DOSSIER

Adolescenti nell'epoca della trasformazione digitale: un approccio sociologico, normativo e culturale

Adolescents in the Era of Digital Transformation: A Sociological, Legal, and Cultural Approach

a cura di M. Paola Mittica, Michele Martoni, Enrico Maestri, Giorgio Manfré

edited by M. Paola Mittica, Michele Martoni, Enrico Maestri, Giorgio Manfré

Introduzione

Introduction

Enrico Maestri[1], Giorgio Manfré[2],
Michele Martoni[3], M. Paola Mittica[4]

Dalla commistione tra realtà *online* e realtà *offline* emergono nuovi ambienti di vita – non luoghi, mondi onlife, infosfere e metaversi – in grado di includere tutti gli spazi informativi digitali *online* e analogici *offline*, in cui l'essere umano è contemporaneamente presente.

A differenza dei e delle Millenials – la generazione precedente che, pur avendo abbracciato largamente le dimensioni esperienziali offerte da internet, conserva ancora la memoria dell'analogico e dell'*offline* – gli e le adolescenti delle I-Generation Zeta e Alpha non hanno più alcuno scarto rispetto alla tecnologia digitale: nascono e affrontano il proprio compito evolutivo in un nuovo ambiente ibrido, dove *online* e *offline* si integrano.

Ciò comporta l'emersione di forme esperienziali inedite che incidono su vari aspetti della crescita – dallo sviluppo del potenziale cognitivo e delle competenze, alle capacità relazionali, ai diversi livelli di attività psico-fisica – nella costante esposizione a ecosistemi che sfidano la nostra capacità sia di comprensione, sia di vigilanza critica di fronte a meccanismi poco trasparenti, che influenzano il discernimento e orientano le azioni delle e degli adolescenti.

Questo profondo mutamento antropologico scuote i pattern di riferimento consolidati, che hanno un impatto sullo spazio pubblico, sulla politica stessa e sulle aspettative della società e delle giovani generazioni, mettendo alla prova anche le relazioni tra adulti e adolescenti in termini di cura, controllo e consenso.

Alla luce di queste considerazioni, il Dossier mette in dialogo la Sociologia del diritto con le sensibilità di sociologi, filosofi del diritto, informatici giu-

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 Dipartimento di Giurisprudenza, Università degli Studi di Urbino. michele.martoni@uniurb.it

4 Dipartimento di Giurisprudenza, Università degli Studi di Urbino. maria.mittica@uniurb.it

Data invio: 4 ottobre 2025. Data accettazione: 10 ottobre 2025.
DOI: https://doi.org/10.54103/1972-5760/30047

ridici e giuristi lungo quattro assi tematici: a) *regolativo*, volto a osservare i diversi livelli di normatività della società digitale, dal codice informatico alla base delle tecnologie digitali come regola tecnica, alle conseguenze che questi algoritmi hanno sul sistema sociale, con l'obiettivo di svolgere una riflessione critica su come le tecnologie digitali, in modo sempre meno trasparente e più pervasivo, stiano progressivamente assumendo il controllo della regolamentazione dei nuovi ambienti di vita; b) *culturale*, con un focus sulle forme di fragilità che interessano le e gli adolescenti, che possono non soltanto compromettere il diritto fondamentale alla salute, inteso in senso ampio come diritto a una "vita sana" e al "benessere", ma anche sfociare in forme di anomia e generare comportamenti devianti, come il cyberbullismo, portando a processi di colpevolizzazione di soggetti che, in realtà, sono afflitti da un profondo vuoto normativo; c) *etico*, lungo il quale approfondire alcune delle problematiche sollevate dalle tecnologie digitali che influenzano il discorso pubblico, i processi decisionali, educativi e formativi; d) *governativo*, nel tentativo di far emergere il debole riferimento a infanzia e adolescenza nella recente regolamentazione giuridica, soprattutto europea, e comprenderne le ragioni.

Alla parte di analisi seguono le domande sui possibili interventi. Una risposta è nell'impiego di strumenti adeguati (anche di carattere tecnologico) al livello della formazione, che possano intervenire sia sulle forme di fragilità provocate dall'esposizione alle tecnologie digitali, prevenendo disagio e anomia, sia sull'uso consapevole nella fruizione delle nuove tecnologie. L'altra risposta è in una più accurata attenzione da parte del legislatore circa la nuova realtà che interessa i minori, tanto in termini di cura e promozione del libero sviluppo della persona e delle diverse specificità umane, quanto di individuazione e controllo dell'impatto dei sistemi che governano questi ambienti di vita sui diritti dei minori, esposti a problemi di sicurezza, governance e giustizia dei dati, discriminazione algoritmica, responsabilità, e sempre più a sottili forme di influenza e manipolazione.

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

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.

Cittadinanza digitale e minori

Digital Citizenship and Minors

Giovanni Pascuzzi [1]

Sommario

Dopo aver definito le nozioni di (i) cittadinanza digitale, (ii) spazio digitale, (iii) divario digitale e (iv) competenze digitali, il saggio si propone di individuare i problemi giuridici posti dall'uso delle tecnologie digitali da parte dei minori. In particolare, viene esposto un piccolo inventario dei principali diritti e doveri che sorgono in conseguenza dell'esercizio della cittadinanza digitale da parte dei minori focalizzando infine l'attenzione sulla necessità, per i minori, di saper essere cittadini digitali.

Parole chiave: Minori, Spazio digitale, Cittadinanza digitale, Diritti e doveri, Competenze digitali

Abstract

After defining the concepts of (i) digital citizenship, (ii) digital space, (iii) digital divide, and (iv) digital skills, this essay aims to identify the legal challenges posed by minors' use of digital technologies. Specifically, it presents a concise inventory of the main rights and duties that emerge as a result of minors exercising digital citizenship, ultimately focusing on the need for minors to develope the ability of being digital citizens.

Keywords: Minors, Digital Space, Digital Citizenship, Rights and Duties, Digital Literacy

1. La cittadinanza digitale

Tradizionalmente il concetto di cittadinanza individua il nesso che lega un individuo ad un ordine costituito mettendone a fuoco le sue principali articolazioni: aspettative e pretese, diritti e doveri, modalità di appartenenza e di differenziazione, strategie di inclusione e di esclusione.

1 Consiglio di Stato. Già Facoltà di Giurisprudenza, Università di Trento. postmaster@giovannipascuzzi.eu

Data invio: 5 agosto 2025. Data accettazione: 4 ottobre 2025.
DOI: https://doi.org/10.54103/1972-5760/30049

Con l'avvento dell'era digitale (Pascuzzi 2025) si è cominciato a parlare di "cittadinanza digitale" (Pascuzzi 2021).

Per il Consiglio d'Europa la cittadinanza digitale è "la capacità di partecipare attivamente, in maniera continuativa e responsabilmente alla vita della comunità (locale, nazionale, globale, online e offline) a tutti i livelli (politico, economico, sociale, culturale e interculturale)". Il Consiglio d'Europa definisce cittadino digitale la "persona che possiede le competenze per la cultura democratica così da essere in grado di impegnarsi in modo competente e positivo con le tecnologie digitali in evoluzione; di partecipare attivamente, continuamente e responsabilmente alle attività sociali e civiche; di essere coinvolto in un processo di apprendimento permanente (in contesti formali, informali e non formali) e di impegnarsi a difendere continuamente i diritti umani e la dignità"[2].

Per l'Unione europea "la cittadinanza digitale è un insieme di valori, competenze, atteggiamenti, conoscenze e comprensione critica di cui i cittadini hanno bisogno nell'era digitale. Un cittadino digitale sa come utilizzare le tecnologie ed è in grado di interagire con esse in modo competente e positivo"[3].

Per quel che riguarda l'Italia, non abbiamo una definizione esplicita di cittadinanza digitale sul piano giuridico. Cionondimeno essa compare nel nostro ordinamento in una pluralità di significati.

Il Codice dell'amministrazione digitale (d. lgs. 82/2005 - CAD) intitola la sezione II del capo I alla "Carta della cittadinanza digitale". Detta sezione si apre con l'articolo 3 che riconosce il diritto all'uso delle tecnologie, ovvero riconosce a chiunque il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti del Codice nei rapporti con le pubbliche amministrazioni e i gestori di pubblici servizi anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo. La Carta della cittadinanza digitale comprende altri aspetti che vanno dalla effettuazione di pagamenti in modalità informatica (art. 5) al diritto a servizi online semplici e integrati (art. 7); dalla alfabetizzazione informatica dei cittadini (art. 8) alla partecipazione democratica elettronica (art. 9).

Si deve anche ricordare che la cittadinanza digitale ha formato oggetto, di recente, di un altro intervento normativo: la legge 20 agosto 2019, n. 92 (introduzione dell'insegnamento scolastico dell'educazione civica). L'articolo 5 di detta legge prevede che l'educazione alla cittadinanza digitale sia parte dell'insegnamento trasversale dell'educazione civica (reso obbligatorio sin dalla scuola dell'infanzia).

2 Recommendation CM/Rec (2019) 10 of the Committee of Ministers to member States on developing and promoting digital citizenship education.

3 Conclusioni del Consiglio sull'istruzione digitale nelle società della conoscenza europee 2020/C 415/10, nota 7.

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

Il concetto di cittadinanza digitale ha a che fare con l'esistenza di strumenti, l'accesso concreto ad essi, il possesso delle competenze necessarie per adoperarli, la titolarità di diritti e doveri, la partecipazione alla vita politica e alle scelte collettive, ed altro ancora. Un concetto, quindi, molto ampio e in continua evoluzione.

2. Lo spazio digitale e i minori

Internet è lo strumento principale che rende possibile l'esercizio della cittadinanza digitale. Internet è quindi un mezzo che finisce, però, con il diventare anche un luogo.

Una delle caratteristiche della rete Internet è il suo disancoraggio dallo spazio fisico ovvero il suo carattere aterritoriale. Se acquistiamo un bene in un negozio individuiamo con facilità i soggetti che concludono il contratto e il diritto applicabile. Molto più difficile capire le stesse circostanze in una transazione online: non sappiamo con certezza chi sia il venditore, dove sia nel mondo reale, quali server vengano coinvolti, quale diritto regoli il contratto, quale giudice dovrà decidere le controversie che dovessero insorgere.

Si è diffusa la convinzione che la rete abbia creato una sorta di mondo parallelo con proprie regole (o, addirittura, senza regole). Per individuare questo mondo si usano espressioni come "cyberspazio" o "spazio telematico", o, ancora "spazio cibernetico".

La cittadinanza digitale si sviluppa in questo spazio parallelo. Uno spazio creato dalla tecnologia che deriva da essa più di un profilo di vulnerabilità.

Seppur creata ed usata prevalentemente dagli adulti per le più svariate attività (usi economici e imprenditoriali: si pensi ai nuovi modelli di business o alla nascita dei grandi player della rete che hanno assunto un potere economico molto significativo, o, ancora, allo smart working; usi sociali: si pensi alle reti sociali virtuali; usi istituzionali: si pensi alla digitalizzazione della pubblica amministrazione; usi politici: si pensi ai cosiddetti partiti virtuali e al voto elettronico; usi formativi: si pensi alla didattica a distanza) Internet viene adoperata in maniera massiva anche dai minori (Alfieri 2022).

Scopo di questo articolo è di scandagliare la disciplina emanata a livello sovranazionale, europeo ed italiano che si occupa del rapporto tra cittadinanza digitale e minori (Maestri 2017).

3. La Dichiarazione comune sui diritti e i principi digitali per il decennio digitale

Redigere un inventario di tutte le problematiche giuridiche innescate dall'esercizio della cittadinanza digitale da parte di minori è tutt'altro che agevole[4] (Vizzoni 2025).

Un significativo punto di partenza è rappresentato dalla "Dichiarazione comune sui diritti e i principi digitali per il decennio digitale" solennemente proclamata, a gennaio del 2023, dal Parlamento europeo, dal Consiglio e dalla Commissione[5].

I principi della Dichiarazione si articolano attorno a 6 temi: (i) Mettere le persone al centro della trasformazione digitale; (ii) Solidarietà e inclusione; (iii) Libertà di scelta; (iv) Partecipazione allo spazio pubblico digitale; (v) Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità; (vi) Sostenibilità.

Nell'esplicitare i contenuti di tali punti, i firmatari hanno fatto riferimento anche alle tematiche giuridiche connesse alla trasformazione digitale indicando le azioni da attivare e, spesso, anche i nuovi diritti che devono essere riconosciuti.

