatività ambientale, diffusa, impersonale e distribuita (Bayamlıoğlu, Leenes 2018).

In tale configurazione, "Code is Law" non si limita più a esprimere una metafora euristica della normatività digitale, ma si struttura come principio modulare di riconfigurazione sistemica della regolazione, articolandosi in modalità eterogenee – infrastrutturali, algoritmiche, adattive – capaci di assorbire e riformulare le funzioni normative tradizionali all'interno di un ambiente computazionale performativo e distribuito.

L'obiettivo sociologico-giuridico del saggio è quello di esplorare le forme contemporanee della regolazione digitale, distinguendo tra differenti modelli normativi – *Lex Informatica, Lex Algorithmica, Lex ex Machina, Lex*

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

Cryptographica – e esaminata le ricadute normative di tale trasformazione, interrogando l'efficacia delle recenti risposte legislative europee (GDPR, DSA, DMA, AI Act), interpretate come tentativi di riappropriazione giuridica dello spazio digitale.

I casi di studio – dai sistemi DRM (*Digital Rights Management*) alla moderazione algoritmica, dagli *smart contracts* alle clausole deregolative e responsabilizzanti del Digital Services Act, dell'AI Act e del GDPR – illustrano come la tecnica non si limiti a integrare il diritto convenzionale, ma in alcuni ambiti lo superi, contribuendo alla produzione di una normatività tecnologica autonoma.

Nella parte conclusiva, l'attenzione si sposta verso il profilo soggettivo di "Code is Law", concentrandosi sulla figura del minore, intesa come soggettività fragile, computazionalmente costruita e normata da dispositivi performativi. Il minore, in quanto *attante* esposto e *punto funzionale* di una normatività opaca, rappresenta dunque oggi il luogo critico in cui si misura la tenuta del diritto come istituzione capace di nominare, proteggere e riconoscere la persona.

Lo scopo è quello di descrivere l'efficacia conformativa degli ambienti digitali nella formazione dell'identità minorile e nella riconfigurazione della tutela giuridica.

2. Il "code" come fonte normativa prevalente nello spazio digitale

L'emergere di uno spazio digitale come nuovo ambiente di interazione sociale ha imposto una riconsiderazione radicale delle fonti della normatività. In questo contesto, la formula "Code is Law", coniata da Lawrence Lessig, non rappresenta solo una provocazione teorica, ma una diagnosi strutturale: il codice informatico – inteso come insieme di architetture software e hardware – ha assunto una funzione regolativa analoga a quella della legge. Il diritto, tradizionalmente ancorato alla scrittura, alla deliberazione e all'interpretazione, si trova oggi affiancato, e talvolta surclassato, da regole auto-eseguibili e auto-applicative (Hildebrandt, 2020, p. 68).

La crescente affermazione delle tecnologie digitali come dispositivi regolativi autonomi evidenzia una profonda asimmetria tra regole tecniche e norme giuridiche. Tale disallineamento non è soltanto concettuale o simbolico, ma produce effetti tangibili sul piano della regolazione sociale, giuridica ed economica. Come ha osservato Roger Brownsword (2005, 2019), ci troviamo di fronte a una forma di "tecnodiritto", ovvero un ordine normativo in cui la forza vincolante delle regole non deriva più dall'autorità statale o dalla legittimazione procedurale, ma dall'efficacia computazionale delle soluzioni incorporate nei sistemi digitali.

A differenza delle norme deontiche, che prescrivono comportamenti lasciando margini di discrezionalità e possibilità di disobbedienza, le regole tecniche si attuano automaticamente. Come osservava Niklas Luhmann (1983, p. 7), mentre le norme giuridiche proteggono gli attori da condotte deviate, le regole tecniche costringono direttamente alla conformità.

Questo scenario produce un'inversione nel rapporto tra tecnica e diritto: in molte aree della regolazione digitale – dalla protezione dei dati alla gestione dei contenuti, dalla cybersicurezza alla proprietà intellettuale – non è più la legge a "domare" la tecnica, ma la tecnica a dettare i comportamenti conformi nello spazio digitale. Le architetture regolative digitali, fondate su protocolli tecnici e logiche computazionali, modellano il comportamento senza passare per le categorie della normatività tradizionale, spostando il baricentro della regolazione dallo spazio deliberativo a quello ingegneristico.

Nonostante l'espressione "Code is Law" sia divenuta una formula iconica della regolazione tecnologica, Lessig non ha mai inteso attribuire al codice lo statuto di fonte normativa in senso proprio. Come da lui stesso chiarito (2006, p. 5), il codice è "legge" solo in senso funzionale: una modalità architettonica di regolazione che, pur producendo effetti vincolanti, resta distinta dal diritto positivo. Leenes (2011, p. 145) sottolinea correttamente che Lessig non utilizza l'espressione in senso letterale, ma descrittivo. De Filippi (2018) evidenzia come tale formula sia stata frequentemente equivocata, trasformandosi in un'asserzione normativa anziché rimanere un'analisi delle capacità regolative del codice.

Analogamente, la *Lex Informatica* di Reidenberg (1998) – da cui Lessig deriva parte del proprio impianto concettuale – non è configurata come diritto, ma come dispositivo extragiuridico con funzione regolativa. Reidenberg parla esplicitamente di un sistema parallelo, dotato di proprietà analoghe a quelle della legge, ma distinto dalla regolazione giuridica convenzionale. In entrambi i casi, la dimensione normativa del codice viene affermata sul piano dell'efficacia sociale, non della validità giuridica.

Lessig distingue quattro modalità di regolazione: la legge, le norme sociali, il mercato e l'architettura. Di tutte, è quest'ultima a operare nel modo più cogente e meno contestabile, proprio perché non richiede l'intervento dell'interpretazione né la mediazione della coscienza soggettiva.

In questo senso, la normatività del codice è autonoma rispetto all'ermeneutica e all'intenzionalità soggettiva: vincola anche chi non sa di essere vincolato. Il codice, scrivibile, modificabile, auto-eseguibile, può diventare un sistema normativo che non ha bisogno di essere "obbedito", perché è già "in esecuzione". Lessig introduce così una differenza cruciale tra vincoli oggettivi (quelli che agiscono nella realtà esterna) e vincoli soggettivi (quelli interiorizzati e anticipati dal soggetto). Solo i secondi richiedono una forma di apprendimento, di consapevolezza o intenzionalità; i primi, come nel caso dell'architettura, si impongono indipendentemente dalla conoscenza

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

che ne ha il soggetto. La libertà, in questa visione, non è il vuoto di vincoli, ma l'effetto di una specifica composizione architettonica degli stessi. Come afferma Lessig, "la libertà è costruita", plasmata da strutture e da piattaforme che, seppur invisibili, generano ciò che può o non può essere fatto (Zittrain 2008).

Questa forma di regolazione "by code" raggiunge la sua massima espressione nei modelli "by design", tipici della normativa europea vigente (GDPR, AI ACT, DSA, DMA)[5]: *privacy by design*, *security by design*, *transparency by design*, *ethics by design* (Pascuzzi 2020). Qui, la norma giuridica non è più un enunciato deliberativo, ma una funzionalità inglobata nell'architettura tecnica.

In questo scenario, la distinzione classica tra fonte normativa e dispositivo esecutivo si dissolve. Il risultato è un nuovo regime di regolazione in cui la tecnica diventa il vettore primario della normatività, e il diritto è chiamato a ridefinire il proprio ruolo, non più come monopolio della regola, ma come co-autore di un ambiente normativo ibrido.

Uno degli aspetti più innovativi del pensiero di Lessig è la consapevolezza che la regolazione si distribuisce su diversi livelli dell'ecosistema digitale. Il codice informatico, come forma di architettura, possiede una forza vincolante che agisce direttamente sull'ambiente d'azione degli utenti. Ma questa capacità regolativa non si limita al livello del software: essa si articola in un modello multilivello, nel quale la regolazione più efficace non discende dall'alto, bensì dal basso.

Nel suo fondamentale contributo *The Wealth of Networks*, Yochai Benkler (2006) ha mostrato come l'ambiente digitale sia strutturato in quattro livelli: l'infrastruttura fisica (hardware e cavi), l'infrastruttura logica (protocolli e sistemi operativi), il livello dei contenuti (informazioni e dati) e quello delle regole (norme giuridiche e politiche pubbliche). In questa architettura, l'efficacia della regolazione è inversamente proporzionale all'altezza del livello: quanto più si interviene a livello inferiore, tanto maggiore è l'impatto sui livelli superiori. Una norma giuridica che incide sul livello dei contenuti può essere facilmente elusa o reinterpretata, mentre un vincolo tecnico introdotto a livello di protocollo di rete determina in modo strutturale ciò che è possibile o impossibile fare (Lessig 2006).

I sistemi DRM (*Digital Rights Management*), ad esempio, incorporati nel codice dei software, cancellano di fatto il principio del *fair use*, bloccando *ex ante* ogni utilizzo del contenuto digitale. Qui il codice non si limita a implementare la norma: la sostituisce. È il dispositivo tecnico che produce la normatività effettiva, agendo prima, e in modo più vincolante, della norma giuridica.

5 General Data Protection Regulation (GDPR), Regolamento UE sull'intelligenza artificiale (AI ACT), Digital Services Act (DSA), Digital Markets Act (DMA).

In questa prospettiva, si evidenzia un profondo dislivello regolativo tra regole tecniche e norme giuridiche. Come ha mostrato Brownsword (2005, pp. 49-65), la "practical effectiveness" delle prime – la loro capacità di impedire e non solo di costringere – si impone su quella delle seconde, fondate sulla defettibilità (Sartor 2005) e sulla deliberazione.

Il diritto resta significativo solo se riesce a intervenire sui livelli tecnici, integrandosi con essi o contrastandoli attraverso strategie di design normativo (Koops, Leenes 2014). La "regolazione by design" è una risposta a questa trasformazione, ma è anche una conferma della perdita di centralità del diritto discorsivo.

Il concetto di tecno-regolazione (Lettieri 2020), dunque, non designa soltanto una nuova tecnica regolativa, ma segnala una ristrutturazione delle gerarchie normative. Il diritto, se non riesce a confrontarsi con questa trasformazione, rischia di essere ridotto a livello di "glossa marginale" rispetto al dispositivo tecnico, cioè a mero commento di ciò che è già stato programmato.

Da un punto di vista sociologico-giuridico, questa visione trova solide basi nella teoria dei sistemi sociali di Niklas Luhmann (1990), per il quale il diritto costituisce un sistema funzionalmente differenziato che opera attraverso codici binari (lecito/illecito), costruendo aspettative normative contro-fattuali in grado di ridurre la complessità sociale. L'analogia con il funzionamento delle tecnologie digitali risulta evidente: anche il codice informatico funziona come sistema codificato, che riduce la complessità delle situazioni sociali traducendole in operazioni computabili. La distinzione binaria (0/1) diventa così una forma di descrizione orientativa (Nassehi 2024), analoga a quelle proprie del diritto (lecito/illecito), dell'economia (utile/non utile) o della scienza (vero/falso).

In questo contesto, il concetto teubneriano di *attanti normativi non umani* risulta particolarmente fecondo. Gunther Teubner (2006) ha mostrato come la capacità regolativa non sia prerogativa esclusiva degli attori umani o delle istituzioni giuridiche, ma possa essere attribuita anche a entità tecniche – come algoritmi o infrastrutture digitali – che, in quanto *attanti*, ovvero agenti non umani dotati di effetti normativi, partecipano attivamente ai processi comunicativi di regolazione sociale.

Questa trasformazione richiama l'idea di Bruno Latour (2005) secondo cui gli artefatti tecnologici sono "actants", attori dotati di capacità regolativa, che orientano i comportamenti attraverso la materialità delle loro funzioni. Il "by design" non è una mera strategia di implementazione tecnica: è una modalità di codifica normativa che agisce a monte della deliberazione, riducendo la discrezionalità, eliminando l'ambiguità e rendendo impossibile la violazione. L'utente non è più soggetto responsabile, ma terminale operativo in un ambiente regolativo chiuso (Luhmann 1983).

La crescente pervasività del codice informatico nella regolazione dei comportamenti digitali – e la sua capacità di anticipare, prevenire o addirittura

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

impedire certe azioni – rende evidente che non ci troviamo più di fronte a una mera infrastruttura tecnica, ma a un nuovo paradigma normativo.

Gli algoritmi contemporanei non si fondano su causalità, ma su correlazioni statistiche, *pattern recognition* e inferenze probabilistiche. Non mirano tanto a spiegare o a giustificare la norma, ma a prevedere e ottimizzare comportamenti (Ferrari 2021).

In questo senso, non siamo più nell'ambito della razionalità idealtipica weberiana, ma in quello della razionalità funzionale sistemica, come l'ha elaborata Luhmann: autoreferenziale, osservazionale, *black-boxed* e orientata alla riduzione della complessità secondo codici binari di decisione.

In definitiva, più che una prosecuzione della razionalità legale-burocratica weberiana (Catanzariti 2021), il paradigma "Code is Law" rappresenta a nostro avviso la sua *desemantizzazione funzionale*, secondo un modello cibernetico e autoreferenziale di selezione delle decisioni: ciò che Luhmann chiamerebbe "decisioni senza decisori" (*Entscheidungen ohne Entscheidungsträger*).

Questo mutamento non è neutro nei confronti delle teorie giuridiche tradizionali. Se la legge era riuscita storicamente a istituzionalizzare la propria autonomia attraverso la mediazione testuale, l'incorporazione automatica delle regole nel software apre uno scenario inedito: la chiusura anticipata del senso e la soppressione della discrezionalità giuridica (Karavas 2009). A questo punto, la questione non è più se il codice sia diritto, ma se il diritto possa ancora differenziarsi in un contesto in cui il medium digitale struttura il significato prima ancora che la comunicazione abbia luogo ("*Code instead of Law*").

3. Lessig dopo Lessig: modelli normativi digitali tra Lex Informatica, Lex Algorithmica, Lex ex Machina e Lex Cryptographica

La trasformazione della normatività nella società digitale non si esaurisce nel confronto tra diritto e codice, né si riduce alla mera dialettica tra regole giuridiche e regole tecniche. È ormai necessario adottare una mappa più articolata dei modelli regolativi emergenti, capace di descrivere non solo le fonti della normatività, ma anche le forme e i processi della sua produzione.

Mentre il diritto statuale fonda la propria legittimità su categorie moderne – soggetto, volontà, responsabilità – viceversa la normatività tecnica opera secondo regole binarie, automatiche e insindacabili, prive di margini interpretativi o eccezioni. Le tecnologie digitali definiscono l'ambiente stesso dell'agire, secondo una logica ambientale e non più strumentale (Mann 2024). In tale quadro, la soggettività giuridica tende a dissolversi in una funzione sistemica, e la regolazione giuridica tradizionale mostra una crescente inefficacia di fronte alla chiusura operativa dei sistemi computazionali.