La Dichiarazione dedica delle indicazioni precise relativamente ai minori.

In particolare, nel Capitolo V, dedicato a "Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità" si legge testualmente quanto segue:

> Protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale.
> 20. I bambini e i giovani dovrebbero essere messi nelle condizioni di compiere scelte sicure e informate e di esprimere la propria creatività nell'ambiente digitale.
> 21. Si dovrebbero migliorare le esperienze, il benessere e la partecipazione all'ambiente digitale dei bambini e dei giovani attraverso materiali e servizi adeguati all'età.
> 22. Occorre prestare particolare attenzione al diritto dei bambini e dei giovani di essere protetti da tutti i reati commessi attraverso le tecnologie digitali o facilitati da tali tecnologie.
> Ci impegniamo a:

4 In prima approssimazione si può vedere il Commento generale n. 25 sui diritti dei minorenni in relazione all'ambiente digitale, adottato dal Comitato delle Nazioni Unite sui Diritti dell'Infanzia durante la sua 86° Sessione (18 gennaio - 5 febbraio 2021).

5 Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, in GUCE del 23 gennaio 2023, C23/1. L'obiettivo della Dichiarazione è promuovere un modello europeo per la trasformazione digitale, che metta al centro le persone, sia basato sui valori europei e sui diritti fondamentali dell'UE, riaffermi i diritti umani universali e apporti benefici a tutte le persone, alle imprese e alla società nel suo complesso.

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

a) offrire a tutti i bambini e i giovani opportunità per acquisire le necessarie capacità e competenze, tra cui l'alfabetizzazione mediatica e il pensiero critico, per navigare e interagire nell'ambiente digitale in modo attivo e sicuro e per compiere scelte informate;
b) promuovere esperienze positive per i bambini e i giovani in un ambiente digitale sicuro e adeguato all'età;
c) proteggere tutti i bambini e i giovani dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi online e impedire che lo spazio digitale sia utilizzato per commettere o facilitare reati;
d) proteggere tutti i bambini e i giovani dal tracciamento, dalla profilazione e dal targeting illegali, in particolare a fini commerciali;
e) coinvolgere i bambini e i giovani nell'elaborazione delle politiche digitali che li riguardano".
Nella Comunicazione "Un decennio digitale per bambini e giovani", la Commissione aveva già delineato una strategia utile a perseguire gli obiettivi appena ricordati[6].

4. La formazione dei minori sulle competenze digitali

Uno studio pubblicato a febbraio 2024, promosso dal Ministero delle Imprese e Made in Italy con la collaborazione scientifica dell'Università Cattolica, ha rilevato che sette ragazzi su dieci usano regolarmente i social media e le piattaforme streaming[7]. Quattro intervistati su dieci raccontano esperienze negative gravi e ripetute (il 42% dei minori e il 53% degli adolescenti dai 13 anni). La maggioranza degli intervistati ha visto contenuti inadatti almeno una volta di recente sulle piattaforme di social media. L'uso della rete espone al rischio di essere vittima di fenomeni come il cyberbullismo (Giarda, Liotta e Spagnuolo 2022).

Essere nativi digitali non significa automaticamente saper andare al di là della mera capacità di cliccare sullo schermo.

L'uso delle tecnologie digitali richiede una preparazione specifica. Una preparazione certamente tecnica, ma anche civile, giuridica, emotiva, comunicativa e valoriale.

Con l'espressione *digital divide* (e quelle ad essa simili come "divario digitale" e "diseguaglianze digitali") si suole indicare la distribuzione non uniforme delle tecnologie dell'informazione e della comunicazione (TIC)

6 Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, "Un decennio digitale per bambini e giovani: la nuova strategia europea per un'internet migliore per i ragazzi (BIK+)", Bruxelles, 11.5.2022 COM (2022) 212 final.

7 https://www.mimit.gov.it/it/notizie-stampa/consumo-dei-media-digitali-e-comportamenti-dei-minori-presentati-i-risultati-della-ricerca-promossa-dal-mimit-con-la-collaborazione-scientifica-delluniversita-cattolica-di-milano.

nella società. L'OECD ha chiarito che il *digital divide* individua il divario esistente tra individui, famiglie, imprese e aree geografiche a diversi livelli socio-economici con riferimento tanto alle opportunità di accedere alle tecnologie dell'informazione e della comunicazione quanto all'uso di Internet per un'ampia varietà di attività[8]. Ma anche il mero accesso alla tecnologia non è sufficiente se non si è in grado di tradurre il proprio accesso a Internet in risultati favorevoli.

La Raccomandazione del Consiglio dell'Unione Europea del 22 maggio 2018 è dedicata alle competenze chiave per l'apprendimento permanente.

Tra le 8 competenze chiave ivi individuate, figura anche la competenza digitale rispetto alla quale la Raccomandazione afferma quanto segue:

> La competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cibersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.

L'espressione "competenza digitale" indica la capacità di saper usare con dimestichezza e spirito critico le tecnologie della società dell'informazione (Ricci 2024). Il ricorso al concetto di competenza sintetizza il possesso di tre specifiche dimensioni del sapere: a) l'alfabetizzazione digitale, ovvero la conoscenza quanto meno degli aspetti di base del sapere informatico (teorico e procedurale) necessario per utilizzare le tecnologie digitali; b) le abilità digitali ovvero il complesso di skills cognitive, metacognitive, sociali, emotive e pratiche che permettono di interagire al meglio con le tecnologie digitali; c) il saper essere cittadini digitali, ovvero la padronanza di valori ed attitudini che consentono di usare responsabilmente alfabetizzazione e abilità digitali.

L'Unione Europea ha varato il progetto DIGCOMP con l'obiettivo di enucleare le competenze digitali dei cittadini[9].

Di seguito si elencano le competenze digitali elaborate dai responsabili del progetto DIGCOMP.

a. Alfabetizzazione dell'informazione e dei dati. Articolare le esigenze di informazione, individuare e recuperare dati, informazioni e contenuti digitali. Giudicare la rilevanza della fonte e del suo contenuto. Archiviare, gestire e organizzare dati digitali, informazioni e contenuti.

8 Understanding the Digital Divide, OECD Digital Economy Papers, No. 49, OECD Pub, 2001.

9 Https://joint-research-centre.ec.europa.eu/digcompen.

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

b. Comunicazione e collaborazione. Interagire, comunicare e collaborare attraverso le tecnologie digitali, pur essendo consapevoli della diversità culturale e generazionale. Partecipare alla società attraverso servizi digitali pubblici e privati e cittadinanza partecipativa. Gestire la propria presenza digitale, identità e reputazione.

c. Creazione di contenuti digitali. Creare e modificare contenuti digitali per migliorare e integrare informazioni e contenuti in un corpus esistente di conoscenze, comprendendo al contempo come devono essere applicati i diritti d'autore e le licenze. Sapere come dare istruzioni comprensibili per un sistema informatico.

d. Sicurezza. Proteggere dispositivi, contenuti, dati personali e privacy in ambienti digitali. Proteggere la salute fisica e psicologica ed essere consapevoli delle tecnologie digitali per il benessere sociale e l'inclusione sociale. Essere consapevoli dell'impatto ambientale delle tecnologie digitali e del loro utilizzo.

e. Risoluzione dei problemi. Identificare i bisogni e i problemi e risolvere i problemi concettuali e le situazioni problematiche in ambienti digitali. Utilizzare strumenti digitali per innovare processi e prodotti. Rimanere aggiornati sull'evoluzione digitale.

L'articolo 8 del Codice dell'amministrazione digitale (d.lgs. 82/2005: CAD) impone allo Stato e alle pubbliche amministrazioni di promuovere iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo.

5. I minori e l'identità digitale

L'esercizio delle prerogative proprie della cittadinanza digitale comporta l'utilizzo di nuovi strumenti essi stessi figli della rivoluzione tecnologica.

Si pensi alla necessità di essere identificati online oppure alla necessità di attivare una procedura di autenticazione online (ad esempio, per accedere ad un social network).

L'ordinamento (per l'Italia v. il d.p.r. 445/2000) individua gli strumenti grazie ai quali è possibile effettuare l'identificazione personale: come esempi si possono citare il documento di riconoscimento oppure il documento di identità.

Norme specifiche sono state emanate per disciplinare l'identificazione digitale dei minori.

L'articolo 3-*bis* del già citato Codice dell'amministrazione digitale riconosce il diritto all'identità digitale. La disposizione prevede il diritto di chiunque di accedere ai servizi online offerti dalle pubbliche amministrazioni e dai gestori di servizi pubblici utilizzando un sistema di identificazione elettronica, come lo SPID (Sistema Pubblico di Identità Digitale) o la Carta di Identità Elettronica (CIE), nonché tramite la c.d. "app IO" (punto di accesso telematico di cui all'art. 64-*bis* CAD).

Il sistema SPID è costituito come un insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, identificano gli utenti per consentire loro il compimento di attività e l'accesso ai servizi in rete.

L'AgID (Agenzia per l'Italia Digitale, ha adottato il 3 marzo 2022, le "Linee guida operative per la fruizione dei servizi SPID da parte dei minori" (Ricciulli 2024). Le citate Linee guida premettono che "la normativa vigente consente la creazione dell'identità digitale in favore di tutti i cittadini. Risulta evidente, tuttavia, la necessità di una tutela specifica per un soggetto fragile come il minore" e spiegano che con l'identità digitale dei minori si mira a garantire il raggiungimento dei seguenti obiettivi: (i) consentire ai minori di acquisire la propria identità digitale, previa richiesta da parte di chi esercita la responsabilità genitoriale; (ii) consentire al minore di fruire autonomamente di servizi online mediante la propria identità digitale, ferma restando - salvo casi specifici - la possibilità di autorizzazione e verifica da parte dell'esercente la responsabilità genitoriale; (iii) consentire ai fornitori di servizi in rete la selezione dei propri utenti in base all'età. Le Linee guida consentono l'utilizzo di SPID, con riferimento ai minori infra quattordicenni, unicamente a partire dai cinque anni e per la fruizione dei soli servizi online erogati dagli istituti scolastici di ogni ordine e grado.

La Carta di identità elettronica (CIE). È il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare[10].

La CIE può essere rilasciato ai cittadini italiani minorenni fin dalla nascita. I minori possono richiedere il documento valido per l'espatrio se entrambi i genitori sono presenti al momento dell'emissione della CIE. La carta d'identità per minori ha le seguenti validità: 3 anni per i minori di 3 anni; 5 anni per i minori di età compresa fra 3 e 18 anni. A partire dai 12 anni compiuti al minore sono rilevate due impronte digitali e dovrà appore la propria firma grafica sul documento. Per i minori di 14 anni è possibile richiedere anche l'indicazione dei nomi dei genitori, o di chi ne fa le veci, sul retro del documento[11].

10 CAD, artt. 1, lett. c, e 66: https://www.cartaidentita.interno.gov.it/.

11 https://www.cartaidentita.interno.gov.it/richiedi/rilascio-e-rinnovo-minorenni/

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

6. I diritti di cittadinanza digitale dei minori

Come ricordato in apertura, la cittadinanza comporta, per definizione, la titolarità di diritti. Basti citare alcune libertà riconosciute dalla Costituzione come la libertà di informazione (diritto ad informare e ad essere informati). Le tecnologie digitali offrono nuovi spazi all'esercizio di queste libertà spesso schiudendo opportunità impensabili prima (si pensi alla possibilità di comunicare in tempo reale con tantissimi individui offerta dai social network come Facebook e Twitter).

Di seguito saranno analizzati alcuni dei diritti di cittadinanza digitale spettanti ai minori.

6.1 Il diritto di accesso allo spazio digitale e la libertà di espressione

Per poter usufruire delle opportunità offerte dalle tecnologie digitali e dalla rete in particolare è necessario innanzitutto garantire l'accesso a quello che abbiamo definito spazio digitale.

L'articolo 3 del regolamento UE 2015/2120 così recita[12]:

> Gli utenti finali hanno il diritto di accedere a informazioni e contenuti e di diffonderli, nonché di utilizzare e fornire applicazioni e servizi, e utilizzare apparecchiature terminali di loro scelta, indipendentemente dalla sede dell'utente finale o del fornitore o dalla localizzazione, dall'origine o dalla destinazione delle informazioni, dei contenuti, delle applicazioni o del servizio, tramite il servizio di accesso a Internet.

Ovviamente una cosa è garantire l'accesso alla rete, altra cosa è l'attività che sulla rete ciascuno di noi compie. Lo stesso regolamento (UE) 2015/2120 (art. 3, par. 1, comma 2) chiarisce che la salvaguardia del diritto di accesso non pregiudica il diritto dell'Unione, o il diritto nazionale conforme al diritto dell'Unione, relativo alla legittimità dei contenuti, delle applicazioni o dei servizi (si pensi a fenomeni come l'*hate speech* o le *fake news*.

Proprio perché consapevoli dell'importanza di garantire l'accesso alla rete (che è anche la premessa per scongiurare il sorgere del *digital divide*) non mancano proposte per introdurre una tutela costituzionale del diritto di accesso ad Internet.

12 Regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio del 25 novembre 2015 che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione (Testo rilevante ai fini del SEE).

L'accesso alla rete (e in particolare alle piattaforme online) acquista connotati particolari con riferimento ai minori.

Conviene preliminarmente ricordare che la Convenzione sui diritti dell'infanzia e dell'adolescenza (fatta a New York il 20 novembre 1989 e ratificata dall'Italia con la legge 27 maggio 1991, n. 176) stabilisce che "Il fanciullo ha diritto alla libertà di espressione. Questo diritto comprende la libertà di ricercare, di ricevere e di divulgare informazioni ed idee di ogni specie, indipendentemente dalle frontiere, sotto forma orale, scritta, stampata o artistica, o con ogni altro mezzo a scelta del fanciullo".

La rete ben può essere considerato un "mezzo" scelto dal fanciullo per esprimersi[13].

La normativa vigente stabilisce dei limiti di età per ritenere valido il cosiddetto "consenso digitale" che finisce per costituire la soglia per operare sulla rete.

La fissazione di tale limite si giustifica in ragione dei rischi che bambini e adolescenti corrono navigando in rete: dipendenza da Internet (European Centre for Algorithmic Transparency roundtables 2025); esposizione a fenomeni di cyberbullismo e, in generale, contenuti violenti o inadatti; rischi legati alla privacy dei minori (Garaci 2023), in quanto le informazioni raccolte possono essere utilizzate per orientare i consumi e gli stili di vita o possono essere riutilizzate per la produzione di materiale pedopornografico; cyber attacchi.

Proprio dalla disciplina in materia di dati personali arrivano indicazioni significative sul punto.

Il Considerando n. 38 del Regolamento generale sulla protezione dei dati (UE) 2016/679 (GDPR)[14] così recita:

> I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze

13 Secondo l'art. 12.1 della Convenzione "Gli Stati parti garantiscono al fanciullo capace di discernimento il diritto di esprimere liberamente la sua opinione su ogni questione che lo interessa, le opinioni del fanciullo essendo debitamente prese in considerazione tenendo conto della sua età e del suo grado di maturità".

L'art. 14 della Convenzione a propria volta così recita: "Gli Stati parti rispettano il diritto del fanciullo alla libertà di pensiero, di coscienza e di religione. Gli Stati parti rispettano il diritto ed il dovere dei genitori oppure, se del caso, dei rappresentanti legali del bambino, di guidare quest'ultimo nello esercizio del summenzionato diritto in maniera che corrisponda allo sviluppo delle sue capacità. La libertà di manifestare la propria religione o convinzioni può essere soggetta unicamente alle limitazioni prescritte dalla legge, necessarie ai fini del mantenimento della sicurezza pubblica, dell'ordine pubblico, della sanità e della moralità pubbliche, oppure delle libertà e diritti fondamentali dell'uomo".

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

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

> e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore[15].

Il GDPR stabilisce che in caso di trattamento basato sul consenso, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, questo può essere fornito direttamente solo a partire dai 16 anni ma lascia agli Stati Membri dell'UE la possibilità di stabilire un'età inferiore purché non al di sotto dei 13 anni.

In Italia il limite è fissato a 14 anni, come stabilito dall'art. 2-*quinquies* del d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali)[16].

L'articolo 8 del GDPR fissa una regolamentazione specifica che, però, non tocca la capacità di agire del minore, che rimane quella fissata dall'ordinamento nazionale. L'articolo 8 si applica solo quando il trattamento dei dati: (i) concerna un'offerta diretta di servizi della società dell'informazione a soggetti minori che hanno almeno 16 anni (o, secondo l'art. 8, una diversa età fissata dal legislatore nazionale); (ii) sia basato sul consenso, secondo quanto disposto dall'art 6, comma 1, lett. a del GDPR[17].

Laddove manchino questi due requisiti, l'art. 8 richiede il consenso dell'esercente la responsabilità genitoriale[18].

---

15 A propria volta il successivo Considerando n. 58 del medesimo regolamento così recita: «Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente».

16 L'articolo 2- (Consenso del minore in relazione ai servizi della società dell'informazione) del d.lgs. 30/06/2003, n. 196 così recita: "1. In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale. 2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi".

17 Se il trattamento ha altra base giuridica, come ad esempio il rispetto di un obbligo di legge, i legittimi interessi, ecc., l'art. 8 GDPR non si applica.

18 Restano comunque salve, a norma del terzo comma dell'art. 8 GDPR le disposizioni nazionali in tema di diritto dei contratti (quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore).

Si tratta quindi di una sorta di maggiore età digitale, raggiunta la quale è ammesso il consenso al trattamento dei propri dati personali anche ad es. con riferimento ad attività di profilazione.

6.1.1 (segue) La verifica dell'età

Problema ulteriore è quello relativo all'onere di controllo sulla veridicità dei dati anagrafici forniti dall'utente al prestatore di servizi on line (Barozzi Reggiani e Vaccari 2025).

Il tema acquista specifica rilevanza quando viene in rilievo l'obiettivo di proteggere i minori dall'accesso a contenuti non adatti alla loro età (si anticipa qui un aspetto di un tema che sarà ripreso più avanti).

Alcune disposizioni normative prescrivono precisi oneri, sotto questo profilo.

Il comma 7, dell'articolo 42, del d.lgs. 8 novembre 2021 n. 208[19] impone ai fornitori di piattaforma per la condivisione di video sono in ogni caso tenuti a predisporre sistemi per verificare, nel rispetto della normativa in materia di protezione dei dati personali, l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori[20].

Il comma 2, dell'art. 13-*bis* della legge 159/2023[21], a propria volta, impone ai gestori di siti web e ai fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, di

19 Decreto legislativo 8 novembre 2021 n. 208. Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato.

20 Per "servizio di piattaforma per la condivisione di video" si intende: un servizio, quale definito dagli articoli 56 e 57 del Trattato sul funzionamento dell'Unione europea, ove l'obiettivo principale del servizio stesso, di una sua sezione distinguibile o di una sua funzionalità essenziale sia la fornitura di programmi o video generati dagli utenti destinati al grande pubblico, per i quali il fornitore della piattaforma per la condivisione di video non ha responsabilità editoriale, al fine di informare, intrattenere o istruire attraverso reti di comunicazioni elettroniche ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, e la cui organizzazione è determinata dal fornitore della piattaforma per la condivisione di video, anche con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di tag e sequenziamento (art. 3, comma 1, lett. c del d.lgs. 208/2021).

21 Legge 13 novembre 2023 n. 159 (Conversione in legge, con modificazioni, del decreto-legge 15 settembre 2023, n. 123, recante misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale).

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

verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto.

In attuazione delle norme citate, l'Autorità per le Garanzie nelle Comunicazioni (AGCOM) ha adottato la delibera n. 96/25/CONS recante "Adozione delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge 13 novembre 2023, n. 159".

Nella delibera AGCOM appena cita si ricorda che uno studio elaborato da un gruppo di esperti creato dalla Commissione Europea ha così sintetizzato le metodologie di verifica dell'età attualmente utilizzate:

(i) Autodichiarazione: gli utenti dichiarano la propria età/fascia di età senza fornire altre prove.

(ii) Identificatori rigidi: gli utenti forniscono documenti di identità verificati (ad esempio passaporto) per dimostrare la loro età.

(iii) Carte di credito: utilizzo dei dati della carta di credito per verificare che un utente abbia più di 18 anni.

(iv) Identità basata su *blockchain*: utilizzo di tecnologie decentralizzate come *blockchain* per creare identità digitali degli utenti, per utilizzare tali identità per l'*age verification*.

(v) Conferma del titolare del conto: basarsi sulla conferma di un titolare di conto verificato esistente che un altro utente ha l'età richiesta per utilizzare la piattaforma.

(vi) Autenticazione multipiattaforma: utilizzo di account utente già esistenti con piattaforme di grandi dimensioni (ad esempio Google, Apple ecc.) per autenticare l'età di un utente per altri prodotti/servizi.

(vii) Stima del viso: utilizzo dell'intelligenza artificiale per analizzare le caratteristiche del viso di una persona per stimarne l'età.

(viii) Profilazione comportamentale: utilizzo dell'intelligenza artificiale per analizzare l'attività online degli utenti per stimarne l'età.

(ix) Test di capacità: testare la capacità o l'attitudine dell'utente per stimare l'età.

(x) Servizi di assicurazione sull'età di terze parti: utilizzo di società terze per i servizi di assicurazione sull'età. Le terze parti potrebbero utilizzare uno qualsiasi degli altri metodi per la garanzia dell'età.

6.2 Il diritto dei minori ad un ambiente digitale sicuro e adeguato all'età

Come si è detto, Internet e in particolare le piattaforme online sono sempre più usate dai minori che possono trarre vantaggio dalle loro potenzialità. Allo stesso tempo, però, l'attività svolta in rete espone i minori a rischi significativi.

L'Organizzazione per la cooperazione e lo sviluppo economico (OECD 2021) ha classificato per categorie i rischi a cui i minori sono esposti, ovvero:

(i) Rischi legati ai contenuti. I minori possono essere esposti in modo inaspettato e involontario a contenuti potenzialmente dannosi per loro: a. contenuti che incitano all'odio; b. contenuti dannosi; c. contenuti illegali; d. disinformazione. Questi tipi di contenuti sono ampiamente considerati come aventi gravi conseguenze negative sulla salute mentale e sul benessere fisico dei minori, ad esempio contenuti che promuovono l'autolesionismo, il suicidio, i disturbi alimentari o la violenza estrema.

(ii) Rischi legati alla condotta. Fanno riferimento ai comportamenti che i minori potrebbero adottare attivamente online e che possono rappresentare un rischio per sé stessi e per gli altri, come a. comportamenti d'odio (ad esempio, minori che pubblicano/inviano contenuti/messaggi d'odio); b. comportamenti dannosi (ad esempio, minori che pubblicano/inviano contenuti violenti o pornografici); c. comportamenti illegali (ad esempio, minori che pubblicano/inviano materiale pedopornografico o contenuti terroristici); e d. comportamenti problematici generati dall'utente (ad esempio, partecipazione a sfide pericolose; *sexting*).

(iii) Rischi legati ai contatti. Si riferiscono a situazioni in cui i minori sono vittime delle interazioni, in contrapposizione all'autore: a. incontri motivati dall'odio; b. incontri dannosi (ad esempio, l'incontro avviene con l'intenzione di danneggiare il minore); c. incontri illegali (ad esempio, possono essere perseguiti penalmente); e d. altri incontri problematici. Esempi di rischi di contatto includono, a titolo esemplificativo ma non esaustivo, adescamento online, coercizione ed estorsione sessuale online, abuso sessuale tramite webcam, cyberbullismo e tratta di esseri umani a scopo di sfruttamento sessuale. Questi rischi si estendono anche a pratiche di frode online come phishing, frodi sui marketplace e furto di identità.

(iv) Rischi per i consumatori. I minori possono anche affrontare rischi in quanto consumatori nell'economia digitale: a. rischi di marketing (ad esempio, loot box, advergame); b. rischi di profilazione commerciale (ad esempio, product placement o ricezione di pubblicità destinate ad adulti, come servizi di incontri); c. rischi finanziari (ad esempio, frodi o spese di ingenti somme di denaro senza la conoscenza o il consenso dei tutori); d. rischi per la sicurezza ed e. rischi legati all'acquisto e al consumo di droghe, medicinali, alcol e altri prodotti illegali o pericolosi. I rischi per i consumatori includono anche i rischi relativi ai contratti, ad esempio la vendita dei dati degli utenti o termini e condizioni iniqui.