È all'interno di questa cornice teorica che si collocano le principali configurazioni della normatività digitale. A partire dalla genealogia aperta da Reidenberg con la *Lex Informatica* (1998) e sistematizzata da Lessig (1999) con il paradigma architetturale di "Code is Law", si possono individuare almeno cinque modelli paradigmatici: *Lex Informatica*, *Code is Law*, *Lex Algorithmica*, *Lex ex Machina* e *Lex Cryptographica*. Ciascuno di questi modelli articola in modo specifico la normazione tecnica e sociale, secondo una propria configurazione epistemica, una forma di vincolo e un grado di trasparenza operativa.

3.1 Lex Informatica: la regolazione come co-progettazione

Un utile punto di partenza per analizzare i modelli paradigmatici della normatività digitale ci è offerto da Rolf H. Weber (2002), che ha sistematizzato – sebbene non in modo esaustivo – alcune delle principali teorie normative emerse nella governance di Internet. Tra queste, la *Lex Informatica*, concetto introdotto da Joel Reidenberg (1998), rappresenta uno dei primi tentativi di descrivere l'emergere di una regolazione tecnica nel cyberspazio.

Ispirandosi alla *lex mercatoria*, Reidenberg propone l'idea di un sistema parallelo di regole – sviluppato attraverso l'architettura dei network e delle tecnologie informatiche – che governa i flussi informativi e influenza direttamente i comportamenti degli utenti. La *Lex Informatica* si configura quindi come una forma di normatività "by design", nella quale le policy sono implementate tecnicamente all'interno dei protocolli e degli standard tecnologici (Maestri 2015).

Tuttavia, questo modello mantiene ancora un'apertura alla grammatica giuridica tradizionale. L'approccio è integrazionista: il diritto può "programmare i programmatori", imponendo vincoli normativi agli standard tecnici. Le regole tecniche possono essere progettate in collaborazione tra soggetti pubblici e privati, in un contesto di co-regolazione. La *Lex Informatica* si presenta così come un paradigma co-regolativo, dove il codice è riconosciuto come strumento normativo, ma rimane permeabile alla partecipazione politica, alla trasparenza procedurale e alla negoziazione istituzionale.

Secondo Weber (2002), la *Lex Informatica* può essere considerata un "sistema parallelo di regole", in grado di produrre soluzioni regolative analoghe a quelle offerte dal diritto. Questo sistema si struttura intorno a due tipologie di regole sostanziali: da un lato, *policy immutabili*, codificate in standard tecnici rigidi; dall'altro, *policy flessibili*, incorporate in architetture adattabili. La principale debolezza di questo modello – osserva Weber (2002) – risiede però nella minore prevedibilità delle relazioni tra soggetti, nonché nella fragile legittimazione democratica degli attori che progettano le soluzioni tecniche.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

Un esempio emblematico della *Lex Informatica* è rappresentato dagli standard di protocollo come TCP/IP, che regolano la comunicazione digitale globale attraverso specifiche tecniche condivise, indipendenti dalla giurisdizione statale. Analogamente, le specifiche del *World Wide Web Consortium* (W3C) stabiliscono regole vincolanti per la struttura e l'accessibilità dei contenuti online, non attraverso norme giuridiche, ma tramite processi cooperativi di definizione tecnica, che costituiscono una forma di normatività incorporata nell'architettura stessa del web.

Un terzo esempio emblematico è rappresentato da ICANN, l'organizzazione che gestisce l'assegnazione dei nomi di dominio e degli indirizzi IP a livello globale. Le sue decisioni, apparentemente tecniche, definiscono concretamente le condizioni di esistenza semantica e accessibilità nello spazio digitale. ICANN incarna così una forma di normatività architettonica tipica della *Lex Informatica*, esercitata al di fuori dei canali giuridici tradizionali ma con effetti giuridicamente rilevanti.

3.2 Code is Law: il potere regolatorio del codice

Questa fase inaugura la normatività computazionale: il codice non si limita a eseguire funzioni, ma struttura direttamente ambienti e comportamenti. Si tratta di una normatività non giuridificata, priva di procedura, formalizzazione o giustificazione. Il "*code*" agisce, ma non argomenta (*agere sine intelligere*): è una macchina sintattica (Cabitza, Floridi 2021), priva di semantica e di pragmatica, che impone comportamenti senza produrre senso.

L'efficacia regolativa si sposta dal diritto al software, dalla prescrizione alla programmazione. Come sottolinea Lessig, questo spostamento può condurre a un mondo in cui il potere normativo effettivo "displaces law" e si trasferisce interamente al codice, producendo una condizione di normatività post-giuridica (Zaccaria, 2022).

Rolf H. Weber (2018), nel commentare criticamente tale approccio, evidenzia alcune implicazioni problematiche. In primo luogo, la normatività del codice non garantisce una sufficiente conformità ai valori giuridici fondamentali, come i diritti individuali o la trasparenza democratica. La logica algoritmica tende, infatti, a sostituire la mediazione deliberativa del diritto con un determinismo tecnologico, in cui le decisioni normative sono prese da chi progetta il software, spesso in assenza di controllo pubblico o accountability istituzionale.

In secondo luogo, la perfettibilità del controllo computazionale è solo teorica: ogni codice può essere potenzialmente aggirato da un altro codice, e ciò rende illusoria l'idea di un dominio totale del comportamento digitale. Infine, Weber (2018) osserva che l'identificazione piena tra diritto e codice – come nel caso degli *smart contract* – può esporre l'intero sistema giuridico

a forme di abuso, soprattutto quando il "code" viene disegnato senza vincoli normativi esterni o senza una cornice etico-giuridica di riferimento.

Già in *Code 2.0*, Lessig stesso (2006) riconosceva i rischi di una regolazione completamente demandata al software: se ogni soggetto può liberamente programmare regole vincolanti in forma di codice, allora il diritto rischia di essere svuotato nella sua funzione garantista e trasformato in un meccanismo automatico privo di interpretazione, discrezionalità e giustificazione.

Il paradigma "Code is Law" rimane dunque centrale per comprendere la trasformazione epistemologica della normatività digitale: da strumento giuridico a forma architettonica dell'azione. Come osserva Garapon (2021, p. 28), "tutto (o quasi) era già contenuto in questa formula", che anticipa il passaggio della norma scritta al design regolativo incorporato nelle infrastrutture.

L'applicazione più chiara del principio "Code is Law" si osserva nei *Digital Rights Management* (DRM), sistemi progettati per limitare automaticamente l'uso dei contenuti digitali, impedendo copie, condivisioni o modifiche, indipendentemente da quanto previsto dalle norme sul diritto d'autore. Il DRM incarna la transizione dal diritto come dispositivo normativo simbolico al codice come struttura autoesecutiva della regola. Il DRM, pertanto, è un laboratorio paradigmatico per comprendere la trasformazione del diritto in ambiente digitale: non solo un mezzo di *enforcement*, ma un costrutto normativo primario, capace di ridefinire ciò che è lecito e illecito attraverso il design tecnologico.

3.3 Lex Algorithmica: la regolazione automatizzata e adattiva

Per *Lex Algorithmica* intendiamo l'insieme delle regole computazionali auto-esecutive, incorporate in sistemi algoritmici, che operano come norme tecniche a efficacia giuridica, riconosciute, accettate o co-progettate dal diritto positivo tradizionale. La *Lex Algorithmica* rappresenta una fase cruciale nell'evoluzione della normatività digitale, in cui il diritto si ibrida con l'intelligenza artificiale e i modelli predittivi, dando origine a una regolazione automatizzata, adattiva e personalizzata. A differenza della fase *Code is Law*, in cui il codice agiva come architettura ambientale normativa, qui l'algoritmo non solo struttura i comportamenti ma produce esso stesso le regole attraverso l'apprendimento dai dati. Come osserva Karen Yeung (2017b), le norme non sono più scritte ex ante da esseri umani, ma vengono apprese, adattate e ottimizzate in modo continuo da sistemi di *machine learning*, dando luogo a una regolazione opaca e difficilmente contestabile, che riduce sensibilmente le possibilità di *accountability* democratica. Julie Cohen (2012) sottolinea come questa nuova forma di regolazione algoritmica non sia neutrale, ma profondamente politica: essa istituisce vere e proprie eco-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

logie comportamentali, in cui il soggetto è governato attraverso la modulazione dell'ambiente informazionale, "indipendentemente dal contesto istituzionale e politico che circonda cause ed effetti" (Catanzariti 2021, p. 88, trad. nostra).

In questo contesto emergono concetti centrali come le *algo-norme* (Hydén 2020), che identificano forme di normatività autoesecutiva derivate da processi di apprendimento algoritmico; la regolazione adattiva, visibile in ambienti come i social media o le piattaforme di e-commerce e, infine, il diritto personalizzato (Casey, Niblett 2019). Le *algo-norme*, come descritto da Hydén (2020), rappresentano una forma di normatività algoritmica che emerge quando le decisioni regolative vengono delegate a sistemi basati su *machine learning* e *deep learning*. Questi sistemi non si limitano ad applicare regole predefinite, ma producono dinamicamente le proprie regole attraverso processi di ottimizzazione e adattamento continuo ai dati. Ne risultano configurazioni normative flessibili, situate, distribuite nel tempo e nello spazio.

Un ulteriore sviluppo della regolazione computazionale è rappresentato dal concetto di *personalized law* (Ben-Shahar, Porat 2021), secondo cui le regole giuridiche non sono più universali e impersonali, ma vengono adattate dinamicamente al singolo individuo. Le norme diventano personalizzabili sulla base di dati biometrici, preferenze comportamentali o inferenze algoritmiche. Il diritto, in questo scenario, si individualizza, con effetti potenzialmente dirompenti sulla parità di trattamento, sulla prevedibilità e sulla giustizia distributiva. La forma estrema di questa tendenza è esemplificata nella microdirettiva (Casey, Niblett 2019): una norma che non si limita a enunciare un principio generale, ma incorpora un algoritmo capace di tradurre tale principio in una direttiva concreta, personalizzata e comunicata in tempo reale al cittadino nel momento in cui ne ha bisogno.

Se la *Lex Algorithmica* rappresenta la fase in cui il diritto convenzionale tenta di riappropriarsi dello spazio regolativo attraverso strumenti come la *compliance by design*, l'*accountability*, il *risk-based approach* e l'obbligo di trasparenza dei sistemi algoritmici, essa segna anche l'ingresso in una nuova dimensione della normatività: quella in cui la responsabilità non è più solo assegnata, ma progettata.

Questa trasformazione implica un passaggio dai vincoli *ex post* (come le sanzioni) ed *ex ante* (come le prescrizioni normative) a vincoli *embedded*, ossia incorporati nell'architettura tecnica dei sistemi intelligenti. Il codice non è più solo strumento di automazione normativa, ma ambiente regolativo proattivo, capace di modulare i comportamenti e di rendere l'azione conforme in quanto già ontologicamente predisposta in tal senso.

In questa prospettiva, la riflessione di Luciano Floridi (2009, p. 171) sulla *distributed moral responsibility* fornisce la cornice teorica adeguata. Non si tratta semplicemente di diffondere la responsabilità tra gli attori (program-

matori, provider, deployer), ma di riconoscere che l'ambiente stesso in cui l'azione si compie è normativamente rilevante. L'integrità dell'IA, come proposta da Hamilton Mann (2024) in *Artificial Integrity*, consiste nella possibilità di concepire sistemi capaci di "frenarsi da soli", analogamente a un veicolo che rallenta automaticamente di fronte a un rischio, senza attendere l'intervento del guidatore o l'attivazione di un codice esterno.

Questa forma di regolazione computabile, che possiamo chiamare *constraint embedded*, rappresenta l'evoluzione più promettente (e più radicale) della *Lex Algorithmica*: non una mera giustapposizione di regole giuridiche e tecniche, ma una co-originazione sistemica di norme e architetture. L'IA viene così pensata non più come agente isolato da disciplinare, ma come nodo funzionale in un ambiente eticamente computato, in cui la responsabilità non è solo prevista, ma morfologicamente integrata nella sua capacità d'azione.

La *Lex Algorithmica*, in questa lettura, non è una fase transitoria verso la *Lex ex Machina*, ma il luogo concettuale in cui si decide se l'IA sarà un soggetto disciplinato *ex post*, o un attante etico computabile *embedded ex ante*. È qui che la normatività del codice, lungi dal cancellare il diritto, ne diventa vettore tecnico, e forse la sua evoluzione più sofisticata.

Esempi embrionali di questa logica sono già presenti nei semafori intelligenti, che personalizzano la segnaletica sulla base del traffico e del comportamento degli automobilisti. In questa prospettiva, il segnale di precedenza rappresenta la norma astratta, il segnale di stop una norma complessa, mentre il semaforo algoritmico incarna la transizione verso la microdirettiva computazionale: una norma che conosce chi la riceve e si adatta in tempo reale alla sua traiettoria.

Un altro esempio paradigmatico è il sistema installato su alcune automobili che impedisce l'avvio del motore in caso di superamento di un test alcolemico: qui la norma è direttamente implementata e fatta valere dal codice, senza spazio per interpretazioni o deroghe.

Anche Hilgendorf e Feldle (2018) rilevano come l'algoritmizzazione della decisione giuridica incida direttamente sulla produzione normativa, aprendo la strada a una *rule-making* computazionale che sottrae spazi alla deliberazione istituzionale. Sul piano delle implicazioni politiche, Rouvroy (2013) ha mostrato come la governamentalità algoritmica anticipi il comportamento individuale attraverso correlazioni statistiche, sostituendo la responsabilità con la predizione e svuotando la struttura teleologica del diritto. Shoshana Zuboff (2019, p. 352), infine, ha descritto questo modello come "instrumentarian power": un potere normativo che non vieta né punisce, ma orienta e condiziona il comportamento attraverso la sorveglianza computazionale e l'interazione anticipatoria.

Un'altra declinazione significativa della *Lex Algorithmica* è rappresentata dal cosiddetto *nudging* digitale, ovvero dalla modulazione comportamen-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

tale tramite micro-interventi progettuali: *layout*, notifiche, *default settings*, colori e temporizzazioni influenzano sistematicamente le scelte dell'utente (Sunstein 2015; Yeung, 2017a). In questo contesto, la normatività non si esprime sotto forma di obblighi o divieti, ma attraverso architetture decisionali personalizzate, che spingono l'utente a fare ciò che l'algoritmo ritiene più conveniente o desiderabile, sostituendo la regola giuridica con un orientamento persuasivo del comportamento.

La *Lex Algorithmica* si manifesta in modo particolarmente significativo attraverso regolamenti come il GDPR e l'AI Act, che tentano – *by design* – di bilanciare il potere predittivo degli algoritmi con principi di trasparenza, spiegabilità e responsabilità. Allo stesso tempo, sistemi di *credit scoring* automatizzati o *pricing* dinamico nelle piattaforme di *e-commerce* mostrano come l'algoritmo agisca da norma adattiva, applicando condizioni diverse a soggetti diversi in base al comportamento pregresso. In questi contesti, il diritto non è più universale, ma personalizzato e performativo.