(v) Rischi trasversali: si tratta di rischi che interessano tutte le categorie di rischio e sono considerati altamente problematici in quanto possono avere effetti significativi sulla vita dei minori in diversi modi. Si tratta di: a) I rischi legati alle tecnologie avanzate implicano che i minori incontrino nuovi pericoli con l'evoluzione della tecnologia, come i chatbot basati sull'intelligenza

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

artificiale che potrebbero fornire informazioni dannose o essere utilizzati per l'adescamento sfruttando le vulnerabilità, o l'uso di tecnologie biometriche che possono portare ad abusi, furti di identità ed esclusione; b) I rischi per la salute e il benessere includono potenziali danni al benessere mentale, emotivo o fisico dei minori. Ad esempio, l'aumento di obesità/anoressia e problemi di salute mentale legati all'uso o all'uso eccessivo di piattaforme online, che in alcuni casi possono avere effetti negativi sulla salute e il benessere fisico e mentale dei minori, come dipendenza, depressione, disturbi d'ansia, disturbi del sonno e isolamento sociale; c) Ulteriori rischi per la privacy e la protezione dei dati derivano dall'accesso alle informazioni sui minori e dal pericolo rappresentato dalle caratteristiche di geolocalizzazione che i predatori potrebbero sfruttare per localizzare e avvicinare i minori; d) Ulteriori rischi per la sicurezza riguardano la sicurezza dei minori, in particolare quella fisica, nonché tutte le problematiche relative alla sicurezza informatica; e) I rischi di abuso riguardano rischi o danni per i minori derivanti dall'uso improprio della piattaforma online o delle sue funzionalità[22].

6.2.1 Esempi di norme tese ad assicurare un ambiente digitale sicuro. Il Digital Service Act

La normazione eurounitaria e nazionale contiene numerosi esempi di norme che mirano a tutelare i minori. Un primo esempio è costituito dal *Digital Service Act.*

L'articolo 28 del regolamento UE sui servizi digitali (Digital Service Act) così recita[23]:

> Protezione online dei minori
> 1. I fornitori di piattaforme online[24] accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio.

22 Le definizioni riportate nel testo sono riprese dall'allegato alla Communication to the Commission, Approval of the content on a draft Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, Brussels, 14.7.2025, C(2025) 4764 final, pag. 62 e ss.

23 Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

24 Per "piattaforma online" si intende : "un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale

> 2. I fornitori di piattaforme online non presentano sulla loro interfaccia pubblicità basata sulla profilazione come definita all'articolo 4, punto 4), del regolamento (UE) 2016/679 che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore.
> 3. Il rispetto degli obblighi di cui al presente articolo non obbliga i fornitori di piattaforme online a trattare dati personali ulteriori per valutare se il destinatario del servizio sia minore.
> 4. La Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme online nell'applicazione del paragrafo 1.

In adempimento di quanto previsto dal comma 4 della norma appena citata, a luglio 2025 la Commissione[25] ha elencato le raccomandazioni principali rivolte ai fornitori di piattaforme online che sono:

- impostare gli account dei minori in privato per impostazione predefinita in modo che le loro informazioni personali, i dati e i contenuti dei social media siano nascosti a quelli con cui non sono collegati;
- modificare i sistemi di raccomandazione delle piattaforme per ridurre il rischio che i bambini incontrino contenuti dannosi;
- consentire ai bambini di bloccare e disattivare qualsiasi utente e garantire che non possano essere aggiunti ai gruppi senza il loro esplicito consenso;
- proibire agli account di scaricare o scattare schermate di contenuti pubblicati da minori per impedire la distribuzione indesiderata di contenuti sessualizzati o intimi e l'estorsione sessuale;
- disabilitare per impostazione predefinita le funzionalità che contribuiscono a un uso eccessivo;
- garantire che la mancanza di alfabetizzazione commerciale dei bambini non sia sfruttata e che non siano esposti a pratiche commerciali che possono essere manipolative, portare a spese indesiderate o comportamenti di dipendenza;
- introdurre misure per migliorare gli strumenti di moderazione e comunicazione, che richiedono un feedback tempestivo, e requisiti minimi per gli strumenti di controllo parentale.

6.2.2 La lotta al cyberbullismo

La rete e i social network possono amplificare a dismisura il fenomeno del bullismo e i suoi effetti devastanti. Il legislatore italiano è intervenuto a

funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento": cfr. art. 3, comma 1, lett. i) del regolamento 2022/2065.

25 Communication to the Commission, Brussels, 14.7.2025, C (2025) 4764 final, cit.

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

porre un argine a questo tipo di devianza emanando la legge 29 maggio 2017, n. 71, modificata e integrata con la successiva legge 17 maggio 2024, n. 176 (Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo). Si tratta di una legge che mira a prevenire il problema facendo leva soprattutto sulla formazione (Zanovello 2024).

L'art. 1, comma 2, della legge 71/2017 definisce "cyberbullismo qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

6.2.3 La tutela tecnologica: il parental control

La tecnologia espone i minori ai rischi ricordati. Ma la stessa tecnologia può offrire una protezione.

Un esempio è costituito dai meccanismi che consentono di verificare l'età della persona (di cui si è già parlato.

Un altro esempio è rappresentato dal "*parental control*" (Biligotti 2023).

L'art. 7 del d.l. 30/04/2020, n. 28[26] (rubricato "Sistemi di protezione dei minori dai rischi del cyberspazio", stabilisce che i contratti di fornitura nei servizi di comunicazione elettronica devono "prevedere tra i servizi preattivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto".

In attuazione della norma citata AGCOM ha emanato la Delibera 9/23/CONS recante Adozione delle linee guida finalizzate all'attuazione dell'articolo 7-*bis* del decreto-legge 30 aprile 2020, n. 28 in materia di "sistemi di protezione dei minori dai rischi del cyberspazio"

26 Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19. L'articolo citato nel testo è stato inserito dalla legge di conversione 25 giugno 2020, n. 70.

Si veda anche l'art. 42, comma 7, del d.lgs. 208/2021 (già citato a proposito della verifica dell'età) a mente del quale "i fornitori di piattaforma per la condivisione di video sono in ogni caso tenuti a: [omissis] h) dotarsi di sistemi di controllo parentale sotto la vigilanza dell'utente finale per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori".

Nella citata delibera AGCOM chiarisce che per "parental control system" (SCP) o sistema di controllo genitoriale si intende un sistema che quantomeno permette di limitare o bloccare l'accesso a determinate attività da parte di un minore, impedendo l'accesso, tramite qualunque applicazione, a contenuti inappropriati per la sua età. Gli operatori devono fornire, come funzionalità minima, la possibilità di impedire ai minori l'accesso a determinati nomi a dominio, siti web o ad applicazioni che contengono materiale inappropriato per la loro età. Gli operatori realizzano i sistemi di parental control mediante almeno una delle soluzioni tecniche: i) basate su DNS o altro filtro a livello di rete dell'operatore, ii) filtraggio tramite applicativo installabile sui dispositivi del consumatore.

6.2.4 La tutela del minore come "consumatore digitale"

In precedenza, nell'elencare i rischi cui i minori sono esposti quando navigano su Internet, sono stati citati anche i rischi corsi dai minori in quanto consumatori (rischi di marketing, rischi di profilazione commerciale, rischi finanziari e così via).

Nella già citata Comunicazione "Un decennio digitale per bambini e giovani", la Commissione UE si evidenzia come i minori utilizzano spesso prodotti e servizi digitali progettati per gli adulti e sono esposti a una serie di tecniche di commercializzazione online, o ne sono i destinatari. Attraverso i sistemi di raccomandazione dei social media e altri algoritmi, le pubblicità mirate, il marketing di influenza e la ludicizzazione del marketing, contenuti nocivi o inappropriati sono presentati ai giovani utenti, approfittando della loro inesperienza e mancanza di autocontrollo (si pensi alla promozione commerciale di prodotti a elevato contenuto di grassi, zuccheri o sale tra i minori che può aggravare comportamenti alimentari inappropriati.

Anche in questo caso l'ordinamento ha introdotto delle norme utili a depotenziare i rischi corsi dai minori in quanto consumatori (Marcello 2023).

Il comma 9, dell'art. 37 del citato d.lgs. 208/2021 stabilisce che "I dati personali relativi a minori comunque raccolti dai fornitori di servizi di media audiovisivi in applicazione delle disposizioni del presente articolo non possono essere trattati a fini commerciali e, in particolare, a fini di marketing diretto, profilazione e pubblicità mirata sulla base dei comportamenti rilevati"[27].

27 Si veda anche l'art. 6-*bis* della direttiva (UE) 2018/1808.

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

7. I doveri dei minori per la cittadinanza digitale

Il concetto di cittadinanza rinvia, oltre che alla titolarità di diritti di cui si è parlato nei precedenti paragrafi, anche alla necessità di osservare i doveri connessi allo specifico status di cittadino digitale.

Anche i minori sono tenuti ad osservare le regole dello spazio digitale (Pierantoni 2024).

Se il minore pone in essere un comportamento che integra una fattispecie di reato egli ne risponde in sede penale laddove abbia più di quattordici anni[28].

Se il comportamento posto in essere dal minore cagiona danno, a risponderne sono i genitori ex art. 2048 del codice civile[29].

La giurisprudenza ha sottolineato che incombe sui genitori un obbligo formativo nei confronti dei figli minori in ordine alla modalità più corrette per l'utilizzo delle tecnologie digitali (Andreola 2021)[30].

---

28 Cass. civ., Sez. III, Ord., 10/05/2024, n. 12901 si è occupata delle conseguenze civilistiche di una vicenda esitata nella condanna di un minore sul piano penale. Questi i fatti: nel 2001, F.F. e C.C., entrambi minorenni, avevano avuto una relazione amorosa, terminata, nel novembre dello stesso anno, per decisione della ragazza; nell'ultimo periodo della loro relazione, C.C., ottenuto il consenso di F.F., aveva filmato un loro rapporto sessuale; - dopo che ella aveva messo fine al rapporto, lo stesso C.C., per reazione a questa decisione, senza il consenso della ragazza, aveva dapprima mostrato il video agli amici e successivamente lo aveva diffuso mediante la creazione di un cd-rom e mediante proiezioni presso la scuola, sinché il filmato era stato pubblicato su internet; per queste condotte era stato sottoposto a procedimento penale per i reati di pornografia minorile, di pubblicazioni e spettacoli osceni, di diffamazione e minaccia ed era stato condannato, con sentenza passata in giudicato, per i primi due delitti.

29 Tribunale Trani, Sez. I, sentenza 30/11/2021, n. 2062 ha condannato i genitori di un minore a risarcire il danno cagionato dal figlio minorenne per aver diffuso su You Tube un video artigianale che rappresentava due persone nell'atto di consumare un rapporto sessuale.

30 Nella motivazione della sentenza del Tribunale di Trani citata alla nota precedente si legge quanto segue:

"La posizione del minore G.D., assume, ad avviso di questo giudicante, rilevanza illecita nel campo civilistico.

Ed infatti, la sconsiderata scelta di postare il video su un portale di larghissima utilizzazione tra i frequentatori della rete si è inevitabilmente ripercossa sulla reputazione e sull'onore dei minori, soggetti ed esposti alla critica sociale della comunità di appartenenza.

Di tale condotta devono rispondere anche i genitori del minore G.D.; su tale profilo, non può non rilevarsi come la disposizione di cui all'art. 2059 c.c. onera i genitori di provare e dimostrare il corretto assolvimento dei propri obblighi educativi e di controllo sul figlio, solo in tal modo potendosi esonerare dalla condanna risarcitoria.

Nella specie, nulla in particolare è stato dimostrato, ma al contrario, i fatti - quello della pubblicazione su You Tube del video a contenuto pornografico - esprimono, di per sé, una carenza educativa dell'allora minorenne, dimostratosi in tal modo privo del necessario senso critico, di una congrua capacità di discernimento e di orientamento consapevole delle proprie scelte nel rispetto e nella tutela altrui. Capacità che, invece, avrebbe dovuto già godere in relazione all'età posseduta".

Torna, sotto diverso profilo, il tema delle competenze digitali.

Come si è detto, la rete è un mezzo potente di manifestazione del pensiero e i minori hanno diritto ad utilizzare tale mezzo.

Se si postano messaggi o fotografie su un social network essi diventano immediatamente leggibili e visibili da tantissime persone potenzialmente in tutto il mondo. Siffatta straordinaria possibilità ha pregi e difetti. Da una parte il minore può esprimere il proprio pensiero senza intermediazione. Dall'altra, però, è possibile che la rete diventi veicolo di notizie fasulle (*fake news*) o strumento per incitare all'odio (*hate speech*).

I minori devono rispettare le norme e le regole sociali che disciplinano l'ambiente digitale per garantire un contesto sicuro e responsabile per tutti (ad esempio: non devono condividere informazioni personali di altri senza consenso). Devono essere consapevoli dell'impatto delle proprie azioni online e utilizzare la tecnologia in modo sicuro, consci del fatto che la creazione di un ambiente digitale sicuro e non nocivo dipende anche da loro.

Per i minori, la formazione sulle competenze digitali è, contemporaneamente, tanto un diritto quanto un dovere.

8. Conclusioni

Il concetto di cittadinanza digitale ha caratteristiche diverse dal concetto di cittadinanza in senso tradizionale.

Tra gli elementi fondanti di quest'ultimo c'è un determinato territorio e l'esistenza di un soggetto legittimato ad emanare le regole che disciplinano diritti e da doveri validi in quel territorio.

La cittadinanza digitale non si esercita in un ambito territoriale circoscritto da confini ben precisi ma nello spazio digitale per definizione aterritoriale che però ugualmente riconosce diritti ed impone il rispetto di doveri.

I minori sono sempre più chiamati ad esercitare la propria cittadinanza digitale nello spazio digitale.

I minori sono chiamati soprattutto a saper essere cittadini digitali: per evitare il rischio di esclusione (*digital divide*), per trarre giovamento delle tante opportunità che le tecnologie offrono, per non restare vittime dei pericoli che la navigazione in rete comporta. In una parola: per essere all'altezza delle sfide che la rivoluzione digitale pone.

La cittadinanza digitale presuppone il possesso delle competenze digitali. Impossessarsi delle competenze digitali è al tempo stesso un diritto e un dovere.

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

Bibliografia

Alfieri, D. (2022), Internet: quando la "rete" cattura i minori, *Rivista italiana di informatica e diritto*, 1, pp. 53-61.

Andreola, E. (2021), Misure cautelari a tutela dei minori nei social network, *Famiglia e diritto*, 8-9, pp. 849-868.

Barozzi Reggiani, G. e Vaccari S., (2025), Gli strumenti di c.d. age verification per la protezione dei minori nell'ecosistema digitale, *Giornale di diritto amministrativo*, 3, pp. 321-330.

Biligotti N. (2023), La tutela dei minori nel cyberspazio. Parental Control di Stato e libera circolazione dei contenuti: un delicato equilibrio, *Media laws - Riv. dir. Media*, 1, pp. 358-368.

European Centre for Algorithmic Transparency roundtables (2025), *Minors' health and social media: an interdisciplinary scientific perspective*, pubblicazione del Joint Research Centre.

Garaci, I. (2023) The child's right to privacy in the family context, *European journal of privacy law & technologies*, 1, 84-98.

Giarda R., Liotta J. Spagnuolo A. F. (2022), Vita quotidiana del minore online. Tra esigenze di tutela elimiti tecnologici, *Media laws - Riv. dir. media*, 2022, 183-198.

Maestri, E. (2017) Il minore come persona digitale. Regole, tutele e privacy dei minori sul Web, *Annali online della Didattica e della Formazione Docente*, 13, pp- 7-25.

Marcello, D., (2023), *Circolazione dei dati del minore tra autonomia e controllo: norme e prassi nel mercato digitale europeo*, Napoli, Edizioni scientifiche italiane

Martoni, M. (2023), Persuasive Design Technologies, Dark Patterns e diritti di bambini e adolescenti. I video giochi online come primo ambito di analisi, *Federalismi.it*, 14, pp. 162-179.

OECD, (2021) *Children in the digital environment: Revised typology of risks*, OECD Digital Economy Papers, No. 302, OECD Publishing, Paris.

Pascuzzi, G., (2025), *Il diritto dell'era digitale*, Bologna, Il Mulino, 2025.

Pascuzzi, G. (2021), *La cittadinanza digitale. Competenze, diritti e regole per vivere in rete*, Bologna, Il Mulino.

Pierantoni, D., (2024) Minori su Internet: profili di responsabilità, *Rivista italiana di informatica e diritto*, 2, pp. 400-414.

Ricci, R., (2024), *Le competenze digitali nella scuola: un ponte tra passato e futuro*, Bologna, Il mulino.

Ricciulli, F. (2024), L'identità e l'identificazione digitale del minore tra normative nazionale e internazionale e i provvedimenti delle autorità competenti, *Rivista italiana di informatica e diritto*, 2, pp. 355-370.

Vizzoni, L. (2025), *I "minori digitali" tra doveri educativi e tutele*, Bari Cacucci.

Zanovello, F., (2024) prevenzione e contrasto del bullismo e del cyberbullismo. Tra novità e criticità della l. n. 70/24, *Le Nuove Leggi Civili Commentate*, 4, pp. 826-850.

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

I minori nella società digitale tra verifica dell'età, deepfake e disinformazione. Alcune considerazioni informatico-giuridiche

Minors in the Digital Society: Age Verification, Deepfakes, and Disinformation. Some Considerations on Law and Informatics

Giovanni Ziccardi[1]

Sommario

L'articolo affronta il tema della tutela dei minori nella società digitale, con particolare attenzione ai sistemi di verifica dell'età, al fenomeno dei deepfake, all'esposizione alla disinformazione e all'utilizzo di chatbot e intelligenze artificiali. L'obiettivo è individuare criticità normative, tecniche e sociali, proponendo una risposta integrata che tuteli i diritti dei minori senza pregiudicare quelli degli altri utenti.

L'analisi impiega un approccio informatico-giuridico multidisciplinare, esaminando fonti normative europee e italiane (tra cui GDPR, Digital Services Act, regolamenti AGCOM), documenti dell'EDPB, e casi concreti (TikTok, Replika, Europol-Cumberland). Il contributo integra riflessioni teoriche con esempi pratici, attingendo anche da ambiti educativi, psicologici e tecnologici. L'approccio è sia descrittivo che propositivo.

L'articolo propone un approccio sistemico alla protezione dei minori online, articolato su tre assi: normativo, tecnologico ed educativo. Sul piano normativo, si suggerisce di rafforzare gli obblighi di age verification, aggiornare le definizioni di contenuti vietati e armonizzare le sanzioni. Dal punto di vista tecnologico, si auspica la progettazione di sistemi "privacy-by-design" e trasparenza algoritmica. Infine, l'educazione critica ai media e alla realtà digitale deve essere potenziata nelle scuole e nelle famiglie. Il coinvolgimento di tutti gli stakeholder – istituzioni, piattaforme, educatori, genitori – è essenziale per creare un ambiente digitale equo e sicuro per le nuove generazioni.

Parole chiave: verifica dell'età; tutela dei minori; disinformazione digitale; deepfake; intelligenza artificiale generativa

1 Dipartimento di Scienze Giuridiche "Cesare Beccaria", Università degli Studi di Milano. giovanni.ziccardi@unimi.it

Data invio: 1 luglio 2025. Data accettazione: 3 settembre 2025.
DOI: https://doi.org/10.54103/1972-5760/30050

Abstract

This article addresses the protection of minors in the digital society, focusing on age verification systems, deepfakes, exposure to disinformation, chatbots, and AI tools. The aim is to identify legal, technological, and social challenges, proposing an integrated response that safeguards minors' rights without undermining thoseof other users.

The analysis adopts a multidisciplinary legal and informatics approach, examining European and Italian legal sources (including GDPR, Digital Services Act, AGCOM regulations), EDPB documents, and case studies (TikTok, Replika, Europol's Operation Cumberland). The article combines theoretical reflections with practical examples, drawing from educational, psychological, and technological domains, using both descriptive and normative arguments.

This contribution advocates for a systemic approach to online minor protection, structured around three dimensions: regulatory, technological, and educational. on the regulatory level, the article recommends strengthening age verification requirements, updating legal definitions of prohibited contents, and ensuring consistent enforcement. Technologically, it calls for the implementation of "privacy by design" solutions and algorithmic transparency. Finally, critical digital and media literacy education must be promoted in schools and families. The involvement of all stakeholders – public authorities, tech companies, educators, and families – is key to foster a fair and safe digital environment for younger generations.

Keywords: age verification; child protection; digital disinformation; deepfake; generative artificial intelligence

1. Introduzione: il nodo centrale della verifica dell'età e gli evidenti limiti delle normative esistenti

Il delicato tema della tutela dei minori online deve inevitabilmente fare i conti con la capacità concreta (e realistica) di controllarne l'accesso ai servizi digitali in base all'età (Li 2025; Pasquale *et al*. 2022). Si tratta di un argomento "storico" dell'informatica giuridica che non presenta unicamente aspetti legali e tecnologici ma, anche, psicologici ed educativi (Pesci 2024; Ghiglia 2023). Questo problema ha sollevato, negli ultimi quindici anni, un acceso dibattito a livello mondiale, soprattutto con riferimento alla sempre maggiore disponibilità di contenuti pornografici e violenti (facilmente) accessibili ai minori (Stardust *et al.* 2024; Yar 2020; Blake 2019).

Attualmente, sia la normativa europea sia quella italiana fissano specifiche soglie di età per l'uso lecito dei dati personali dei minori nei servizi della società dell'informazione (Murgo 2024) e hanno, da tempo, elaborato l'idea

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

di una *privacy del minore* persino nel contesto familiare e nei confronti delle ingerenze dei genitori (Garaci 2023).

L'art. 8 del Regolamento europeo sulla protezione dei dati del 2016 (d'ora in avanti: GDPR), in particolare, stabilisce in linea generale come il trattamento dei dati di un minore sia lecito solo a partire dai 16 anni. Ha però consentito agli Stati membri di abbassare tale soglia fino a un minimo di 13 anni, con un approccio che ha destato interesse, e dubbi, anche al di fuori dall'Unione Europea (Caggiano 2022).

L'Italia, attraverso il d.lgs. 101/2018 (di adeguamento della normativa nazionale al GDPR), ha fissato il limite a 14 anni, richiedendo sotto tale limite di età il consenso di chi esercita la responsabilità genitoriale (art. 2-*quinquies* del D.lgs. 196 del 2003).

Ne consegue che, formalmente, nel nostro ordinamento un minore di 14 anni *non potrebbe* attivare autonomamente un account sui social network o, comunque, fruire di servizi online che implichino il trattamento dei suoi dati personali (Savonardo, Marino 2021).

Al contempo, questa fissazione di soglia di età ai 14 anni è stata vista dalla politica italiana come una sorta di *segnale di fiducia* e di responsabilizzazione verso i minori online e verso i gestori delle piattaforme (Macenaite, Kosta 2017), muovendo però dalla premessa di una maturità tecnologica, nel nostro Paese, che in molti contesti è ancora ben lontana da raggiungere.

Le principali piattaforme globali, dal canto loro, prevedono nei termini di servizio un'età minima di 13 anni per l'iscrizione, in coerenza con le normative internazionali (anche nordamericane) e con il limite-base del GDPR (Talley 2021).

In teoria, quindi, bambini e preadolescenti dovrebbero restare *esclusi* dai social network e da molte altre piattaforme fino alla soglia dell'adolescenza avanzata. In pratica, tuttavia, questi divieti d'accesso per età risultano facilmente *aggirabili* e la loro efficacia è a dir poco limitata (Biolcati *et al.* 2016).

Si pensi che, nella maggior parte dei casi, la modalità standard di verifica dell'età in fase d'iscrizione si riduce a una *autodichiarazione dell'utente* (la classica selezione della data di nascita), meccanismo che un minore può falsificare senza difficoltà.

Non sorprende, dunque, che la realtà fotografi numeri ben diversi da quelli attesi per legge: la gran maggioranza dei preadolescenti europei (11-13 anni) ha già almeno un profilo social attivo, e molti di essi ne possiede più di uno.

La mancanza di meccanismi efficaci di *age verification* vanifica dunque, nei fatti, la tutela normativa, lasciando schiere di under-14 liberi di creare account mentendo sulla loro età e di muoversi in ambienti virtuali concepiti per utenti più grandi (Nagel 2011).

Questo quadro è ovviamente assai frustrante sia per il legislatore sia per l'interprete nel momento in cui cercano di impostare un ragionamento coerente, e costruttivo, sui minori online e sulle loro attività.