3.4 Lex ex Machina: la giustizia eseguibile dalle macchine[6]

Preliminarmente è necessario distinguere tra *normatività computazionale* (Solum 2019) e *computational law* (Hildebrandt 2018). La prima caratterizza la fase *Code is Law*, in cui il codice agisce come forza regolativa implicita, ambientale e non giuridificata. La seconda, invece, appartiene alla fase della *Lex ex Machina*, in cui il diritto stesso è concepito per essere computato ed eseguito da macchine, con una sintassi logica causale e deduttiva.

Mentre nella *normatività computazionale* il codice struttura ambienti e comportamenti senza formalizzazione giuridica, nella *computational law* il codice diventa forma giuridica automatizzata, portando con sé problemi di trasparenza, spiegabilità e giustificazione. Si tratta, dunque, di due modalità differenti e successive del rapporto tra diritto e tecnica.

Un ulteriore salto qualitativo avviene con la *Lex ex Machina*, fase in cui la regolazione algoritmica non si limita a orientare comportamenti, ma automatizza l'intera funzione giuridica: la selezione della norma, l'analisi del precedente, la valutazione della rilevanza dei fatti. Si tratta di una trasformazione che investe l'attività giuridica nella sua funzione decisoria, e che si manifesta soprattutto nella cosiddetta giustizia predittiva.

Il codice informatico evolve in *computational law*: il diritto non solo viene eseguito da macchine, ma è progettato per essere computabile, come spiega Mireille Hildebrandt (2018). Le norme assumono una forma eseguibile, trattabile da un motore logico, strutturate secondo sintassi deduttive e au-

6 L'espressione "Lex Ex Machina" è tratta dall'omonima "Conference on Law's Computability" tenutasi al Jesus College, presso l'Università di Cambridge, il 13 dicembre 2019.

tomatizzate. Il diritto non è più pensato per l'uomo, ma per la macchina: è *law for machines*.

Questa trasformazione corrisponde, come nota Antoine Garapon (2021), a una rivoluzione grafica: una mutazione profonda delle modalità con cui le norme sono concepite, rappresentate e applicate. Non è più il testo a definire la legalità, ma la modellazione dei comportamenti attraverso il dato. Il diritto, osserva provocatoriamente un avvocato francese citato da Garapon, non è più "ciò che è scritto nei libri", ma "ciò che si legge nella curva statistica". Le decisioni non sono più il frutto di una deliberazione giuridica fondata su principi, ma di un processo tecnico-calcolante che produce anticipazioni comportamentali sulla base del passato.

Garapon sottolinea inoltre come questa nuova forma di normatività non si limiti alla giurisdizione, ma si estenda alla produzione delle norme stesse, attraverso strumenti di analisi predittiva del comportamento giurisprudenziale e modelli grafici che diventano, di fatto, la nuova fonte del diritto. L'esempio emblematico è la costruzione di diagrammi per la determinazione degli indennizzi nei licenziamenti, in cui la curva statistica sostituisce il ragionamento normativo, anticipando le decisioni giudiziarie con tale precisione da rendere superflua la funzione interpretativa del giurista.

Il rischio maggiore, avverte Garapon (2021), non è tanto l'uso della tecnologia, ma l'autorevolezza che il digitale esercita sul giudizio, grazie alla sua efficienza, alla sua precisione e alla sua percezione di neutralità. Si afferma così un sovvertimento della gerarchia epistemica: il sapere computazionale soppianta quello umano.

Non mancano, su questo punto, critiche radicali. Come mostrano Sartor e Santosuosso (2024), la "*decisione con l'IA*" comporta uno spostamento epistemico nella funzione del diritto: dall'argomentazione al calcolo, dalla giustificazione al risultato. I sistemi di *legal analytics* e *predictive justice* non si limitano a fornire supporto, ma orientano l'esito delle decisioni sulla base di precedenti statisticamente rilevanti, ridefinendo il concetto stesso di giurisdizione. Il rischio è duplice: da un lato, la cristallizzazione di bias pregressi nei modelli predittivi; dall'altro, la trasformazione del diritto in una "*macchina normativa*", che funziona senza comprensione e senza contesto.

Tra le critiche più articolate alla *Lex ex Machina* vi è quella di Barberis (2023), secondo cui l'inferenza algoritmica non può vantare alcun valore giuridico in quanto incapace di produrre ragioni dotate di significato, intenzionalità e valore argomentativo. A tale posizione si affianca l'analisi ermeneutica di Tuzet (2009), che sottolinea come le decisioni algoritmiche compromettano il carattere dialogico dell'interpretazione giuridica, e quella analitica di Poggi (2009), che denuncia la disintegrazione della logica giuridica a favore di una computazione puramente esecutiva.

Queste critiche, a nostro avviso, restano ancorate a una concezione intenzionalista e strumentalista della razionalità normativa, incapace di cogliere

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

la *mutazione ambientale* introdotta dalla regolazione computazionale. Come osserva Mann (2024), l'intelligenza artificiale non è una macchina nel senso meccanicistico del termine, bensì un ambiente sintattico performativo, che ristruttura le condizioni di possibilità (*affordances*) dell'agire normativo. Non si tratta dunque di sostituire la soggettività del giudice con l'automatismo, ma di prendere sul serio il fatto che l'ambiente stesso, nel quale il diritto opera, è stato digitalmente riconfigurato.

La *Lex ex Machina* non è un'illusione di calcolo, come si paventa nel denso volume curato da Carleo (2017), né una negazione della giuridicità (Cardon 2016; Supiot 2006): è un nuovo paradigma di azione regolativa (Solum 2019), in cui la sintassi costituisce (almeno in parte) la semantica, e l'efficacia procedurale prende il posto dell'intenzionalità soggettiva. In questo contesto, intelligibilità, giustificabilità e responsabilità non scompaiono, ma si riconfigurano in relazione all'ambiente computazionale che le ospita.

Se è vero che l'IA non comprende nel senso umano del termine, è altrettanto vero – come mostrano le teorie distribuzionali del linguaggio (Firth 1957), la filosofia computazionale del significato (Floridi 2011), e le riflessioni sull'intenzionalità operativa (Dennett 1989) – che una macchina può generare effetti semantici, performare analogie, produrre decisioni regolate, anche in assenza di comprensione cosciente, "semplicemente funzionando; una tecnologia funzionante sospende le pretese di consenso e assorbe quelle di dissenso" (Nassehi 2024, p. 164, trad. nostra).

Ecco perché, come propone Hildebrandt (2018) – distinguendo tre modelli di interazione tra diritto e tecnologie computazionali – occorre passare da una mera esecuzione computazionale (*Law for Machines*) a una *computational law* nel senso pieno: un diritto eseguibile sì (*Law by design*), ma progettato con razionalità giuridica (*Legal Protection by Design*), sottoposto a revisione, controllo e auditabilità. Solo così si potrà preservare il senso del diritto come forma di giustizia, anche in ambienti dominati dalla *machine-based legality*.

All'interno del paradigma della *Lex Ex Machina*, si collocano poi due fenomeni distinti ma convergenti: da un lato il proliferare di strumenti di *Legal Tech*, dall'altro la prospettiva teorica della *Legal Singularity*. Entrambi rappresentano forme di automazione della funzione giudiziaria, ma si differenziano profondamente per ambizione, portata e implicazioni normative.

La *Legal Tech* si riferisce all'insieme di tecnologie digitali – basate su machine learning, NLP, sistemi esperti – applicate alla gestione, analisi e predizione di dati giuridici. Essa include software per la ricerca giurisprudenziale automatizzata, la classificazione semantica degli atti processuali, la gestione documentale nei tribunali e persino strumenti di *legal analytics* capaci di prevedere gli esiti di un contenzioso (Surden 2014; Ashley 2017). Questi strumenti operano come estensioni operative del lavoro giuridico, contribuendo all'efficienza ma restando subordinati all'intervento umano.

Rientrano in un modello di supporto decisionale, dove la discrezionalità e la giustificazione sono ancora, almeno formalmente, appannaggio del giudice.

Ben diversa è l'idea di *Legal Singularity*, teorizzata da Alarie, Niblett e Yoon (2017), secondo i quali in un futuro non troppo lontano sarà possibile costruire un sistema predittivo talmente accurato, completo e auto-aggiornante da incarnare un diritto perfettamente anticipabile e computabile in ogni sua applicazione.

Queste dinamiche non restano astratte, ma trovano già applicazione in contesti giuridici concreti. Sul versante della *Legal Tech*, si moltiplicano le esperienze di giustizia automatizzata e predittiva: ad esempio, il sistema COMPAS (Lagioia, Rovatti, Sartor 2023) è utilizzato in numerosi Stati americani per supportare le decisioni di libertà vigilata e condizionale, attraverso la valutazione del rischio di recidiva basata su algoritmi opachi.

Sul versante della *Legal Singularity*, è paradigmatico il progetto *Blue J Legal*, cofondato da Benjamin Alarie in Canada, che sviluppa sistemi predittivi basati su machine learning per risolvere questioni tributarie, lavoristiche e di diritto societario, offrendo "opinioni legali probabilistiche" istantanee.

Analogamente, i *risk engines* utilizzati nel settore assicurativo (*trust scoring*) o bancario (*credit scoring*) operano valutazioni ex ante su individui, sostituendo la discrezionalità umana con modelli computazionali di decisione automatizzata.

La moderazione algoritmica è un altro laboratorio di *Lex ex machina*: un diritto senza legislatori, in cui l'intelligenza artificiale si sostituisce al giudizio umano, mettendo in crisi l'idea stessa di normatività democratica.

Le piattaforme digitali – da YouTube a Facebook, da TikTok a X (ex Twitter) – delegano a sistemi automatici di filtraggio, ranking e rimozione la gestione quotidiana del flusso informativo (Gillespie 2018).

Questo tipo di regolazione – spesso descritta come *governamentalità algoritmica* (Rouvroy 2013) – agisce secondo logiche di efficienza, engagement e tutela dell'immagine della piattaforma. Le policie di moderazione, benché formalmente dichiarate, vengono implementate attraverso black box algoritmiche non accessibili all'utente né al giudice. Ciò produce una profonda asimmetria informativa tra attori pubblici e privati, e tra piattaforme e soggetti digitali.

Dal punto di vista giuridico, questa architettura solleva interrogativi cruciali: la libertà di espressione può essere limitata da operatori privati attraverso criteri tecnici non verificabili? L'autocensura indotta dall'interazione con l'algoritmo è una violazione indiretta dei diritti fondamentali? Il soggetto digitale ha diritto a una motivazione algoritmica o a una contestazione effettiva?

La risposta del diritto convenzionale appare debole. Nonostante il Digital Services Act (DSA) e il Regolamento europeo sull'intelligenza artificiale (AI Act) tentino di imporre obblighi di trasparenza e procedure di contestazio-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

ne, la realtà resta dominata da architetture di potere computazionale che configurano un *diritto invisibile*, senza norme esplicite ma con effetti giuridici concreti.

3.5 Lex Cryptographica: la regolazione come protocollo tecnico decentralizzato

La *Lex Cryptographica* rappresenta la forma estrema della normatività tecnica: un modello regolativo basato su protocolli decentralizzati, eseguibili automaticamente e immuni da controllo istituzionale. In questo paradigma, la regolazione è codificata direttamente nel software, attraverso *blockchain*, *smart contracts* e le *Decentralized Autonomous Organizations* (DAO).

Nel panorama della regolazione algoritmica, le tecnologie blockchain segnano un punto di svolta: esse propongono un modello di normatività che pretende di fare a meno della fiducia personale e sociale. La blockchain si presenta come un ambiente *trustless*: un'infrastruttura in cui la cooperazione tra soggetti non si fonda più su relazioni di fiducia, ma sulla certezza matematica garantita dalla crittografia, dall'immutabilità del registro distribuito e dal consenso algoritmico.

Questa promessa di eliminazione della fiducia – *trustless* – è, però, paradossale. Come sottolineano De Filippi e Wright (2018), la blockchain non elimina la fiducia: la ricodifica. Non ci si fida più degli attori sociali, bensì dell'ambiente computazionale che struttura le interazioni. Non è la fiducia a sparire, ma è la fiducia tradizionale che si dissolve nella fiducia nell›infrastruttura tecnica. La blockchain diventa così una *digital architecture of trust*, in cui il trust è disincarnato, performato tecnicamente e reso invisibile.

La blockchain rappresenta la massima espressione della *Lex Cryptographica*: una "confidence machine" (De Filippi, Wright 2018), che consente la coordinazione tra attori senza bisogno di fiducia, proprio perché *trustless*. Ma questa assenza di fiducia non coincide con la sua superfluità: come ricorda Maurizio Ferraris (2021), *non esiste società senza fiducia, così come non esiste fiducia senza registrazione.* La blockchain, in tal senso, rappresenta un caso limite di *registrazione totale*, che paradossalmente elimina la fiducia per sostituirla con la verifica algoritmica permanente. Anche Niklas Luhmann (2002) distingueva tra fiducia (*trust*) come *riduzione della complessità* e fiducia (*confidence*) come *affidamento sistemico* su strutture impersonali: nella *Lex Cryptographica*, questo secondo livello si esaspera, e la fiducia personale viene completamente rimpiazzata da un automatismo tecnico.

La radicalizzazione di questo paradigma si manifesta nelle *Decentralized Autonomous Organizations* (DAO): enti collettivi regolati esclusivamente da *smart contract*, senza alcuna intermediazione umana. Nelle DAO, la regola non è più formulata e poi applicata: è direttamente eseguita. Non esiste

separazione tra produzione normativa ed enforcement. È il trionfo della *Lex Cryptographica*: il diritto viene scritto nel codice e il codice esegue se stesso (De Filippi, Wright 2018).

In questo senso, la blockchain realizza un doppio movimento: da un lato promette trasparenza, sicurezza, incorreggibilità; dall'altro lato instaura un ordine normativo rigido e non contestabile, impermeabile all'adattamento e alla revisione democratica.

Il sogno *trustless* si rivela così un miraggio: non l'abolizione della fiducia, ma la sua trasfigurazione tecnica; non la liberazione del soggetto, ma il suo incasellamento in un sistema autoesecutivo che non lascia spazi di negoziazione. In questo senso, la blockchain non è solo una tecnologia economica, ma un laboratorio politico della regolazione algoritmica, in cui si sperimenta un nuovo tipo di ordine senza alternative.

Questa transizione dalla *Lex Algorithmica* alla *Lex Cryptographica* segna un punto di rottura nella storia della normatività: la progressiva desemantizzazione della norma. Mentre la *Lex Algorithmica* si fonda ancora su inferenze adattive e su margini di contestualizzazione (per quanto opachi), la *Lex Cryptographica* elimina ogni spazio interpretativo in favore dell'autoesecuzione e dell'autoapplicazione. Il codice non argomenta, ma agisce; non persuade, ma vincola.

Anche il fenomeno della *tokenizzazione* costituisce un esempio paradigmatico di questa trasformazione (De Caria 2024). Il diritto, in questi contesti, si converte in token: oggetti digitali programmabili che non rappresentano soltanto diritti, obblighi o status giuridici, ma che li incorporano tecnicamente e ne automatizzano l'esecuzione. Il contratto diventa *smart*, il diritto reale diventa trasferibile con una transazione *on-chain*, la responsabilità si disperde nella logica automatica del codice.