Milioni di bambini, in tutta Europa, semplicemente non dovrebbero essere, per legge, su queste piattaforme. Ma ci sono, condividono i loro dati e, anzi, sono i profili più interessanti per le piattaforme e per i loro contenuti. Non sono solo gli elettori del futuro ma, anche e soprattutto, i più vivaci *consumatori* del presente (Slavtcheva-Petkova 2023).

2. Il Comitato europeo per la protezione dei dati (EDPB) e lo "Statement 1/2025 on Age Assurance"

Negli ultimi anni, questa crescente esposizione dei minori a rischi digitali (Biolcati 2010) ha generato un'intensificazione dell'interesse normativo e regolamentare nei confronti della verifica dell'età come principale strumento di protezione.

Questa tendenza ha preso corpo in una serie di atti giuridici a livello di Unione europea che attribuiscono alla verifica dell'età una funzione strategica nella costruzione di ambienti digitali sicuri, pur senza trascurare il rischio che tali strumenti possano trasformarsi in vettori di sorveglianza generalizzata, discriminazione o profilazione indebita (Frigato 202; Zuboff 2019).

A fronte di questo scenario, l'11 febbraio 2025 il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato la Dichiarazione 1/2025, documento che rappresenta un passo significativo nel delineare principi-guida per un sistema di *age assurance* conforme al GDPR, in grado di garantire una tutela efficace dei minori senza compromettere i diritti e le libertà degli individui, in particolare il diritto alla protezione dei dati personali.

La verifica dell'età, secondo l'impostazione dell'EDPB, non può essere considerata una mera misura tecnica né, tantomeno, una formalità amministrativa. Essa implica una *scelta normativa profonda*, poiché impatta su molteplici diritti fondamentali: dalla privacy alla libertà di espressione, dall'accesso all'informazione al diritto alla non discriminazione. È quindi essenziale che la sua progettazione rispetti un *principio di equilibrio* tra tutela e proporzionalità, soprattutto quando riguarda soggetti vulnerabili come i minori.

Il quadro giuridico europeo offre oggi, a onor del vero, diverse basi normative per l'implementazione di sistemi di verifica dell'età.

La Direttiva 2018/1808/UE sui servizi di media audiovisivi, in primis, prevede l'adozione di misure atte a proteggere i minori dai contenuti dannosi, mentre il Digital Services Act (Reg. UE 2022/2065) considera la verifica dell'età uno strumento utile per adempiere agli obblighi di valutazione e mitigazione dei rischi sistemici da parte delle grandi piattaforme. Il GDPR,

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

infine – si è visto poco sopra – introduce un requisito di età minima per la validità del consenso dei minori ai servizi digitali (art. 8), stabilendo così un nodo giuridico essenziale tra verifica dell'età e legittimità del trattamento dei dati personali.

Ma il vero nucleo problematico risiede nella conciliazione tra la protezione dei minori e il rispetto dei diritti degli interessati.

L'EDPB ribadisce che, nell'ambito della verifica dell'età, l'interesse superiore del minore – principio cardine della Convenzione ONU sui diritti dell'infanzia – deve essere sempre una considerazione primaria. Tuttavia, ciò non implica che altri diritti possano essere compressi arbitrariamente: il trattamento dei dati personali per fini di verifica dell'età deve essere sempre necessario, proporzionato e fondato su una solida base giuridica.

È su questo punto che l'EDPB sviluppa una riflessione centrale: l'importanza della *valutazione del rischio*, che deve guidare l'intero ciclo di vita del sistema di verifica.

La dichiarazione raccomanda esplicitamente l'adozione di Data Protection Impact Assessments (DPIA) nei casi in cui il trattamento comporti rischi elevati per i diritti e le libertà degli interessati. Ancora più rilevante, nel contesto specifico dei minori, è l'adozione di valutazioni dell'impatto sui diritti dell'infanzia (Child Rights Impact Assessments – CRIA), in grado di integrare l'ottica della tutela evolutiva e della partecipazione dei minori stessi alla progettazione dell'ambiente digitale.

Sul piano tecnico, viene poi (inevitabilmente) ribadito il principio di *minimizzazione* dei dati: ogni sistema di verifica dell'età deve limitarsi al trattamento dei soli dati strettamente necessari per l'obiettivo specifico.

Nella maggior parte dei casi non è necessario conoscere l'identità dell'utente, ma solo se questi ha superato una determinata soglia d'età. Soluzioni come i *token di età*, rilasciati da un soggetto terzo e contenenti esclusivamente l'informazione "sì/no" rispetto alla soglia richiesta, rappresentano esempi virtuosi di privacy-enhancing technologies (PETs), ossia approcci tecnici che consentono di ridurre il rischio di re-identificazione e profiling, favorendo la non riferibilità tra dati e servizi.

Il principio di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 GDPR) assume, in questo contesto, un rilievo cruciale.

L'EDPB sottolinea la necessità di adottare architetture decentralizzate, sistemi locali di verifica e strumenti crittografici avanzati, come le "prove a conoscenza zero" (*zero-knowledge proofs*), che permettono di dimostrare il possesso di un'informazione (ad es. avere più di 18 anni) senza rivelare *alcun dato personale aggiuntivo*. Tali strumenti dovrebbero essere adottati come standard tecnologici per tutti i casi in cui l'accesso a determinati contenuti o servizi dipenda dall'età dell'utente.

Un altro aspetto fortemente valorizzato è quello dell'efficacia del sistema di verifica. L'EDPB richiama l'attenzione sul fatto che molte delle tecnologie attualmente in uso – in particolare l'autodichiarazione – risultano del tutto *inefficaci*, poiché facilmente eludibili e prive di meccanismi di controllo.

È quindi necessario che i metodi adottati siano in grado di fornire un livello di accuratezza, affidabilità e robustezza adeguato allo scopo. Inoltre, le soluzioni adottate devono essere *accessibili* a tutti gli utenti, evitando discriminazioni tecnologiche o economiche, ad esempio verso chi non possiede documenti digitali, strumenti biometrici o connessioni stabili (Carr 2025).

La *trasparenza* è un ulteriore pilastro: gli utenti, e in particolare i minori, devono essere informati in modo chiaro e comprensibile circa i dati trattati, le finalità, le modalità di trattamento, gli eventuali soggetti terzi coinvolti e i diritti esercitabili.

Il rispetto degli obblighi informativi previsti dagli articoli 12-14 del GDPR non può essere considerato meramente formale: è una condizione sostanziale di liceità e correttezza del trattamento.

Particolare cautela è richiesta anche nei confronti dei processi decisionali automatizzati. L'EDPB ricorda che, salvo casi eccezionali, il GDPR vieta il ricorso a decisioni automatizzate che producano effetti giuridici su soggetti minori.

Qualora si faccia uso di tecniche automatizzate nella determinazione dell'età, devono essere garantiti *interventi umani* significativi, meccanismi di ricorso efficaci e modalità comprensibili per esercitare i diritti dell'interessato. Il rischio, altrimenti, è quello di sottrarre il minore a forme effettive di tutela, producendo esclusione o discriminazione algoritmica.

Dal punto di vista della sicurezza, il trattamento dei dati per la verifica dell'età deve essere accompagnato da misure tecniche e organizzative proporzionate al rischio. Tecniche di pseudonimizzazione, crittografia, conservazione limitata e politiche di non registrazione sono considerate fondamentali. L'EDPB sottolinea come i modelli di fiducia e i sistemi a basso grado di interdipendenza tra fornitori siano essenziali per garantire la resilienza del sistema anche in caso di violazione dei dati.

Infine, l'intero processo deve essere sorretto da un solido quadro di responsabilità ("accountability"). I titolari del trattamento e le terze parti coinvolte devono poter dimostrare – attraverso documentazione, audit, controlli e sistemi di governance – che ogni fase della verifica dell'età sia conforme alle normative sulla protezione dei dati. La trasparenza del sistema non è solo una garanzia per l'utente ma, anche, un presupposto per la legittimità stessa dell'intervento regolatorio.

L'approccio dell'EDPB, che abbiamo analizzato per primo proprio perché si fonda su una visione bilanciata e sul rigoroso rispetto dei principi del GDPR, offre una cornice utile non solo per il legislatore europeo e nazionale ma, anche, per i progettisti di sistemi, i responsabili del trattamen-

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

to e gli operatori delle piattaforme digitali. Solo attraverso l'integrazione consapevole dei diritti nella progettazione tecnica sarà possibile costruire un ecosistema digitale realmente sicuro, inclusivo e rispettoso della dignità delle persone.

3. Il regolamento AGCOM

Nel panorama normativo italiano, il 2025 ha segnato un passaggio particolarmente significativo in materia di tutela dei minori online con l'adozione di un Regolamento da parte dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM) che impone, per la prima volta in modo organico, l'utilizzo *obbligatorio* di sistemi di verifica dell'età *certificati da terze parti* per l'accesso a contenuti vietati ai minori di diciotto anni.

Il provvedimento si rivolge esplicitamente a siti web e piattaforme digitali che offrono contenuti a rischio per l'integrità psicofisica dei minori, come nel caso della pornografia online, del gioco d'azzardo, della rappresentazione esplicita di violenza o di prodotti potenzialmente nocivi.

In questo senso, il Regolamento AGCOM recepisce e rafforza – sul piano dell'attuazione nazionale – quanto delineato a livello europeo dal Digital Services Act e dal GDPR, collocandosi in un quadro più ampio di armonizzazione degli standard di sicurezza e responsabilità digitale.

L'elemento di maggiore novità introdotto dal Regolamento italiano riguarda l'obbligo, per i fornitori di contenuti classificati come *vietati ai minori*, di integrare sistemi di verifica dell'età robusti e certificati da *soggetti terzi qualificati*, che siano indipendenti sia dal fornitore stesso che dai gestori delle piattaforme di hosting.

Questa misura non solo eleva il livello di affidabilità tecnica dei controlli, ma rappresenta anche un *cambio di paradigma* rispetto alla prassi diffusa dell'autodichiarazione, ritenuta ampiamente insufficiente per garantire una reale protezione dei minori. La certificazione ha una funzione non solo tecnica ma, anche, giuridica: vincola i fornitori all'adozione di standard interoperabili, documentati, soggetti a verifica periodica e conformi ai principi di trasparenza, proporzionalità e sicurezza imposti dal GDPR.

Dal punto di vista tecnologico, il Regolamento apre alla possibilità di impiegare diverse soluzioni di *age verification*, a condizione che esse rispondano a criteri stringenti di efficacia, privacy e inclusività.

Tra le tecnologie ammesse figurano, ad esempio, sistemi basati su credenziali digitali firmate, in cui un'identità "pre-verificata" (da un provider pubblico o privato) attesta il superamento di una soglia d'età attraverso un token crittografico non tracciabile che può essere verificato dal sito di destinazione senza esporre ulteriori dati dell'utente. Una variante di questo modello prevede l'utilizzo di "zero-knowledge proofs" (ZKP), che permettono

a un soggetto di dimostrare di possedere un attributo (ad esempio "ho più di 18 anni") senza rivelare alcuna informazione ulteriore, inclusa l'età esatta o l'identità personale.

Un altro modello considerato idoneo, anche se più invasivo, è rappresentato dalle *verifiche documentali con riconoscimento automatizzato*, che prevedono il caricamento di un documento d'identità e l'utilizzo di tecnologie biometriche per il confronto facciale (Bianda 2019).

Sebbene queste soluzioni offrano un alto grado di affidabilità nella verifica dell'identità e dell'età, esse pongono serie criticità in termini di proporzionalità, minimizzazione dei dati e rischio di violazioni della sicurezza, specialmente se non accompagnate da politiche rigorose di conservazione e separazione dei dati. Per questo motivo, il Regolamento AGCOM richiede esplicitamente che i sistemi utilizzati *non conservino* dati sensibili oltre il tempo strettamente necessario alla verifica e che adottino misure di pseudonimizzazione, cancellazione automatica e crittografia end-to-end.

Un aspetto di rilievo, spesso sottovalutato, riguarda inoltre l'inclusività e l'accessibilità delle tecnologie di verifica. Il Regolamento prevede che i sistemi adottati non debbano escludere o discriminare soggetti privi di documentazione digitale, minorenni emancipati o appartenenti a categorie vulnerabili. In tale ottica, viene incoraggiata l'adozione di *metodi alternativi*, come la verifica tramite intermediari accreditati (ad es. fornitori di identità digitale, enti pubblici, istituti scolastici), che possano attestare l'età dell'utente senza obbligarlo a fornire direttamente documenti o dati biometrici. Questa apertura metodologica dimostra una sensibilità verso il principio di *equità tecnologica*, evitando che la protezione dei minori si traduca, nei fatti, in una nuova forma di digital divide.

Dal punto di vista giuridico, il Regolamento si fonda su un sistema sanzionatorio e di *enforcement progressivo*, che prevede l'intervento dell'AGCOM in caso di mancato adeguamento, fino al blocco dell'accesso al sito mediante provvedimenti di inibizione tecnica (*DNS/IP blocking*). Viene inoltre introdotto un *registro pubblico* dei fornitori conformi, che può svolgere un ruolo di trasparenza e responsabilizzazione verso gli utenti ma, anche, di competizione regolatoria virtuosa tra le piattaforme digitali.

4. Il caso TikTok

Un caso emblematico che ha tragicamente messo in luce le falle strutturali nei sistemi di verifica dell'età e le carenze normative nella protezione dei minori online è quello c che ha riguardato una bambina di 10 anni deceduta a Palermo nel gennaio 2021, mentre partecipava a una pericolosa sfida virale – la cosiddetta *blackout challenge* – diffusa su TikTok. L'evento ebbe un forte impatto sull'opinione pubblica e segnò un punto di svolta anche

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

nell'approccio delle autorità italiane nei confronti delle piattaforme digitali, sollevando interrogativi urgenti sulla responsabilità delle big tech nella tutela dei soggetti vulnerabili (Cantero Gamito 2023).

L'immediatezza dell'intervento del Garante per la protezione dei dati personali fu senza precedenti: l'Autorità dispose con urgenza il *blocco* dell'uso della piattaforma per tutti gli utenti italiani per i quali non fosse stata verificata con certezza l'età anagrafica, ponendo così una delle prime limitazioni effettive all'attività di una grande piattaforma internazionale per motivi legati alla protezione dei minori.

L'istruttoria condotta mise rapidamente in evidenza l'inefficacia del sistema di *age verification* adottato da TikTok all'epoca, che consentiva l'iscrizione con estrema facilità e senza alcuna forma di verifica attendibile: bastava indicare una data di nascita fittizia per accedere a tutte le funzionalità, anche in assenza di qualsiasi supervisione genitoriale.

A rendere ancora più grave il quadro era la configurazione predefinita dei profili, che risultavano *automaticamente pubblici*, esponendo così utenti anche molto giovani a forme incontrollate di visibilità e interazione con estranei.

Questa scelta di design, lungi dall'essere neutrale, rifletteva un'impostazione orientata alla massima condivisione e interazione sociale, in linea con la logica di *engagement* tipica delle piattaforme, ma in aperto contrasto con i principi di "privacy by default" richiesti dall'articolo 25 del GDPR.

In assenza di adeguate protezioni o meccanismi di parental control, i minori venivano resi visibili, raggiungibili e, in alcuni casi, strumentalizzabili senza che né loro né le famiglie ne fossero realmente consapevoli.

L'intervento del Garante, in quel contesto, assunse un valore esemplare non solo sotto il profilo sanzionatorio ma, allo stesso tempo, come segnale politico e normativo.

L'Autorità richiamò esplicitamente TikTok ai suoi doveri di conformità rispetto all'art. 8 del GDPR – che prevede, per i minori di 14 anni in Italia, il necessario consenso dei titolari della responsabilità genitoriale per il trattamento dei dati – oltre che alle norme italiane in materia di protezione dei minori e ai principi generali di sicurezza dei servizi digitali.

Tuttavia, il Garante non si limitò a un'interpretazione formalistica del quadro normativo: in una nota pubblica, il presidente Pasquale Stanzione sottolineò che "il Garante può bloccare i social, ma il primo controllore è il genitore", evidenziando così la corresponsabilità familiare nel processo di tutela e la necessità di una vigilanza attiva che vada oltre le soluzioni puramente tecnologiche.

Tuttavia, quanto emerso nel caso TikTok rivela una tensione strutturale tuttora irrisolta tra la *law in the books* e la *law in action*.

Da un lato, il diritto europeo e italiano dispongono principi avanzati, come l'obbligo di consenso informato, la protezione rafforzata dei dati dei mino-

ri e la progettazione per default della privacy; dall'altro, mancano strumenti sanzionatori efficaci, meccanismi di verifica interoperabili e standard tecnici comuni a livello sovranazionale. Non esiste, ad esempio, un sistema di *certificazione* europeo per i metodi di verifica dell'età, né una disciplina condivisa che imponga livelli minimi di affidabilità o inclusività nei sistemi adottati dalle piattaforme. Questa asimmetria tra doveri normativi e strumenti tecnici lascia ampi margini di discrezionalità alle imprese, che spesso adottano soluzioni simboliche e facilmente aggirabili, con effetti potenzialmente nocivi.

Sotto il profilo tecnologico, il caso solleva ulteriori criticità. Il meccanismo di *age verification* implementato da TikTok – basato, nella sostanza, sull'autodichiarazione priva di qualsiasi validazione – rappresenta una delle soluzioni meno affidabili disponibili. Non solo è tecnicamente inadeguato, ma è anche in contrasto con le linee guida europee, che mettono in guardia proprio contro i metodi di verifica che si fondano unicamente sulla buona fede dell'utente, specie quando questi è un soggetto vulnerabile. A distanza di anni, molte piattaforme continuano a utilizzare simili modelli, eludendo l'obbligo di dimostrare la proporzionalità, l'efficacia e la non discriminazione dei sistemi di controllo adottati.

Alla luce di questi elementi, appare evidente l'urgenza di un intervento *multilivello*, capace di combinare regolazione normativa, standard tecnici e strumenti di *enforcement* efficaci.

Le autorità garanti nazionali e sovranazionali dovrebbero essere dotate di poteri adeguati non solo per sanzionare ma, anche, per prescrivere concretamente modelli di progettazione responsabile, in linea con i principi di "data protection by design and by default". Allo stesso tempo, è indispensabile coinvolgere l'industria in forme di co-regolamentazione e autoregolazione tecnologica affinché siano adottate soluzioni scalabili, interoperabili e rispettose dei diritti fondamentali.

Il caso TikTok rappresenta dunque molto più di un tragico episodio isolato: è uno specchio dei *limiti sistemici* dell'ecosistema digitale contemporaneo, in cui il diritto, la tecnica e, soprattutto, l'etica faticano ancora a dialogare in modo efficace (Scalzaretto 2023).

Solo attraverso una convergenza più stretta tra norme giuridiche, progettazione tecnica e responsabilità sociale sarà possibile evitare che simili tragedie si ripetano e costruire davvero un ambiente digitale a misura di minore.

5. Il caso Replika: chatbot e minori esposti a contenuti inappropriati

L'evoluzione recente dell'intelligenza artificiale generativa ha aperto nuovi scenari anche rispetto alla fruizione digitale dei contenuti da parte dei minori.

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

Un episodio paradigmatico è rappresentato dalla vicenda di Replika, un popolare chatbot basato su intelligenza artificiale creato dalla startup statunitense Luka Inc.

Lanciato nel 2017, Replika si presenta come un "amico virtuale" personalizzabile, capace di conversare in modo realistico con l'utente simulando empatia e sostegno emotivo.

La promessa di un avatar mosso dall'intelligenza artificiale in grado di migliorare il benessere emotivo ha attratto milioni di utenti nel mondo, inclusi molti giovani; tuttavia, dietro l'apparenza rassicurante, sono emerse gradualmente zone d'ombra che hanno allertato le autorità.

In assenza di adeguati filtri, minorenni anche molto giovani potevano scaricare e utilizzare Replika liberamente, entrando in dialogo con l'intelligenza artificiale senza alcuna supervisione né controllo sull'appropriatezza dei contenuti.

Già a inizio 2023 si erano registrati i primi casi di interazioni inquietanti: alcuni utenti – spesso fragili o poco più che adolescenti – hanno denunciato vere e proprie molestie sessuali virtuali da parte del chatbot.

Replika, sfruttando le capacità generative del suo modello linguistico, era in grado di assumere toni romantici ed erotici "spinti" nelle conversazioni, fino a simulare scenari espliciti inadatti a un pubblico minorenne.

Di fatto esistevano due versioni: una gratuita "amichevole" e una a pagamento con contenuti romantici/erotici più avanzati. Nessun vero ostacolo impediva a un utente minorenne di accedere a quest'ultima, dal momento che l'app non prevedeva alcuna verifica effettiva dell'età all'iscrizione o durante l'uso.

Il servizio dichiarava nelle policy di essere vietato ai minori, ma tale divieto restava lettera morta, affidato unicamente all'onere degli utenti di dichiararsi maggiorenni.

Di fronte a questa situazione, l'Autorità Garante italiana è intervenuta con decisione. Nel febbraio 2023, a tutela urgente, ha ordinato la sospensione di Replika nel territorio nazionale, motivandola con i rischi specifici per i minori derivanti dal chatbot. L'indagine istruttoria che ne è seguita ha confermato diverse violazioni gravi: Replika non disponeva di una base giuridica valida per trattare i dati personali degli utenti europei, forniva un'informativa privacy inadeguata e – ciò che qui più rileva – era totalmente privo di sistemi per *escludere* l'accesso dei bambini al servizio.

In altri termini, l'azienda non aveva né verifiche dell'età né filtri sui contenuti generati dall'intelligenza artificiale in presenza di utenti minorenni.

Neppure dopo il blocco iniziale la società ha saputo porre rimedio a queste carenze, il che ha condotto nel 2025 all'esito sanzionatorio: il Garante ha irrogato a Luka Inc. una multa di 5 milioni di euro, accertando formalmente la violazione dei principi del GDPR e del diritto italiano.

Come ribadito nel provvedimento finale, la posizione del gestore era aggravata proprio dall'assenza di meccanismi di verifica dell'età, che ha consentito ai minori di usare un servizio potenzialmente pericoloso e non tarato per loro.

Contestualmente, l'Autorità ha aperto una nuova indagine sull'algoritmo di intelligenza artificiale generativa di Replika, per esaminarne i dati di addestramento e la conformità alle regole europee (un tema legato alla privacy e alla sicurezza generale del sistema).

Il caso Replika evidenzia emblematicamente le insidie che le applicazioni di intelligenza artificiale conversazionale possono comportare per i più giovani, in assenza di adeguate tutele. Da un lato, un chatbot avanzato può esercitare un forte ascendente psicologico su utenti adolescenti, instaurando con loro un rapporto quasi simbiotico e di dipendenza emotiva (il cosiddetto "companion AI").

Dall'altro, i contenuti che l'intelligenza artificiale genera in risposta alle sollecitazioni dell'utente possono facilmente oltrepassare i confini dell'appropriatezza: come visto, Replika era programmato per assecondare anche registri molto intimi e sessualizzati, sfociando in interazioni del tutto inadatte a un minore.

In assenza di un filtro editoriale o umano, l'intelligenza artificiale può produrre output estremi o falsi con apparente naturalezza.

Il fatto che una macchina possa molestare verbalmente un adolescente, o fornirgli consigli potenzialmente dannosi spacciandosi per "amico", pone interrogativi urgenti sul tipo di esposizione cui i minori possono andare incontro.

Inoltre, sotto il profilo giuridico, casi come questo mostrano la difficoltà di inquadrare servizi innovativi nel perimetro normativo esistente: Replika sfuggiva alle maglie delle tradizionali regolamentazioni sui contenuti (non essendo catalogabile come contenuto editorialmente controllato) e, fino all'intervento del Garante, operava in una sorta di vuoto regolatorio.

La risposta delle istituzioni italiane – tra le prime al mondo – segnala comunque un indirizzo chiaro: i fornitori di servizi di intelligenza artificiale generativa devono farsi carico della protezione dei minori, implementando fin dall'inizio controlli d'età e limiti sui contenuti che tengano conto della loro presenza.

Il "caso Replika" ha fatto scuola, preannunciando un'epoca in cui sarà necessario vigilare attentamente anche sugli algoritmi conversazionali, affinché l'innovazione non vada a detrimento dei diritti dei più giovani.

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

6. Disinformazione, teorie del complotto e polarizzazione algoritmica tra gli adolescenti

Nella vita online degli adolescenti un capitolo cruciale è rappresentato dall'informazione e disinformazione.

Le nuove generazioni tendono, infatti, a usare i social network non solo per svago o interazione personale ma, anche, come fonte primaria di notizie e aggiornamenti sul mondo, utilizzando canali come WhatsApp, Instagram e TikTok per informarsi su notizie di attualità.