Le DAO portano questo paradigma all'estremo: esse sono organizzazioni il cui funzionamento è integralmente regolato da *smart contracts*, ovvero da codice eseguibile distribuito sulla blockchain. Le regole dell'organizzazione non sono iscritte in statuti formali, ma nel codice stesso, che agisce come struttura regolativa auto-applicativa e inemendabile se non attraverso procedimenti formali interni.

Dal punto di vista teorico-giuridico, gli *smart contracts* vincolano le parti attraverso meccanismi di autoesecuzione, le DAO operano mediante logiche di consenso distribuito anziché mediante organi deliberativi, e l'infrastruttura della blockchain garantisce l'applicazione delle regole attraverso protocolli condivisi, senza ricorso a giudici o interpreti umani, fondando così una normatività radicalmente *trustless.*

La *Lex Cryptographica* (De Filippi, Mannan, Reijers 2022) che ne deriva, appare come una nuova forma di normatività senza Stato, senza giurisdizione e senza giudici, ma non per questo priva di effetti giuridici. Anzi: proprio

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

la sua efficacia automatica e il suo carattere globale ne fanno uno dei fenomeni più incisivi per la riconfigurazione del diritto nel XXI secolo.

In questo contesto si riapre un dibattito teorico fondamentale: *Code is Law* rappresenta una semplice estensione del paradigma autoritario del *Rule by Law*, oppure ne costituisce una radicalizzazione e un superamento? Se il *Rule by Law* tradizionale rimane comunque interno a un ordine giuridico (sebbene strumentalizzato), il *Rule by Code* segna una traslazione della normatività dalla legge alla tecnica.

La tensione si manifesta con particolare evidenza nel caso della identità digitale, che se affidata esclusivamente a meccanismi tecnici di certificazione e riconoscimento, rischia di dissolvere la persona giuridica nel semplice profilo digitale, erodendo lo spazio dell'autonomia e del riconoscimento.

In definitiva, *Lex Cryptographica* inaugura una *rule by code* che non si limita a rimpiazzare la norma con l'algoritmo, ma riformula la stessa idea di normatività: non più produzione giuridica contestabile, ma esecuzione automatica e inemendabile di condizioni tecniche predefinite.

4. Il diritto può ancora regolare la tecnologia digitale?

Nel contesto di crescente egemonia della regolazione tecnica e algoritmica, il diritto legislativo non è rimasto immobile. Al contrario, negli ultimi anni, soprattutto in ambito europeo, si è sviluppata una produzione normativa imponente, che mira a riaffermare il primato della legge nella governance dello spazio digitale.

Questo cambiamento di paradigma nella governance digitale può essere letto, in chiave interpretativa, come un *regulatory turn* dell'Unione Europea: un'inversione di tendenza che segna il passaggio da un approccio inizialmente neutrale o frammentario nei confronti delle tecnologie digitali, a una strategia giuridica coerente e sistematica volta a riaffermare la sovranità normativa europea. Tale svolta si manifesta in una serie di strumenti normativi – dal GDPR al DSA, dal DMA fino all'AI Act – che non solo intendono disciplinare le dinamiche del mercato e della comunicazione online, ma anche ribilanciare l'asimmetria tra regole tecniche e norme giuridiche. Pur non impiegando esplicitamente l'espressione *regulatory turn*, diversi autori (Veale e Zuiderveen Borgesius, 2021; Pollicino e Dunn, 2024; Pizzetti, Orofino e Longo, 2024; Torchia, 2023) riconoscono nella recente produzione normativa dell'UE un tentativo di riappropriazione giuridica dello spazio digitale e di affermazione di un modello europeo di regolazione fondato su trasparenza, accountability e tutela dei diritti fondamentali.

La *Regulatory Turn* europea si radica in una duplice genealogia concettuale: una *pars destruens*, che denuncia il degrado dello spazio digitale in

termini di potere e diseguaglianza, e una *pars construens*, che propone nuovi modelli normativi in grado di restituire centralità al diritto.

La *pars destruens* è rappresentata da diagnosi critiche che descrivono l'ecosistema digitale come uno spazio di potere privatizzato, opaco e post-statuale. Mazzuccato (2019) parla di *feudalesimo digitale*, denunciando la concentrazione di potere normativo nelle mani delle piattaforme come nuove signorie digitali. Reijers (2020), riprendendo la teoria dei *sovrani funzionali*, evidenzia il ruolo para-statuale degli attori tecnologici nella definizione delle regole del vivere online. Pasquale (2015), con l'espressione *sovrani digitali*, approfondisce ulteriormente la capacità delle piattaforme di esercitare una sovranità normativa senza mandato democratico. Come osserva Maria Rosaria Ferrarese (2022), siamo di fronte all'emersione di "nuovi poteri" privati, penetranti e opachi, in grado di esercitare una regolazione efficace senza transitare attraverso le forme tradizionali dello Stato di diritto. La forza di questa normatività risiede nella sua invisibilità: l'utente non percepisce di essere soggetto a una norma, ma semplicemente a un vincolo tecnico, a una funzionalità operazionale.

La *pars construens*, al contrario, riunisce quei filoni teorici che aspirano a ricondurre lo spazio digitale entro il perimetro del diritto. Hildebrandt (2018) e Brandford (2023) propongono una *rule of law by design*, fondata sull'incorporazione ex ante di principi giuridici nei sistemi tecnici. Diver (2022) introduce la nozione di *digisprudence* per designare un diritto che si esercita nella progettazione stessa delle architetture digitali. Suzor (2018), infine, rilancia un *digital constitutionalism* che individua nella Costituzione digitale una forma di bilanciamento tra poteri tecnici e diritti fondamentali. Questi approcci, pur diversi tra loro, convergono nell'idea che la tecnologia debba essere regolata attraverso forme innovative di giuridificazione, capaci di affrontare la normatività tecnica non con mera resistenza, ma con un progetto politico-giuridico attivo.

Il Regolamento generale sulla protezione dei dati (GDPR), il Digital Services Act (DSA), il Digital Markets Act (DMA), l'AI Act, il Data Governance Act e molte altre iniziative legislative disegnano un progetto coerente e ambizioso di riconquista giuridica dell'infosfera. L'Europa si è assunta il compito di disciplinare il potere digitale mediante l'introduzione di vincoli giuridici a piattaforme, algoritmi, mercati e sistemi decisionali automatizzati, secondo una logica di tutela dei diritti fondamentali, trasparenza, responsabilità e concorrenza (Sartor 2020). Eppure, nonostante l'articolazione di questo sforzo regolativo, resta aperta una questione teorica fondamentale: questa reazione normativa opera un bilanciamento effettivo rispetto alla tecno-regolazione oppure si limita a un aggiustamento tardivo, formalistico, forse persino ancillare? In altri termini: il diritto riesce ancora a regolare la tecnologia, oppure si adatta a essa, ne assume il linguaggio e la struttura, si riconfigura come interfaccia della governance digitale senza

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

modificarne i presupposti? La risposta, tutt'altro che univoca, richiede una disamina articolata. Da un lato, va riconosciuto che i testi normativi europei introducono per la prima volta obblighi giuridici stringenti nei confronti degli attori tecnologici globali: il GDPR ha posto limiti chiari alla raccolta, al trattamento e alla profilazione dei dati personali, istituendo diritti soggettivi nuovi come quello alla portabilità e alla deindicizzazione; l'AI Act classifica i sistemi di intelligenza artificiale in base al rischio, imponendo requisiti di trasparenza, sicurezza, governance e supervisione umana; il DSA e il DMA ridefiniscono le responsabilità delle piattaforme digitali dominanti, imponendo obblighi di moderazione dei contenuti, accesso ai dati, audit algoritmici e separazione funzionale tra servizi (Ebers, Navas 2020). Questi strumenti rappresentano tentativi concreti di ricostruire una sovranità normativa pubblica nello spazio digitale. Dall'altro lato, tuttavia, va rilevato che la forza regolativa di questi strumenti è limitata da vincoli strutturali profondi. In primo luogo, si tratta quasi sempre di dispositivi *ex post*, che agiscono su comportamenti già avvenuti, attraverso meccanismi di accountability, compliance, valutazione d'impatto e sanzione. La regolazione non precede il fatto tecnico, ma lo segue, cercando di porvi rimedio. In secondo luogo, molte delle obbligazioni introdotte si traducono in oneri procedurali, che non modificano la logica operativa delle piattaforme, ma la incapsulano entro cornici formali. Il diritto si ritira dalla normazione dei fini e si rifugia nella normazione delle forme. Ancor più rilevante è la tendenza, sempre più marcata, a incorporare i principi giuridici nella progettazione tecnica stessa: *privacy by design* (Cavoukian 2009), *ethics by design* (Mantelero 2018), *transparency by design* (Wachter, Mittelstadt, Floridi 2017) (come già previsti nel GDPR e rafforzati nel quadro regolativo dell'AI Act e del DSA, che ne istituzionalizzano la valenza tecnica e giuridica), *human oversight by design* (European Commission 2021). Questa strategia, pur nata dall'esigenza di prevenire abusi, finisce per accettare la logica della regolazione infrastrutturale, secondo cui il rispetto delle norme avviene non mediante controllo giuridico esterno, ma attraverso l'automazione del vincolo. Il diritto si converte in specifica funzionale, requisito tecnico, opzione configurabile. Come ha osservato Roger Brownsword (2020), in questi casi si produce un diritto senza giudice (*law without a judge*): efficace ma acefalo, conforme ma non deliberativo. Il rischio di questa evoluzione è duplice. Da un lato, l'ibridazione tra diritto e tecnologia può tradursi in una deresponsabilizzazione della normatività: nessuno è responsabile di ciò che il sistema decide, purché lo decida in modo tecnicamente conforme. Dall'altro, si rafforza un modello di regolazione automatica che marginalizza la dimensione argomentativa e interpretativa del diritto, ossia ciò che ne costituisce il nucleo democratico, con il rischio concreto di una deriva tecnocratica (Floridi 2022; Hildebrandt 2020). In questo senso, il tentativo europeo di normare il digitale rappresenta al tempo stesso una risposta e una conferma del paradigma che vor-

rebbe limitare. È una risposta, perché reintroduce vincoli legali, principi costituzionali, categorie di responsabilità. Ma è anche una conferma, perché assume la struttura tecnica come dato immodificabile, adattandosi ad essa piuttosto che trasformarla. La sfida per il diritto, allora, non è solo quella di regolare la tecnologia, ma di resistere alla sua naturalizzazione, riaffermando la possibilità di scelte normative che non siano già scritte nel codice.

A conferma della radicalità del cambiamento, è utile richiamare una convergenza teorica inaspettata ma feconda: quella tra l'approccio sistemico di Niklas Luhmann e la visione materialistica di Karl Marx. Entrambe, pur da prospettive opposte – cinicamente neo-funzionalista l'una, dialetticamente critica l'altra – riconoscono che la tecnologia non è mai neutrale, ma una forza autonoma che struttura l'ambiente sociale (Manfré 2008).

Per Marx (1867), la tecnologia rappresenta una forza produttiva materiale: il suo sviluppo altera i rapporti sociali e, con essi, le forme stesse della soggettività e del potere. Per Luhmann (1990), la tecnologia agisce come sottosistema operativo autoreferenziale, costruendo i propri codici e il proprio ambiente senza bisogno di legittimazioni esterne.

Nel contesto digitale contemporaneo, queste due intuizioni convergono. Il codice non solo funziona come sistema operativo ambientale, secondo la logica luhmanniana, ma incarna anche rapporti di dominio produttivo, come avrebbe evidenziato Marx. La regolazione algoritmica, lungi dall'essere un mero fatto tecnico, si presenta come una forma materializzata di governance economica e sociale, che integra produzione, controllo e normazione in un unico ambiente performativo.

In questa prospettiva, l'egemonia del codice si configura non solo come una trasformazione della normatività, ma come una ristrutturazione delle basi materiali e simboliche del potere, in cui il diritto rischia di operare sempre più come un supplemento formale posteriore, anziché come istanza originaria di regolazione.

Mentre da un punto di vista teorico, in risposta all'egemonia del codice come forma di regolazione tecnica, il dibattito contemporaneo ha conosciuto una polarizzazione tra due posizioni estreme: da un lato, il positivismo giuridico antiformalista, che rifiuta ogni riduzione del diritto alla computabilità, appellandosi al carattere ermeneutico, indeterminato e contestuale della normatività giuridica; dall'altro, il *legalismo computazionale*, che identifica il diritto con un sistema di regole formalizzabili e dunque traducibili in codice eseguibile.

È in questo contesto teorico-giuridico che emergono due proposte teoriche di *terza via*, fondate sulla consapevolezza che il codice possiede capacità normative reali, seppur parziali, e che la sfida non è tanto negarne l'efficacia, quanto costituirne i limiti e le condizioni di legittimità.

La prima è quella di Laurence Diver, che nella sua monografia *Digisprudence. Code as Law Rebooted* (2022) rifiuta sia il determinismo tec-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

nologico di Lessig, sia il riduzionismo computazionale dei fautori del diritto codificato. Diver denuncia i rischi del *legalismo computazionale*, ovvero l'illusione che il diritto possa essere integralmente tradotto in codice, cancellando le dimensioni discorsive, contestuali e interpretative della normatività giuridica. La sua *digisprudence* segna un cambio di paradigma nella riflessione della normatività digitale. Con questo termine, Diver intende una forma di riflessione giuridica non più centrata sull'enunciato normativo, ma sulla materialità della norma incorporata nel design computazionale. La *digisprudenza* propone di giuridificare il design, di trattarlo come una forma di legislazione pratica implicita – una *affordance* – vincolata da principi di legittimità, trasparenza e giustizia.

La seconda è rappresentata da Mireille Hildebrandt (2015, 2018), tra le maggiori teoriche del *digital constitutionalism*. In opposizione al determinismo tecnologico, Hildebrandt non rifiuta il "*law by design*", ma ne riconosce il potenziale solo a condizione che le architetture digitali siano progettate secondo i principi fondamentali del *Rule of Law*: giustificabilità, contestabilità, responsabilità. La sua proposta di *computational hermeneutics* (Hildebrandt, 2021) intende mantenere aperta la possibilità di interpretazione e giustificazione anche all'interno di sistemi algoritmici.

Nonostante la differenza di accenti, entrambi gli autori convergono su un punto essenziale: il diritto non può più essere pensato senza il design, ma deve essere progettato per garantire la propria vocazione emancipativa e democratica. La normatività digitale non può essere né subita né accettata acriticamente, ma va *normata*, proprio attraverso una *giurisprudenza computazionale critica* (Diver 2022) o un *costituzionalismo computazionale responsabile* (Hildebrandt 2018). In questo senso, il *by design* non è solo una tecnica, ma una forma di ragione normativa che *prepara le condizioni di input*, ponendo limiti, possibilità e contro-potere al codice.

Nel dibattito contemporaneo sulla regolazione digitale, una caratteristica ancora largamente sottovalutata dal positivismo anti-formalista, su cui si è arroccata una parte significativa della dottrina giuridica, riguarda la *natura epistemica del codice contemporaneo*. Quando si rifiuta il code come "cosa altra" dal diritto, lo si immagina ancora come un sistema rules-driven, simbolico, lineare, monòtono: un meccanismo deduttivo che applica regole fisse, come un sistema esperto degli anni Novanta. Ma proprio qui si coglie l'anacronismo dell'obiezione.

Il vero salto qualitativo del code contemporaneo non è nell'automazione della regola, ma nella sua trasformazione epistemica in sistema *data-driven* (Cristianini 2023). Il codice non è più simbolico ma statistico, non è più normativo in senso prescrittivo ma congetturale e probabilistico. I sistemi di *machine learning* e *deep learning* non eseguono regole: generano modelli inferenziali, basati su correlazioni, pattern e adattamenti continui. Non deducono, ma inferiscono sulla base di dati. Non si tratta quindi di una

normatività rigida, bensì plastico-adattiva, capace di modellare ambienti e comportamenti sulla base di feedback e previsioni. Ed è proprio questa flessibilità modellante che rende il codice *più normativo* del diritto, non meno.

Questa trasformazione, da *rules-driven* a *data-driven*, non cancella la normatività, ma la rende più efficace, perché più immanente agli ambienti digitali che il codice stesso costruisce. Negare questa dimensione significa combattere una guerra con armi epistemologiche spuntate, contro un nemico che ha già cambiato terreno, linguaggio e logica operativa.

Il code non deduce: induce, generalizza, corregge, correla, apprende. Le decisioni che produce non sono motivate da intenzioni soggettive, né da algoritmi deterministici, ma sono inferenzialmente giustificate sulla base di dati e correlazioni apprese. In questo, paradossalmente, il codice si avvicina al diritto, che anch'esso giustifica le proprie decisioni non sulla base di motivazioni psicologiche, ma attraverso argomentazioni inferenziali analogiche e induttive (Luhmann 2013, pp. 55-56) coerenti con norme, valori e precedenti.

Ma c'è di più. Il codice non si limita a normare un ambiente preesistente, come farebbe una legge rispetto alla società. Il codice costruisce l'ambiente che regola. Le architetture digitali non sono solo strumenti, ma mondi artificiali, ambienti performativi progettati per funzionare secondo le logiche operative del software. In questo senso, la normatività del *code* non è semplicemente regolativa, ma costitutiva e performativa: plasma i comportamenti, produce spazi d'azione, genera metriche di conformità. Non si limita a dire cosa è consentito o vietato, ma modella direttamente ciò che è possibile o impossibile fare (*affordance/disaffordance*).

Alla luce di tutto ciò, si comprende come il bersaglio polemico del "code is law" sia stato reso troppo facile. È vero che il tecno-determinismo lessighiano è stato criticabile per la sua visione totalizzante, ma è altrettanto vero che il suo nucleo teorico – l'idea che il codice sia una forma di normatività ambientale – resta pienamente valido.

È in questa cornice che, a nostro avviso, la *terza via* – quella proposta da Diver e Hildebrandt – appare come realizzazione implicita del progetto lessighiano del "by design": proprio la necessità di *regolare il codice con il codice*, di fare *law by design*, testimonia la superiorità normativa del codice che viene percepito come necessario terreno di battaglia normativa.

Se il codice costruisce l'ambiente e modula le azioni, allora il diritto, per sopravvivere, non può limitarsi a interpretare o limitare: deve performare. È in gioco non solo la giuridicità delle regole, ma la soglia stessa dell'azione regolativa. Ciò che viene meno non è il diritto in quanto tale, ma la pretesa che esso sia l'unico luogo legittimo della normatività sociale. In questo senso, la normatività digitale non è un'espansione tecnica del diritto, ma una sfida ontologica alla sua esclusività.

Un aspetto trascurato ma decisivo del diritto nell'era digitale è la presenza di vere e proprie *clausole deregolative*, inserite all'interno degli stessi testi nor-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

mativi. Si tratta di formule giuridiche che, lungi dal disciplinare attivamente il comportamento dei soggetti o degli artefatti, autorizzano l'autonomia della tecnica, rinunciando alla funzione classica di imposizione normativa. È il legislatore stesso che, consapevolmente, *depotenzia il diritto*, lasciando campo alla regolazione automatica.

Il GDPR, per esempio, pur riconoscendo la centralità del consenso, trasforma tale consenso in un dispositivo di deresponsabilizzazione *ex lege*, che libera da obblighi ogni attore che lo ottenga, anche in situazioni di evidente asimmetria informativa o manipolazione del design (Zuboff 2019). Si produce così una paradossale *degiuridificazione del diritto alla protezione*, mascherata da potenziamento del controllo individuale.

Il Digital Services Act (DSA), attraverso la cosiddetta clausola del buon samaritano (art. 6), stabilisce che le piattaforme non perdano il beneficio dell'esenzione di responsabilità (*safe harbour*) per il solo fatto di aver agito volontariamente per individuare e rimuovere contenuti illeciti o per conformarsi al diritto dell'Unione. Apparentemente neutra, tale disposizione incoraggia una forma di moderazione algoritmica proattiva, eseguita direttamente dagli Internet Service Provider, senza però garantire adeguati meccanismi di controllo giurisdizionale ex ante. In tal modo, la clausola finisce per legittimare una governance privata dei contenuti, in cui l'intervento pubblico risulta indebolito o posticipato, e la discrezionalità tecnica della piattaforma diviene il perno della normazione.

Inoltre, il meccanismo di *notice and takedown*, previsto dal GDPR e dal DSA e da altri atti legislativi che tutelano i diritti digitali, impone un onere significativo, *supererogatorio*, sugli utenti per segnalare contenuti illeciti online. Mentre questa procedura può sembrare prima facie un modo per migliorare la tutela dei diritti online, può essere considerata un *dispositivo responsabilizzante* (Fisher 2018) per gli utenti comuni. Non tutti gli utenti però hanno la conoscenza, il tempo o le risorse per segnalare prontamente ogni contenuto illecito che incontrano.

Anche l'AI Act, nonostante l'ambizione regolativa, contiene una clausola deregolativa strutturale: lo stralcio della responsabilità da danno algoritmico, in fase finale di negoziazione, rappresenta un ritiro del diritto rispetto alla sua funzione rimediale. L'assenza di una disciplina della responsabilità lascia il cittadino esposto a un sistema decisionale opaco, senza possibilità di rimedio in caso di errore, danno o abuso.

In tutti questi casi, non è la tecnica a sottrarre spazio al diritto, ma è il diritto stesso a cedere il passo alla tecnica, scegliendo di non esercitare la propria forza regolativa. La clausola deregolativa rappresenta dunque una figura nuova del diritto postmoderno: non consiste nell'assenza di norma, ma nella presenza di una norma che autorizza l'assenza, ossia in una delegittimazione preventiva del diritto.

5. La persona come presenza algoritmica: il caso del minore

La trasformazione digitale non investe soltanto i modelli di regolazione e governance, ma incide profondamente anche sulla natura della soggettività. La persona, infatti, non è più concepita come centro autonomo di deliberazione e responsabilità, bensì come oggetto computabile di osservazione, classificazione e previsione. Seguendo l'impostazione di Gunther Teubner, si può parlare – come si è detto – di *attanti giuridici*: entità che acquisiscono rilevanza normativa all'interno di *regimi inter-legali*, dove il diritto tradizionale coesiste, si intreccia o soccombe rispetto alla normatività operativa incorporata nelle architetture tecniche (Teubner 2006, 2012). In questa prospettiva, la soggettività non è data, ma performata dall'ambiente normativo digitale.

La prima generazione che ha attraversato la fase cruciale dell'adolescenza in simbiosi con dispositivi digitali è la Generazione Z. È all'interno di questa cerchia generazionale che si manifesta con maggiore evidenza l'impatto delle tecnologie digitali sulla formazione dell'identità. A differenza del mondo offline, dove l'età anagrafica continua a rappresentare una soglia normativa, nel contesto online essa risulta largamente trascurata: la registrazione ai social media è tecnicamente accessibile anche ai minori di tredici anni attraverso semplici espedienti di autocertificazione. La soglia minima dei tredici anni, istituita dal COPPA Act statunitense del 1998, ha finito per imporsi come standard globale, pur essendo inadeguata a tutelare soggetti cognitivamente vulnerabili.

Come suggerisce Jonathan Haidt (2024), si potrebbe agire in sintonia con quei genitori che ritengono necessario imporre limiti di età all'accesso a internet da parte dei figli. Una soluzione praticabile per rispondere a questa esigenza sarebbe quella di mettere a disposizione dei genitori un meccanismo per contrassegnare i device dei figli come appartenenti a un minore. Questo contrassegno, integrabile a livello di hardware o software, indicherebbe in modo inequivocabile alle aziende l'obbligo di rispettare restrizioni legate all'età anagrafica dell'utente, vietando l'accesso in assenza di consenso parentale: un'implementazione di protezione by design, che sposta il baricentro normativo dalla responsabilità individuale alla configurazione tecnica dell'ambiente digitale.

L'apporto teorico di Niklas Luhmann consente di articolare ulteriormente questa prospettiva. Nei sistemi sociali complessi, le persone tendono a essere ridotte a *punti funzionali*, ossia interfacce sistemiche che assolvono al compito di selezionare, elaborare e distribuire informazione secondo logiche comunicative autoreferenziali (Luhmann 1995). Nell'ambiente computazionale, questa dinamica si radicalizza: la persona non è più il referente della norma, ma una variabile funzionale che viene gestita in termini di efficienza comunicativa e valore estratto.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

A tal riguardo, anche la lettura marxiana può offrire una chiave critica decisiva per comprendere la soggettività digitale. Se Luhmann la dissolve nei flussi sistemici e Teubner la ricostruisce come attante co-costruito, da parte sua Marx (1844) individua nella tecnica una forma di alienazione sociale. Il soggetto non è semplicemente osservato o performato, ma espropriato: perde il controllo sui prodotti della propria attività (oggi: dati, preferenze, interazioni), che vengono oggettivati in architetture digitali dalle quali è escluso. Nell'ambiente digitale, l'alienazione non è solo economica, ma ontologica: il minore, come ogni individuo, viene ridotto a "forza-lavoro informazionale" (Fuchs 2020), continuamente catturata, modellata, valorizzata, senza possibilità di autodeterminazione. La sua soggettività viene così reificata in codice, trasformata in vettore di valore computazionale. In questo senso, la persona digitale non è solo attante o funzione, ma soggetto alienato, separato da sé stesso attraverso un processo di espropriazione normativa e simbolica.

Numerosi studi empirici mostrano come l'immersione precoce e prolungata nei social media abbia effetti differenziati sulla salute mentale di ragazzi e ragazze.

Twenge (2018) e Haidt (2024) documentano un aumento significativo di ansia, depressione e disturbi alimentari tra gli adolescenti, con particolare incidenza tra le adolescenti, soggette a un'esposizione costante al confronto sociale e al perfezionismo estetico. Come, in particolare, sottolinea Jonathan Haidt (2024), a un certo punto della cosiddetta transizione digitale le adolescenti si sono ritrovate assoggettate al confronto socio-valoriale centinaia di volte di più di quanto lo fossero mai state nell'arco dell'intera evoluzione umana. Ciò le ha esposte maggiormente ad aggressività e cattiveria, alimentate dalla struttura stessa dei social media, che favorisce il conflitto relazionale. Inoltre, a partire dal 2010, queste stesse dinamiche hanno iniziato a coinvolgere, con effetti simili, anche i ragazzi. Spostando l'attenzione sull'importanza attribuita a follower e like – indipendentemente dal genere e dall'età – la Rete ha progressivamente hackerato la percezione del proprio valore sociale, generando una vera e propria ossessione per i feedback ricevuti (Turkle 2015). Tutti questi sviluppi hanno concorso a compromettere un diritto fondamentale, quello alla salute mentale, che dovrebbe essere garantito come inviolabile per tutti gli adolescenti (Ehrenberg 2010).

Tale disagio può essere letto anche attraverso la categoria sociologica dell'anomia (Durkheim 1969), intesa come disintegrazione delle regole condivise e smarrimento identitario. Nelle generazioni cresciute online, la mancanza di relazioni stabili radicate in ambienti offline produce una soggettività errante, fragile, sprovvista di coordinate normative affidabili. Ciò comporta una nuova forma di anomia digitale: i legami sono intermittenti, la visibilità è fluida, la normatività è frammentata. Il risultato è quello di un'esistenza

orientata non più da comunità stabili, ma da reti che si disattivano e riattivano senza continuità (Manfré 2025).

Ora, a nostro avviso, il concetto durkheimiano di anomia può offrire un contributo decisivo per comprendere il senso di vuoto normativo che ha investito la Generazione Z. Tale generazione manifesta una crescente difficoltà a radicarsi in contesti sociali stabili, offline, dove le relazioni sono fondate sulla continuità e sulla prossimità. Il tessuto sociale tradizionale – fatto di legami duraturi tra individui in carne e ossa – è stato progressivamente sostituito da reti digitali in cui le connessioni sono fluide, intermittenti e spesso prive di riconoscibilità stabile. Come già osservava Karl Mannheim (2008), la comunità organica che storicamente ha sostenuto la formazione identitaria degli adolescenti lascia spazio a una normatività instabile, discontinua, disincarnata. Vivere in un contesto anomicamente strutturato espone i minori a fragilità psicosociali profonde, che non possono essere affrontate con nostalgiche idealizzazioni del passato, bensì con una rinnovata attenzione alla valorizzazione della soggettività e del potenziale espressivo individuale, all'interno di ambienti capaci di rigenerare forme di socialità normativamente sensate.

A questa vulnerabilità si aggiunge una trasformazione radicale del rapporto tra memoria individuale e memoria sociale. Come evidenzia Elena Esposito (2001), la digitalizzazione ha spostato le funzioni mnemoniche dalla mente individuale ai dispositivi e alle infrastrutture tecnologiche, producendo un *outsourcing* cognitivo sistemico. Tanto più il cervello viene alleggerito dallo sforzo di ricordare, tanto maggiore è il rischio di atrofia delle capacità critiche. La memoria sociale – intesa come struttura comunicativa che seleziona e stabilizza l'informazione rilevante – non serve tanto a ricordare quanto a dimenticare: a ordinare e semplificare il flusso informazionale. Questo processo, apparentemente efficiente, può però generare un effetto collaterale insidioso: una perdita di profondità nella costruzione dell'identità personale, soprattutto nei nativi digitali. Come già osservato altrove (Manfré 2022), l'abitudine a delegare ogni funzione di richiamo mnemonico a supporti esterni finisce per ridurre la capacità di concentrazione e l'autonomia riflessiva dei soggetti, portando a una vera e propria involuzione cognitiva rispetto alle generazioni precedenti.

In un contesto segnato dalla complessità delle interazioni digitali e dalla crescente automazione delle relazioni sociali, la nozione di *persona* non può più essere assunta come punto di partenza naturale o ontologico. Seguendo la teoria dei sistemi di Niklas Luhmann, possiamo interpretare la *persona* non come un soggetto dotato di interiorità stabile, ma come una riduzione semantica funzionale alla comunicazione. Luhmann definisce la persona come "il termine che denota che non si riesce a osservare per quale ragione le aspettative acquisiscano maggiore probabilità quando sono connesse entro un sistema psichico" (Luhmann 1990). In altri termini, la persona è una

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

costruzione osservativa che consente di stabilizzare l'incertezza tipica della doppia contingenza tra sistemi, garantendo una sufficiente prevedibilità nelle interazioni.

Applicando questa intuizione al contesto digitale, possiamo affermare che qui anche la persona opera come una *black box* semantica, un'interfaccia osservabile entro cui fluiscono dati, comportamenti, preferenze, identificatori biometrici e affettivi.

In linea con la concezione sistemica di Luhmann, il minore emerge quindi come un *soggetto desoggettivizzato*, la cui identità non precede l'interazione, ma si costruisce retroattivamente nella codifica algoritmica delle sue tracce digitali. La soggettività fragile non è un accidente, ma il risultato inevitabile di un ecosistema informazionale che chiede non soggetti consapevoli, ma nodi efficienti di elaborazione dati.

La stabilità del riconoscimento, così come la legittimità dell'interazione, non deriva da una sostanza soggettiva ma dalla capacità di essere osservati come nodi identificabili nei processi algoritmici. In questo senso, la persona digitale si colloca esattamente tra *habeas corpus* e *habeas data*: da un lato è corpo osservato, dall'altro archivio permanente di dati e metadati. Come *black box* algoritmica, essa non è mai completamente accessibile, né ai sistemi tecnici né ai sistemi sociali; e, pur tuttavia, è ciò su cui si costruiscono aspettative stabili, comportamenti legittimi, accessi consentiti o negati.

Il carattere profetico del pensiero luhmanniano consiste proprio nel mostrare come l'ordine sociale emergente – oggi anche in forma digitale – non dipenda dalla trasparenza delle identità, ma dalla capacità dei sistemi di ridurre l'opacità strutturale attraverso forme di personalizzazione semantica. In questo senso, la persona digitale è il risultato di una mediazione sistemica tra visibilità, rilevanza e controllo: è ciò che permette la comunicazione tra *black box* digitali e sociali, e insieme ciò che viene continuamente *programmato* e *riprogrammato* dall'ambiente algoritmico.

Nel quadro teorico delineato da Niklas Luhmann, la persona non rappresenta un'entità ontologicamente data, ma una costruzione semantica funzionale alla comunicazione tra sistemi complessi. In contesti di *doppia contingenza*, dove ogni sistema (psichico o sociale) opera come una *black box* – ovvero come un'entità opaca, intrasparente all'altro – la *persona* funge da dispositivo di riduzione dell'imprevedibilità: un'interfaccia comunicativa, che permette ai sistemi di orientarsi nel mutuo riconoscimento, senza mai giungere a una reale trasparenza interiore (Luhmann 1995).

Applicare tale impostazione alla figura del minore nell'ambiente digitale significa riconoscerne la soggettività non tanto come espressione di un'identità profonda e psicologicamente data, quanto come risultato emergente di aspettative comunicative strutturalmente funzionali. Il minore diviene così una *persona digitale*, una costruzione osservabile e osservata, riconfigurata

continuamente nei suoi input e output relazionali, nel gioco riflessivo tra visibilità algoritmica e opacità sistemica.

Tale costruzione della persona digitale si innesta in una configurazione normativa ambigua, sospesa tra *habeas corpus* (la protezione del corpo fisico del minore) e *habeas data* (la tutela dei suoi dati e tracciati digitali) (Maestri 2020). Il corpo stesso della persona, nella rete, si smaterializza in una molteplicità di segnali e impronte digitali che producono effetti giuridici, morali e comportamentali. In tal senso, la persona digitale non è più una semplice "estensione" della persona fisica, ma un oggetto informazionale morale normativamente attivo, la cui presenza nell'infosfera si configura nei media algoritmici che ne condizionano esistenza e riconoscibilità (Floridi 2009).

Il minore rappresenta una figura paradigmatica del paziente morale nell'infosfera floridiana. Ma è anche la soglia critica in cui la fragilità ontologica e quella giuridica si sovrappongono.

In questo scenario, il minore emerge come paziente morale privilegiato, non solo per la sua vulnerabilità psicologica, ma perché esposto a un ambiente performativo che lo costruisce come nodo di calcolo. Questa condizione impone un rovesciamento del paradigma della responsabilità: non più centrata sull'agente intenzionale, ma sul progettista dell'ambiente. Non è più (solo) questione di soggetti che agiscono, ma di ambienti digitali che normano, anticipano, incanalano i comportamenti. È per questo che Floridi (2014) parla di *tecnologie di terz'ordine*: non strumenti, non agenti, ma ambiti ontologici artificiali in cui si vive, si agisce, si decide.

L'azione è così spostata da un piano intenzionale a un piano architetturale, dove la responsabilità non è solo dell'agente, ma dell'intera rete di progettazione e implementazione dell'ambiente informazionale.

Nello spazio digitale, ogni forma di presenza – anche quella del minore – è tecnicamente disciplinata da architetture digitali che ne definiscono la visibilità, l'accesso e la possibilità di interazione. La sua soggettività giuridica viene progressivamente plasmata all'interno di ambienti computazionali che non solo reagiscono al comportamento, ma lo anticipano e lo orientano, producendo quelle che sono state chiamate le *algorithmic subjectivities* (Baumer, Taylor, Brubaker, McGee 2024), intese come configurazioni relazionali del sé emergenti dall'interazione tra minori, interfacce, algoritmi e norme sociali codificate in ambienti digitali (Armano, Briziarelli, Flores, Risi 2022).

Questo approccio, sviluppato nell'ambito della *Human-Computer Interaction* (HCI), rovescia la prospettiva tradizionale centrata sull'esperienza del minore-utente: non è il minore a disporre dell'ambiente digitale, ma è piuttosto la sua soggettività a essere prodotta all'interno dell'ambiente algoritmico. La soggettività del minore è co-costruita da interazioni che coinvolgono non solo preferenze e identità, ma anche *affordances* tecniche e logiche predittive, che regolano le condizioni di possibilità del suo essere online (Dourish 2016).

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

Il minore non è soltanto un attante algoritmico, ma incarna una nuova forma di soggettività regolata in profondità: una *habitus machine* (Airoldi 2022), concetto che designa quei dispositivi digitali che, in quanto artefatti normativi prediscorsivi, modellano silenziosamente il contesto d'azione, generando schemi comportamentali automatizzati. Non si tratta solo di rispondere a norme esplicite, ma di interiorizzare pattern normativi invisibili incorporati nell'architettura tecnica. L'*habitus machine* non è il risultato di una deliberazione autonoma, ma di una regolazione sistematica e anticipatoria dell'azione, resa operativa attraverso metriche, notifiche, *ranking* e dispositivi normativi emozionali[7]. La soggettività del minore viene così prodotta come comportamento previsto, tracciato, misurabile e performato, secondo una logica di ottimizzazione funzionale che esclude la disobbedienza e riduce la possibilità stessa della deviazione.

In quest'ottica, il minore non è soltanto un soggetto vulnerabile, ma un *attante algoritmico*: un'entità co-costituita attraverso l'aggregazione, l'analisi e il feedback di micro-interazioni (click, scroll, tempo di permanenza). La sua soggettività è una funzione emergente della progettazione algoritmica degli ambienti digitali, in cui anche gesti minimi diventano dati interpretabili, tracciabili, predittivi. Il rischio è che tali dinamiche conducano a una *anomia computazionale*, dove il minore, svuotato delle garanzie dell'habeas corpus, viene contratto in una figura di *habeas data*, ridotto a vettore informazionale manipolabile.

Questa condizione produce effetti giuridicamente rilevanti. In primo luogo, il minore è esposto a una normazione silenziosa e pervasiva, che agisce *ex ante*, prima ancora che egli possa esercitare la propria volontà. In secondo luogo, si realizza una *doppia colpevolizzazione* del minore: da un lato come vittima di architetture tecniche pensate per suscitare dipendenza e manipolazione comportamentale; dall'altro come soggetto colpevolizzato da regimi normativi che lo ritengono responsabile di condotte apprese all'interno di ambienti normativi disfunzionali. La vulnerabilità del minore, invece di essere oggetto di tutela, diventa così leva di sorveglianza, profitto e controllo.

Alla luce di queste trasformazioni, il diritto è chiamato a ripensare le categorie classiche della soggettività e della tutela, interrogandosi non solo sul "chi" è il minore, ma sul "come" esso viene costruito nei sistemi digitali.

---

7 In questo senso, l'aggettivo 'prediscorsivi' richiama il concetto di *habitus* elaborato da Pierre Bourdieu (1977), inteso come sistema incorporato di disposizioni pratiche e cognitive che orientano l'azione al di là della coscienza riflessiva e dell'enunciazione esplicita. Trasposto al contesto tecnologico, tale concetto permette di comprendere come le tecnologie digitali operino come dispositivi di naturalizzazione e automatizzazione delle pratiche: esse "fanno fare", cioè inducono comportamenti, vincoli e scelte, senza transitare per il linguaggio normativo tradizionale o per la formalizzazione discorsiva delle regole. In tal modo, la normatività si esprime sotto forma di una performatività tecnica incorporata, pre-giuridica e non necessariamente consapevole.

In questa prospettiva, non è più solo l'utente a esperire il mondo tecnologico, ma è il minore stesso a emergere come soggettività costruita e resa operazionale da un'interazione algoritmica con ambienti digitali performativi.

Tale meccanismo trasforma il minore in un *paziente morale* (Floridi 2009): non solo agente, ma soggetto la cui vulnerabilità richiede una particolare attenzione normativa in quanto esposto a un ambiente che determina *ex ante* le sue possibilità di azione, relazione e costruzione identitaria. Il paziente morale è colui che subisce la normazione, che non dispone delle conoscenze necessarie per negoziare la propria esposizione al potere computazionale (Durante, 2019), né per sottrarsi alla performatività tecnica che struttura ogni dimensione della sua esperienza digitale.

In questo quadro, la soggettività del minore si presenta come una soggettività fragile, regolata da aspettative di sistema e continuamente negoziata nei codici della rete: una black box semantica che permette alla comunicazione di avere luogo, ma che espone allo stesso tempo a nuovi rischi di anomia, disinibizione e alienazione normativa (Suler 2004).

Il caso dei minori – e, più in generale, degli adolescenti – costituisce quindi la lente paradigmatica attraverso cui osservare questa metamorfosi. Il minore, infatti, è un soggetto vulnerabile, iper-esposto, spesso privo degli strumenti critici per comprendere la natura predittiva, invisibile e pervasiva della normazione algoritmica. Ambienti digitali come piattaforme sociali, videogiochi, strumenti educativi e spazi di socializzazione non si limitano a registrare comportamenti: li anticipano, li orientano, li performano. Metriche predittive, logiche di engagement e dispositivi normativi emozionali – like, notifiche, badge, feedback – costruiscono la soggettività adolescenziale sulla base di parametri computazionali, creando un ambiente normativo implicito e continuo, in cui la prestazione e la conformazione sono ininterrotte. L'infanzia e l'adolescenza vengono così normate tecnicamente attraverso una *disciplina digitale* invisibile ma efficace, che produce forme specifiche di conformazione comportamentale, ansia performativa e interiorizzazione di standard artificiali.

Come osserva Michele Willson (2018), il minore non è semplicemente monitorato, ma è plasmato da ecosistemi algoritmici che normalizzano comportamenti e traiettorie di sviluppo sin dalla nascita, creando una soggettività predittivamente guidata verso modelli di "normalità" costruiti tecnicamente.

Il processo di quantificazione (Lupton 2016) che attraversa la formazione della soggettività adolescenziale non è neutrale: come evidenzia Willson (2018), le metriche algoritmiche producono categorie di normalità e devianza, orientando implicitamente gli standard di comportamento desiderabile e conforme.

La soggettività adolescenziale si forma così all'interno di un ambiente performativo continuo, in cui ogni azione è valutata, incentivata o pena-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

lizzata da sistemi invisibili, automatizzati, non negoziabili. Questo carico normativo costante produce, il più delle volte, forme di disagio mentale e psicosociale – ansia, depressione, dipendenza, isolamento – non come effetti accidentali, ma come esiti strutturali di una regolazione opaca e non contestabile (Barocas, Selbst 2016; Mittelstadt, Allo, Taddeo, Wachter, Floridi 2016). Il minore non è allora più solo un soggetto debole da tutelare: è *un punto di condensazione normativa,* il cui trattamento segnala lo stato di salute dell'intero sistema giuridico nell'epoca computazionale.

Una delle aree in cui la regolazione algoritmica produce effetti profondi e spesso drammatici sulla soggettività è quella della costruzione dell'identità giovanile. Gli adolescenti si trovano immersi in ambienti digitali regolati da meccanismi di visibilità, ranking, engagement, che orientano in modo sottile la percezione di sé, il rapporto con il corpo, la relazione con l'altro. I sistemi algoritmici, progettati per massimizzare il tempo di permanenza e la responsività, sfruttano le vulnerabilità emotive e cognitive tipiche di questa fascia d'età.

Il like, il commento, la notifica non sono strumenti neutri, ma dispositivi normativi emozionali, che strutturano l'esperienza dell'autostima, dell'appartenenza, del riconoscimento. I soggetti più esposti – per età, fragilità psichica, esclusione sociale – vengono così costantemente confrontati con standard performativi artificiali, che producono – come abbiamo detto – ansia, depressione, dipendenza, alienazione. La salute mentale diventa una variabile influenzata da logiche di calcolo e predizione, e la soggettività fragile viene silenziosamente normata secondo criteri computazionali.

Le metriche di engagement funzionano come vettori normativi impliciti, che strutturano il bisogno di riconoscimento, l'autostima e il senso di appartenenza.

Il risultato è l'emersione del fenomeno del "me quotidiano" (Negroponte 1995): termine che indica un sistema conformato e personalizzato sugli interessi, sui pregiudizi e sulle idiosincrasie dell'agente informazionale. La soggettività fragile viene così inglobata in una logica predittiva che non solo valuta il minore per ciò che è, ma soprattutto per ciò che potrebbe diventare, sulla base di dati parziali e algoritmi opachi, in linea con quanto descritto da Willson (2018) sulla trasformazione della tutela in gestione predittiva del rischio.

Il disagio adolescenziale non può più essere compreso come deviazione individuale o problema psicologico isolato, ma come *effetto sistemico* di un ecosistema normativo disfunzionale, in cui la soggettività rimane vincolata.

Le tre vulnerabilità classiche dell'ambiente digitale – anonimato, accessibilità e convenienza – sono oggi integrate da nuove forme di distorsione cognitiva e affettiva: la disinibizione online (Suler 2004), la distanziazione tra sé reale e sé digitale, la dissoluzione del giudizio morale e la frammentazione del sé in "dividui" (Rouvroy 2013) delineano un soggetto adolescenziale vulnerabile non per natura, ma per design.

I dispositivi digitali diventano *psico-dispositivi* di iper-captazione dell'attenzione (Stiegler 2010), capaci di disgregare ogni forma di attenzione riflessiva, con effetti diretti sul piano dell'identità e della salute mentale. Il minore è progressivamente catturato in un regime di *iper-attenzione frammentata*, modellata dal design stesso delle piattaforme.

Il compito del diritto, allora, non è solo quello di proteggere il minore in quanto tale, ma di riconoscere nel minore il punto limite in cui si manifesta una fragilità costitutiva dell'umano nella società automatizzata, e a partire da questo estremo, ripensare l'intera architettura della tutela giuridica.

In tale scenario, il diritto è chiamato a riformulare il paradigma della tutela, superando il modello universalistico e post-deliberativo del soggetto astratto, per adottare una logica differenziale, situata e anticipatoria (Rodotà 2007). Si tratta di spostare il centro della normatività dalla regolazione degli atti alla regolazione degli ambienti: non solo intervenendo *ex post* sui contenuti, ma *ex ante* sulle architetture e sulle logiche computazionali che determinano visibilità, interazione e riconoscimento (Nissenbaum 2009; Solove 2004).

Una delle sfide principali in questo ambito riguarda la tutela della privacy dei minori, che rappresenta oggi un punto critico per la giustizia algoritmica. Il GDPR ha riconosciuto l'esigenza di protezione rafforzata, stabilendo che il trattamento dei dati personali dei minori sia legittimo solo con il consenso esplicito del titolare della responsabilità genitoriale (art. 8), e attribuendo agli Stati membri la facoltà di fissare soglie d'età (tra i 13 e i 16 anni). Tuttavia, la complessità tecnica dei processi di raccolta e profilazione rende illusorio il controllo informato da parte di genitori e minori, mentre le pratiche di consenso risultano spesso opache, condizionate da design ingannevoli e prive di alternative reali (Lupton, Williamson 2017).

Inoltre, i meccanismi di verifica dell'età sono frammentari, tecnicamente incerti e giuridicamente fragili: l'autoverifica è aggirabile; la verifica biometrica è invasiva e inaffidabile nei soggetti in crescita; la verifica tramite ID è onerosa e poco implementata. Ciò fa sì che, pur essendo formalmente tutelata, la privacy dei minori online resta esposta a un'economia predatoria della sorveglianza, fondata sulla *datafication* dell'infanzia (Livingstone, Stoilova, Nandagiri 2019).

L'ansia, la depressione, la dipendenza digitale e la disforia sociale sono sintomi di una soggettività costruita e vincolata da ambienti che, lungi dall'essere neutri, perseguono finalità economiche di massimizzazione dell'attenzione e della profilazione commerciale.

La questione assume un rilievo ancora maggiore quando si considera l'effetto della *governance predittiva* sulla responsabilità individuale. La responsabilità giuridica, nella sua configurazione classica, presuppone volontà, imputabilità e nesso causale. Ma nell'universo della regolazione algoritmica, il soggetto è valutato non per ciò che ha fatto, ma per ciò che *potrebbe fare*,

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

sulla base di modelli statistici e classificazioni di rischio. L'adolescente non è più destinatario di diritti, ma target predittivo. Ne deriva una soggettività condizionata e frammentata, priva dei presupposti epistemici e normativi della responsabilità giuridica tradizionale (Citron, Pasquale 2014; Floridi 2014).

Il soggetto si fa così un vettore predittore, un insieme di dati interpolati, un target profilato. La sua soggettività giuridica viene ridefinita a partire dalla visibilità computazionale, e non dalla deliberazione autonoma. Ciò comporta una crisi della responsabilità classica: se la decisione è automatica, chi è responsabile dell'errore? Se l'esito è probabilistico, si può ancora parlare di imputazione individuale? Il diritto si trova di fronte a una soggettività disumanizzata, su cui non è più possibile applicare meccanismi tradizionali di giustificazione o contestazione.

Tale mutamento incide anche sulla rappresentazione sociale del soggetto: i sistemi algoritmici non vedono persone, ma dati. La persona non è più titolare di uno statuto, ma di una valutazione dinamica. Ciò genera forme di discriminazione algoritmica non più fondate su categorie giuridiche esplicite, ma su inferenze implicite, spesso opache. Il principio di uguaglianza formale viene così minato da pratiche che, pur non violando direttamente il diritto, producono effetti normativi discriminatori.

La soggettività algoritmica si configura come una soggettività condizionata, frammentata, esposta a poteri normativi non negoziabili. Questo disagio deve essere letto anche come conseguenza della governance predittiva: algoritmi predittivi che, come sottolinea Willson (2018), anticipano e disciplinano la vita del minore in base a probabilità statistiche, riducendo lo spazio della libertà a favore di una gestione attuariale delle esistenze.

Il minore non è più soggetto nella sua libertà, ma oggetto tracciabile e prevedibile, computato secondo logiche funzionali. Questo determina uno slittamento profondo della responsabilità: non è più il soggetto a rispondere delle proprie azioni, ma è l'ambiente a costituirne la possibilità, il contesto e i limiti operativi.

Questo scenario impone al diritto una sfida di fondo: la riconfigurazione della tutela giuridica in ambienti computazionali.

La protezione dei minori non può limitarsi a una disciplina ex post dei contenuti o dei comportamenti devianti. Occorre, invece, spostare l'asse della normatività dalla governance degli atti alla governance degli ambienti: non solo regolare ciò che accade, ma intervenire preventivamente sull'architettura delle piattaforme, sul design algoritmico e sulla logica funzionale che determina le forme della visibilità, dell'interazione e del riconoscimento. Solo così è possibile opporre una resistenza giuridica alla normazione invisibile e autoesecutiva che struttura l'esperienza digitale del soggetto fragile.

Il minore, in quanto *attante* esposto e *punto funzionale* di una normatività opaca, rappresenta dunque oggi il luogo critico in cui si misura la tenuta

del diritto come istituzione capace di nominare, proteggere e riconoscere la persona. L'esigenza di una protezione costituzionale della soggettività fragile non è una mera istanza etica o psicologica, ma un *imperativo giuridico-funzionale*: l'unica via per evitare che la soggettività venga progressivamente ridotta a una funzione del codice è che la persona, come categoria giuridica, venga dissolta nei flussi performativi della regolazione algoritmica.

Nello spazio digitale la protezione del minore richiede un mutamento profondo del paradigma normativo. Il diritto non può limitarsi a regolamentare contenuti o comportamenti ex post, ma deve agire *ex ante* sulle architetture stesse, intervenendo sugli ambienti che producono soggettività. È necessaria una traslazione del principio di legalità dalla norma alla forma, dalla regola alla struttura, dall'atto al contesto. Solo così sarà possibile garantire una tutela effettiva della soggettività fragile, non più come mera espressione astratta di dignità, ma come configurazione concreta e situata in un ecosistema normativo automatico.

Il minore, in quanto soggetto iper-esposto e normato da dispositivi opachi e performativi, diventa la *cartina di tornasole* della giustizia algoritmica. Il suo statuto giuridico non può essere ridotto a quello di utente consenziente – come incredibilmente previsto dal GDPR all'art. 8, che accetta la finzione di un consenso libero e informato da parte dei minori – ma deve essere ripensato come centro vulnerabile di imputabilità e di diritto.

In definitiva, il minore rappresenta il paradigma della soggettività fragile nell'infosfera, ma non ne è purtroppo l'unico interprete. Come suggerisce Luciano Floridi, nella società dell'informazione ognuno di noi è al contempo agente e paziente morale, perché siamo esposti – anche inconsapevolmente – agli effetti normativi di ambienti digitali progettati non per tutelare l'autonomia personale, ma per ottimizzare il funzionamento sistemico del codice stesso (Floridi 2014). Come scrive Floridi (2009, p. 173):

> il cyberspazio catturato sta conquistando il suo vincitore. Le ICT stanno re-ontologizzando il nostro mondo, cioè ne stanno modificando la natura essenziale così come stanno creando nuove realtà.

L'infosfera, lungi dall'essere un mero contenitore di interazioni, è un ambiente computazionalmente performato, che tende a ridurre la persona a una funzione, a un nodo, a un input predittivo, a un inforg. In questo contesto, la vulnerabilità non è più soltanto una condizione minorile, ma una condizione ontologica universale, che investe chiunque abiti l'ambiente digitale in quanto tale. Ciò perché "il *code* è ontocentrico", orientato cioè alla strutturazione dell'essere, mentre il diritto è normocentrico, ossia legato alla regolazione dell'agire; il *code* non si limita a disciplinare comportamenti, ma *costruisce mondi*, mentre il diritto cerca di normare azioni già situate.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

Riconoscere questa trasformazione è il primo passo per re-istituire una tutela giuridica capace di opporsi alla riduzione algoritmica della persona e di riaffermare la dignità del soggetto nell'epoca computazionale.

Anche se, da un punto di vista sociologico, come osserva Michele Willson (2018), all'interno di ambienti computazionali normativi rimane aperta la possibilità che i minori sviluppino pratiche di resistenza e di riappropriazione creativa delle tecnologie, sovvertendo gli usi prescritti e reclamando spazi di agency. Questo margine di resilienza sottolinea che, pur in una condizione di fragilità sistemica, la soggettività digitale non è del tutto determinata, e può ancora generare processi di risignificazione e trasformazione critica dell'ambiente informazionale.

6. Conclusione. Per una teoria critica della normatività digitale

La rivoluzione digitale ha spostato il baricentro della normatività: dal diritto al codice, dalla norma simbolica al dispositivo tecnico, dalla deliberazione democratica all'implementazione automatica. Il diritto non è semplicemente affiancato dalla tecnica: è riassorbito, reso ancillare rispetto a forme di regolazione più rapide, pervasive, invisibili.

La normatività si è trasformata: da prescrizione pubblica a funzione ambientale; da enunciato giuridico ad algoritmo operativo; da responsabilità soggettiva a profilazione predittiva.

Questa mutazione produce effetti profondi sulla soggettività e sul concetto stesso di regola. La regolazione algoritmica non enuncia ma struttura, non comanda ma condiziona, non argomenta ma anticipa. Il soggetto giuridico ne esce trasformato: da individuo responsabile a target computazionale.

Il compito della teoria sociologica del diritto è allora quello di misurarsi con la metamorfosi della normatività nello spazio digitale, dove la regolazione si distribuisce in forme eterogenee: norme giuridiche, codici computazionali, standard tecnici, policy private e architetture ambientali. Su questi processi, la sociologia del diritto ha già offerto letture pluralistiche, analizzando la coesistenza e la conflittualità tra regimi normativi differenti. Ciò che oggi si impone, tuttavia, è un'evoluzione ulteriore: una teoria capace di osservare come la soggettività venga modellata da dispositivi normativi computazionali e performativi, che operano attraverso selezioni automatizzate, profilazioni e metriche adattive. Non basta descrivere la moltiplicazione delle fonti: occorre interrogare i poteri che le articolano, esigere trasparenza, reclamare forme procedurali di contestabilità.

Così, il futuro del diritto non sarà restaurazione del passato, ma ridefinizione critica della normatività: eterarchica, computazionale, performativa. Solo una teoria consapevole dell'asimmetria tra codice e legge, tra efficienza e giustizia, potrà orientare la tecnica verso fini pubblici. Non per riaffermare

il primato della legge o del "diritto della società" capitalistica neo-liberale, ma per costruire una grammatica normativa all'altezza della complessità dell'infosfera – capace anche di riconoscere, nel "diritto della soggettività" delle nuove generazioni, l'ambito in cui si giocano oggi le tensioni tra regolazione automatica e autonomia, tra conformazione algoritmica e aspirazione all'auto-normazione.

Bibliografia

Accoto G., (2017), *Il mondo dato. Cinque brevi lezioni di filosofia digitale*, Milano, Egea.

Airoldi M., (2022), *Machine Habitus: Toward a Sociology of Algorithms*, Cambridge UK, Polity Press.

Alarie B., (2016), The path of the law: Towards legal singularity, *University of Toronto Law Journal, 66* (4), pp. 443-462.

Alarie B., Niblett A., Yoon A. H, (2018), How artificial intelligence will affect the practice of law, *University of Toronto Law Journal, 68* (1), pp. 106-124.

Armano E., Briziarelli M., Flores J., Risi E., (2022), *Platforms, Algorithms and Subjectivities: Active Combination and the Extracting Value Process*. *An Introductory Essay*, in Armano E., Briziarelli M., Risi E., eds., *Digital Platforms and Algorithmic Subjectivities*, London, University of Westminster Press, pp. 1-18.

Ashley K. D., (2017), *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambridge, Cambridge University Press.

Barberis M, (2023), *Separazione dei poteri e giustizia digitale*. Milano, Mimesis.

Barocas S., Selbst A. D., (2016), Big Data's Disparate Impact, *California Law Review*, 104, pp. 671-732, https://doi.org/10.2139/ssrn.2477899

Baumer E. P. S., Taylor A. S., Brubaker J. R., McGee M., (2024), Algorithmic subjectivities, *ACM Transactions on Computer-Human Interaction,* 31 (3), 35, pp. 1-34, https://doi.org/10.1145/3660344

Bayamlıoğlu E., Leenes, R., (2018), The 'rule of law' implications of data-driven decision-making: A techno-regulatory perspective, *Law, Innovation and Technology,* 10 (2), pp. 295-313, https://doi.org/10.1080/17579961.2018.1527475

Ben-Shahar O., Porat A., (2021), *Personalized law: Different rules for different people*, Oxford University Press.

Benkler Y., (2006), *The wealth of networks: How social production transforms markets and freedom*, New Haven, Yale University Press.

Bourdieu P., (1977), *Outline of a theory of practice*, Cambridge University Press.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

Bradford A., (2023), *Digital Empires: The Global Battle to Regulate Technology*, Oxford University Press.
Brownsword R., (2005), Code, control, and choice: Why East is East and West is West, *Legal Studies, 25* (1), pp. 1-21, https://doi.org/10.1111/j.1748-121X.2005.tb00268.x
Brownsword R., (2008), *Rights, Regulation, and the Technological Revolution*, Oxford University Press.
Brownsword R., (2019), *Law, technology and society: Reimagining the regulatory environment*, Abdingon, Routledge.
Brownsword R., (2020), *Law 3.0: Rules, regulation and technology*, Abingdon, Routledge.
Cabitza F., Floridi L., (2021), *L'intelligenza artificiale. L'uso delle nuove macchine*, Milano, Bompiani.
Cardon D., (2016), *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, Milano, Mondadori.
Carleo A., a cura di, (2017), *Calcolabilità giuridica*, Bologna, Il Mulino.
Casey A. J., Niblett A., (2019), A framework for the new personalization of law, *University of Chicago Law Review*, *86* (2), pp. 333-358.
Catanzariti M., (2021), Algorithmic law: Law production by data or data production by law?, in Micklitz H.W., Pollicino O., Reichman A., Simoncini A., Sartor G., De Gregorio G., eds., *Constitutional challenges in the algorithmic society*, Cambridge, Cambridge University Press.
Cavoukian A., (2009), *Privacy by Design: The 7 foundational principles*, Information and Privacy Commissioner of Ontario.
Citron D. K., Pasquale F, (2014), The scored society: Due process for automated predictions, *Washington Law Review*, 89 (1), pp. 1-33.
Cohen J. E., (2012), *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, New Haven, Yale University Press.
Colomba V., a cura di, (2005), *I diritti nell'era digitale: libertà di espressione e proprietà intellettuale*, Parma, Diabasis.
Cristianini N., (2023), *Come le macchine sono diventate intelligenti senza pensare in modo umano*, Bologna, Il Mulino.
De Caria R., (2024), *The tokenised economy and the law*, Cheltenham, Edward Elgar Publishing.
De Filippi P., Hassan S., (2016), Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code, *First Monday Journal*, 21 (12).
De Filippi P., Wright A., (2018), *Blockchain and the Law: The Rule of Code*, Harvard, Harvard University Press.
De Filippi P., Mannan M., Reijers W., (2022), The alegality of blockchain technology, *Policy and Society, 41* (3), pp. 358-372, https://doi.org/10.1093/polsoc/puac006

Dennett D. C., (1989), *The Intentional Stance*, Cambridge (MA), MIT Press.
Diver L. E., (2022), *Digisprudence: Code as Law Rebooted*, Edinburgh, Edinburgh University Press.
Dourish P., (2016), Algorithms and their others: Algorithmic culture in context, *Big Data & Society*, 3 (2), pp. 1-11.
Durante M., (2019), *Potere computazionale: L'impatto delle ICT su diritto, società, sapere*, Milano, Mimesis.
Durkheim E., (1969), *Il suicidio. L'educazione morale*, Torino, Utet.
Easterbrook F. H., (1996), *Cyberspace and the Law of the Horse*, 1996 University of Chicago Legal Forum, (1), pp. 207-216.
Ebers M., Navas S., eds., (2020) *Algorithms and Law*, Cambridge, Cambridge University Press.
Ehrenberg A., (2010), *La società del disagio. Il mentale e il sociale*, Torino, Einaudi.
Esposito E., (2001), *La memoria sociale. Mezzi per comunicare e modi di dimenticare*, Roma-Bari, Laterza.
European Commission, (2021), *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*, COM, 206 final.
Ferrarese M. R., (2022), *Poteri nuovi. Privati, penetranti, opachi*, Bologna, Il Mulino.
Ferrari V., (1992), *Le funzioni del diritto*, Roma-Bari, Laterza.
Ferrari V., (2021), Diritto e nuove tecnologie della comunicazione, *Rendiconti di Lettere – Istituto Lombardo Accademia di Scienze e Lettere, 155,* pp. 13-26.
Ferraris M., (2021), *Documanità. Filosofia del mondo nuovo*, Roma-Bari, Laterza.
Finocchiaro G., (2008), *Diritto di Internet*, Bologna, Zanichelli.
Firth J. R., (1957), *Papers in Linguistics 1934-1951*, London, Oxford University Press.
Fisher M., (2018), *Realismo capitalista*, Roma, Nero Editions.
Floridi L., (2009), *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, Giappichelli.
Floridi L., (2011), *The Philosophy of Information*, Oxford, Oxford University Press.
Floridi L., (2014), *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford, Oxford University Press.
Floridi L., (2022), *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, Raffaello Cortina.
Fuchs C., (2020), *Communication and Capitalism: A Critical Theory*, London, University of Westminster Press.

Garapon A., Lassègue J., (2021), *Giustizia digitale. Determinismo tecnologico e decisione giudiziaria*, Bologna, Il Mulino.

Gillespie T., (2018), *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*, New Haven, Yale University Press.

Goldoni M., (2007), Politiche del codice. Architettura e diritto nella teoria di Lessig, *Archivio Marini*, recuperato da http://www.archiviomarini.sp.unipi.it/350/1/lessig.pdf

Goldoni M., (2015), The politics of code as law: towards input reasons, in Reichel J., Lind A. S., eds., *Freedom of Expression, the Internet and Democracy,* Leiden, Brill, pp. 115-133.

Haidt J., (2024), *La generazione ansiosa. Come i social hanno rovinato i nostri figli*, Milano, Rizzoli.

Hildebrandt M., (2015), *Smart technologies and the end(s) of law: Novel entanglements of law and technology*, Cheltenham, Edward Elgar Publishing.

Hildebrandt M., (2018), *Law for Computer Scientists and Other Folk*, Oxford, Oxford University Press.

Hildebrandt M., (2020), Code-driven law: Freezing the future and scaling the past, in Markou C., Deakin S., eds., *Is law computable? Critical perspectives on law and artificial intelligence,* Oxford, Hart Publishing, pp. 67-83.

Hildebrandt M., (2021), *The Meaning and the Mining of Legal Texts*, in Barry D. M., ed., *Understanding the Digital Humanities*, New York, Palgrave, 145-160.

Hilgendorf E., Feldle J., eds., (2018) *Digitization and the law*, Baden-Baden, Nomos Verlag.

Hydén H., (2020), *Sociology of digital law and artificial intelligences*, in Přibáň J., ed., *Research handbook on the sociology of law*, Cheltenham, Edward Elgar Publishing, pp. 357-369.

Johnson D. R., Post D. G., (1996), Law and borders: The rise of law in cyberspace, *Stanford Law Review, 48* (5), pp. 1367-1402.

Karavas V., (2009), The force of code: Law's transformation under information-technological conditions, *German Law Journal, 10* (4), pp. 463-482, https://doi.org/10.1017/S2071832200001164

Koops B. J., Leenes R., (2014), Privacy regulation cannot be hardcoded: A critical comment on the 'privacy by design' provision in data-protection law, *International Review of Law, Computers & Technology, 28* (2), pp. 159-171, https://doi.org/10.1080/13600869.2013.801589

Lagioia F., Rovatti R., Sartor G., (2023), Algorithmic fairness through group parities? The case of COMPAS-SAPMOC, *AI & Society, 38*, pp. 459-478, https://doi.org/10.1007/s00146-022-01400-x

Latour B., (2005), *Reassembling the social: An introduction to actor-network-theory*, Oxford, Oxford University Press.

Leenes R. E., (2011), Framing techno-regulation: An exploration of state and non-state regulation by technology, *Legisprudence, 5* (2), pp. 143-169, https://doi.org/10.2139/ssrn.2182439
Lessig L., (1999), *Code and Other Laws of Cyberspace*, New York, Basic Books.
Lessig L., (2006), *Code: Version 2.0*, New York, Basic Books.
Lettieri N., (2020), Law in Turing's Cathedral: Notes on the algorithmic turn of the legal universe, in Barfield W., ed., *The Cambridge handbook of the law of algorithms*, Cambrdige, Cambridge University Press, pp. 691-721.
Livingstone S., Stoilova M., Nandagiri R., (2019), *Children's data and privacy online: Growing up in a digital age. An evidence review*, London School of Economics and Political Science.
Luhmann N., (1982), *Sistema giuridico e dogmatica giuridica*, Bologna, Il Mulino.
Luhmann N., (1983), *Struttura delle società e semantica*, Roma-Bari, Laterza.
Luhmann N., (1990), *Sistemi sociali. Fondamenti di una teoria generale*, Bologna, Il Mulino.
Luhmann N., (1995), *Osservazioni sul Moderno*, Armando, Roma.
Luhmann N., (2002), *La fiducia*, Bologna, Il Mulino.
Luhmann N., (2012), *Il diritto della società*, Torino, Giappichelli.
Luhmann N., (2013), *Esistono ancora norme indispensabili?*, Roma, Armando.
Lupton D., (2016), *The quantified self: A sociology of self-tracking*, London, Polity Press.
Lupton D., Williamson B., (2017), The datafied child: The dataveillance of children and implications for their rights, *New Media & Society, 19* (5), pp. 780-794.
Maestri E., (2015), *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Napoli, Edizioni Scientifiche Italiane.
Maestri E., (2020), La persona digitale tra *habeas corpus* e *habeas data*, in Bilotta F., Raimondi F., a cura di, *Il soggetto di diritto. Storia ed evoluzione di un concetto nel diritto privato*, Napoli, Jovene Editore, pp. 177-200.
Manfré G., (2008), *La società della società*, Urbino, QuattroVenti.
Manfré G., (2022), The Uneasiness of Generations, in Corradini A., Manfré G., *Becoming What You Are. Education and Society,* Perugia, I libri di Emil, pp. 71-89.
Manfré G., (2025), Durkheim come interprete della modernità: la Sociologia e la dimensione morale dell'educazione, introduzione a Durkheim E., *La Sociologia e l'Educazione*, Milano, Ledizioni, pp. 7-32.
Mann H., (2024), *Artificial integrity: The paths to leading AI toward a human-centered future*, Hoboken (NJ), Wiley.
Mannheim K., (2008), *Le generazioni*, Bologna, Il Mulino.

Mantelero A., (2018), AI and Big Data: A blueprint for a human rights, social and ethical impact assessment, *Computer Law & Security Review*, 34 (4), pp. 754-772.
Marx K., (1968). *Manoscritti economico-filosofici del 1844*, Torino, Einaudi.
Marx K., (1993), *Il Capitale. Libro I*, Roma, Editori Riuniti (1867).
Mazzucato M., (2019), Preventing digital feudalism, *Project Syndicate*, https://www.sipotra.it/wp-content/uploads/2020/01/Preventing-Digital-Feudalism.pdf
Mittelstadt B. D., Allo P., Taddeo M., Wachter S., Floridi L., (2016), The ethics of algorithms: Mapping the debate, *Big Data & Society, 3*(2), https://doi.org/10.1177/2053951716679679
Nassehi A., (2024), *Patterns: Theory of the digital society*, London, Polity Press.
Negroponte N., (1995), *Being digital*, New York, Knopf Doubleday Publishing Group.
Nissenbaum H., (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, Stanford University Press.
Pascuzzi G., (2020), *Il diritto dell'era digitale*, Bologna, Il Mulino.
Pasquale F., (2015), *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard, Harvard University Press.
Pizzetti F., Orofino M., Longo E., (2024), *La regolazione europea della società digitale*, Torino, Giappichelli.
Poggi F., (2009), Il diritto meccanico. La metafora del diritto come macchina e i suoi limiti, *Diritto e Questioni Pubbliche*, 9, pp. 395-400.
Pollicino O., Dunn P., (2024), *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*, Milano, Bocconi University Press.
Reidenberg J. R., (1998), Lex informatica: The formulation of information policy rules through technology, *Texas Law Review, 76* (3), pp. 553-593.
Reijers W., (2020), Responsible innovation between virtue and governance: Revisiting Arendt's notion of work as action, *Journal of Responsible Innovation, 7* (3), pp. 471-489.
Rheingold H., (1993), *The virtual community: Homesteading on the electronic frontier*, Boston (MA), Addison-Wesley.
Rodotà S., (2007), *Dal soggetto alla persona*, Napoli, Editoriale Scientifica.
Rossato A., (2006), *Diritto e architettura nello spazio digitale. Il ruolo del software libero*, Padova, CEDAM.
Rouvroy A., (2013), Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuality, *Réseaux*, *31* (177), pp. 163-196.
Sartor G., (2005), *Legal reasoning: A cognitive approach to law*, Berlino, Springer.

Sartor G., (2020), Artificial intelligence and human rights: Between law and ethics, *Maastricht Journal of European and Comparative Law, 27* (6), pp. 705-719.
Sartor G., Santosuosso A., (2024), *Decidere con l'IA. Intelligenze artificiali e naturali nel diritto*, Bologna, Il Mulino.
Solove D. J., (2004), *The Digital Person: Technology and Privacy in the Information Age*, New York University Press.
Solum L. B., (2019), Artificially intelligent law, *BioLaw Journal – Rivista di BioDiritto*, (1), pp. 53-62.
Stiegler B., (2010), *Taking care of youth and the generations*, Stanford, Stanford University Press.
Suler J., (2004), The online disinhibition effect, *CyberPsychology & Behavior, 7* (3), pp. 321-326.
Sunstein C. R., (2015), *Choosing Not to Choose: Understanding the Value of Choice*, Oxford, Oxford University Press.
Supiot A., (2006), *Homo juridicus. Saggio sulla funzione antropologica del diritto*, Milano, Mondadori.
Surden H., (2014), *Machine Learning and Law*, Washington Law Review, *89* (1), pp. 87-115.
Suzor N., (2018), Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms, *Social Media + Society*, 4, https://doi.org/10.1177/2056305118787812
Teubner G., (2006), Rights of Non-humans? Electronic Agents and Animals as New Actors, in Politics and Law, *Journal of Law and Society*, 33 (4), pp. 497-521.
Teubner G., (2012), *Constitutional Fragments: Societal Constitutionalism and Globalization*, Oxford University Press.
Teubner G., (2015), *Ibridi ed attanti: Attori collettivi ed enti non umani nella società e nel diritto*, Milano, Mimesis.
Torchia L., (2023), *Lo Stato digitale. Una introduzione*, Bologna, Il Mulino.
Turkle S., (2015), *Reclaiming Conversation: The Power of Talk in a Digital Age*, New York, Penguin Press.
Tuzet G., (2009), Il diritto non è una macchina, *Diritto e Questioni Pubbliche*, 9, pp. 401-422.
Twenge J. M., (2018), *Iperconnessi. Perché i ragazzi oggi crescono meno ribelli, più tolleranti, meno felici e del tutto impreparati a diventare adulti*, Torino, Einaudi.
Veale M., Zuiderveen Borgesius, F., (2021), Demystifying the Draft EU Artificial Intelligence Act, *Computer Law Review International, 22* (4), pp. 97-112.
Wachter S., Mittelstadt B., Floridi L., (2017), Why a right to explanation of automated decision-making does not exist in the General Data Protection

Regulation, *International Data Privacy Law*, 7 (2), pp. 76,99, https://doi.org/10.1093/idpl/ipx005

Weber R. H., (2002), *Regulatory Models for the Online World*, Zurich/Basel/Geneva.

Weber R. H., (2018), "*Rose is a rose is a rose is a rose" – What about code and law*?, *Computer Law* and *Security Review*, *34* (*4*), pp. *701-706*.

Willson M., (2018), Raising the ideal child: Algorithms, quantification and prediction, *Media, Culture & Society*, 41 (5), pp. 620-636, https://doi.org/10.1177/0163443718798901

Yeung K., (2017a), 'Hypernudge': Big Data as a Mode of Regulation by Design, *Information, Communication & Society*, 20 (1), pp. 118-136.

Yeung K., (2017b), Algorithmic regulation: A critical interrogation, *Regulation & Governance, 12* (4), pp. 505-523.

Zaccaria G., (2022), *Postdiritto: Nuove fonti, nuove categorie*, Bologna, Il Mulino.

Ziccardi G. (2006), *Libertà del codice e della cultura*, Milano, Giuffrè.

Zittrain J. L., (2008), *The future of the internet – and how to stop it*, New Haven, Yale University Press.

Zuboff S., (2019), *Il capitalismo della sorveglianza: Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, Luiss University Press.