Questa commistione tra flusso informativo e piattaforme di intrattenimento comporta conseguenze ambivalenti.

Se, da un lato, i ragazzi hanno accesso immediato a una pluralità di fonti e punti di vista, dall'altro risultano particolarmente esposti alle fake news, alle teorie del complotto e alla propaganda virale veicolata dagli algoritmi.

La facilità con cui circolano e attecchiscono narrazioni infondate tra i più giovani è allarmante: basti pensare alla diffusione virale, negli ultimi anni, di teorie complottiste come quelle negazioniste sui vaccini, sulle pandemie orchestrate o su sfide mortali.

Queste teorie trovano terreno fertile sui social media, dove logiche di gruppo e bisogno di appartenenza possono portare gli adolescenti ad abbracciare visioni distorte pur di identificarsi con una comunità virtuale.

Un fattore chiave, notoriamente, è il ruolo degli *algoritmi di raccomandazione* delle piattaforme.

I social network e i siti di video-sharing tendono a mostrare agli utenti contenuti in linea con le loro precedenti interazioni, massimizzando il tempo di visualizzazione e il coinvolgimento.

Questo crea le cosiddette *filter bubbles*, o camere dell'eco, in cui i giovani rischiano di venire alimentati con informazioni unilaterali e progressivamente più estreme.

Ad esempio, un ragazzo che inizi a guardare su YouTube video cospirazionisti o polarizzati su un tema (poniamo, sulle scie chimiche o su teorie antiscientifiche) verrà verosimilmente raggiunto da suggerimenti di nuovi video analoghi, magari ancora più radicali, in un percorso di polarizzazione algoritmica che può condurlo verso posizioni sempre più distorte.

L'ecosistema digitale, progettato per massimizzare l'engagement, talvolta finisce per privilegiare contenuti sensazionalistici, divisivi o emotivamente forti: proprio quelli che costituiscono il nucleo della disinformazione e delle narrazioni complottiste.

Questo circolo vizioso può incidere sulla formazione dell'identità e della visione del mondo nei ragazzi, i quali – se privi di strumenti critici – possono aderire a ideologie estreme o sviluppare percezioni della realtà falsate.

Vi è poi il fenomeno, altrettanto complesso, della *disinformazione personalizzata*: fake news e teorie del complotto oggi non sono confezionate con

approccio "one size fits all", ma vengono sovente targettizzate su specifiche fasce d'età o gruppi di interesse, sfruttando i dati personali disponibili online.

Gli adolescenti, che condividono incessantemente dati e preferenze sui social, diventano così bersagli perfetti per campagne disinformative mirate (si pensi alle pubblicità occulte di prodotti nocivi, ai movimenti negazionisti che reclutano i giovanissimi sul clima o su altri temi, ecc.).

L'impeto partecipativo tipico dell'età adolescenziale può essere manipolato dalle *echo chambers* digitali, trasformando ribellione e bisogno di identità in appartenenza a gruppi virtuali radicalizzati.

Di fronte a questo scenario, appare drammaticamente confermata l'esigenza di un'educazione critica all'informazione (Gallese, Moriggi, Rivoltella 2025).

Ma il compito, sia chiaro, non può ricadere solo sulla scuola: è necessario un impegno congiunto di piattaforme digitali, istituzioni e famiglia.

Le prime dovrebbero investire in sistemi di moderazione e fact-checking più efficaci, oltre che in design algoritmici meno polarizzanti; le seconde dovrebbero promuovere campagne di sensibilizzazione e programmi formativi; la famiglia, dal canto suo, dovrebbe vigilare e dialogare con i ragazzi sui contenuti che questi fruiscono online, colmando il vuoto di riferimento che spesso lascia i minori soli davanti alle fake news.

In mancanza di queste azioni, il rischio è duplice: da un lato una generazione di cittadini digitali poco informati o addirittura disinformati, dall'altro una possibile disaffezione verso la stessa idea di *verità*.

7. Deepfake e contenuti generati dall'intelligenza artificiale: l'impatto su percezione e verità

Tra le nuove frontiere che mettono alla prova la capacità dei minori (e non solo) di discernere il vero dal falso, vi è l'esplosione dei contenuti generati dall'intelligenza artificiale, in particolare i cosiddetti *deepfake*.

Con questo termine si indicano immagini, video o audio creati o alterati tramite algoritmi di intelligenza artificiale in modo talmente realistico da simulare situazioni mai avvenute. Si va dai volti di personaggi celebri sovrapposti ad altri corpi fino alle voci di familiari clonate per ingannare qualcuno al telefono.

I deepfake rappresentano una sfida inedita sul punto della *costruzione della verità*: nell'era in cui ogni testo, suono o immagine può essere contraffatto digitalmente, il tradizionale adagio "seeing is believing" perde di significato.

Per gli adolescenti, nativi digitali abituati a fruire di foto e video come linguaggio quotidiano, il dilagare dei deepfake può avere ripercussioni profonde.

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

Da un lato rischiano di diventare pubblico ingenuo di verosimiglianze ingannevoli: ad esempio, potrebbero imbattersi in falsi video scandalistici di figure pubbliche o in notizie allarmanti corredate da immagini manipolate, prendendoli per autentici e diffondendoli ulteriormente.

Dall'altro lato, essi stessi possono divenire vittime dirette di questa tecnologia.

Un fenomeno molto grave, e purtroppo in crescita, è l'uso di deepfake per il bullismo e la vendetta tra coetanei utilizzando contenuti pornografici. Ragazze minorenni hanno visto il proprio volto artificiosamente inserito su video porno trovati online, allo scopo di umiliarle pubblicamente; analogamente ragazzi possono essere bersaglio di deepfake denigratori.

Non solo ragazze – spesso le più colpite da fenomeni di sexual shaming – ma anche i ragazzi possono subirne gli effetti devastanti. La possibilità di creare con pochi clic immagini esplicite e non consensuali di un compagno di classe configura una nuova forma di abuso digitale che mina la dignità e la sicurezza psicologica delle giovani vittime, causando traumi e vergogna difficilmente rimediabili.

Come evidenziato, questa tendenza erode le basi della fiducia e della sicurezza nei contesti educativi, richiedendo urgentemente strategie di contrasto e sensibilizzazione. Un altro campo dove i contenuti generati da intelligenza artificiale incidono pesantemente è quello della criminalità online. Purtroppo, le stesse tecniche di generazione usate per scopi ludici possono essere sfruttate in modo aberrante, ad esempio per produrre materiale pedopornografico sintetico.

Nel febbraio 2025 Europol ha coordinato la prima operazione globale contro un circuito criminale che diffondeva immagini di abusi su minori create interamente tramite intelligenza artificiale: l'Operazione "Cumberland" ha portato a decine di arresti in 19 Paesi e ha svelato una piattaforma online in cui, previo pagamento, era possibile accedere a video generati digitalmente che mostravano bambini abusati.

Sebbene in tali contenuti non vi fossero vittime reali, Europol ha evidenziato come l'AI-CSAM (*Child Sexual Abuse Material* generato da *Artificial Intelligence*) contribuisca comunque a oggettivare e sessualizzare i bambini, alimentando fantasie e domanda di materiale pedopornografico.

Il caso ha sollevato anche un problema di gap normativo: molte legislazioni nazionali non avevano (fino a quel momento) tipi di reato pensati per punire immagini di abuso "fittizie", rendendo difficoltoso per gli inquirenti intervenire prontamente.

Si tratta di un esempio estremo, ma emblematico, di come i contenuti generativi possano creare danno sociale anche senza una vittima diretta, richiedendo un rapido adeguamento delle leggi e delle strategie di contrasto.

Ma i rischi non terminano qui. I deepfake audio hanno già alimentato truffe ed estorsioni: sono noti casi, anche in cronaca recente, di genitori

contattati da sedicenti rapitori con in sottofondo la voce (clonata via intelligenza artificiale) della figlia in lacrime, per inscenare falsi rapimenti e chiedere riscatti.

Questi *virtual kidnapping scams* sfruttano l'emotività familiare e la potenza dell'intelligenza artificiale vocale, gettando nel panico persone ignare. La facilità con cui pochi secondi di audio da un social network possono essere sufficienti per riprodurre la voce di un adolescente solleva comprensibili allarmi: come proteggersi da un mondo in cui non si può più credere neanche alle proprie orecchie?

Siamo di fronte, in sintesi, a una vera e propria *crisi della realtà*, in cui l'evidenza sensibile (ciò che vediamo/ascoltiamo) non garantisce più verità.

Per i nativi digitali questo scenario rischia di tradursi in due effetti opposti ma ugualmente problematici: o una credulità totale verso qualunque contenuto multimediale accattivante (esponendoli a manipolazioni continue), oppure un cinico scetticismo verso tutto ("non ci si può fidare di nulla"), con conseguente disorientamento e sfiducia anche nelle informazioni corrette.

Come arginare, allora, l'impatto destabilizzante dei contenuti di intelligenza artificiale sulla percezione della verità?

Su un piano normativo, diversi Paesi si stanno muovendo per reprimere gli abusi più gravi: ad esempio il Regno Unito ha annunciato leggi per criminalizzare esplicitamente la diffusione di deepfake pornografici senza consenso.

Anche l'UE, con il *Digital Services Act* e il regolamento sull'intelligenza artificiale, spinge verso *obblighi di trasparenza* (ad esempio etichettare i contenuti sintetici) e strumenti di *rilevazione automatica* dei deepfake.

Tuttavia, norme e tecnologie per il contrasto da sole non bastano.

Occorre inserire, ad esempio, nei programmi educativi moduli didattici sulla *sinthetic media literacy*, per insegnare ai ragazzi a riconoscere indizi di falsificazione nei video e nelle immagini, a usare strumenti di verifica (come il *reverse image search*) e in generale a sviluppare un sano dubbio verso i media digitali iper-realistici.

Allo stesso tempo, a livello psicologico, va creata una rete di supporto per le vittime di *deepfake abuse*, equiparando questo tipo di cyber-violenza alle forme tradizionali di molestia e bullismo, con protocolli di intervento nelle scuole.

Genitori e docenti devono essere formati anche su questi nuovi rischi: ad esempio, un genitore allertato sull'esistenza delle truffe con voce clonata potrà istruire i familiari su come reagire (chiamando subito il numero diretto del congiunto, ad esempio, per verificare).

Sul fronte dei social media, sarebbe auspicabile allo stesso tempo l'integrazione di *filtri automatici* che segnalino o blocchino i deepfake dannosi: alcune piattaforme stanno sviluppando *watermark* invisibili per contrasse-

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

gnare i contenuti originali, o algoritmi che riconoscano imperfezioni tipiche dei media sintetici.

A nostro avviso, anche i contenuti generati dall'intelligenza artificiale costituiscono un banco di prova cruciale per la *tenuta della verità* nell'era digitale. Se ben governati, potranno avere usi positivi (si pensi all'intrattenimento, alla creatività, alla ricostruzione storica); se lasciati senza controllo e senza un'adeguata preparazione del pubblico giovane, rischiano di amplificare all'estremo le patologie informative e relazionali già evidenti.

La posta in gioco è la capacità delle nuove generazioni di distinguere realtà e finzione, di continuare a credere in un nucleo di fatti condivisi su cui basare la convivenza civile. In fondo, la vera sfida che l'intelligenza artificiale pone ai minori d'oggi è una sfida di *coscienza critica*: educarli a vivere in un mondo dove la realtà può essere "falsificata" significa rafforzarli interiormente, dare loro bussola e strumenti per non perdere l'orientamento.

8. Conclusioni: verso un ambiente digitale più giusto e sicuro per i minori. Una proposta sistemica e multidisciplinare

Dalle analisi svolte nei paragrafi precedenti emerge con chiarezza come la questione dei minori nella società digitale sia estremamente *complessa* e *multidimensionale*.

Non esistono soluzioni semplici, né interventi isolati in grado di garantire da soli uno spazio online giusto e sicuro per bambini e adolescenti.

Al contrario, serve un *approccio sistemico*, che coinvolga sinergicamente aspetti normativi, tecnologici, educativi e culturali, facendo dialogare competenze diverse (giuridiche, sociologiche, informatiche, pedagogiche, psicologiche).

In questa conclusione, ci pare opportuno delineare, allora, una proposta d'azione integrata, ispirata ai principi emersi e alle migliori pratiche evidenziate.

In primo luogo, il quadro normativo va aggiornato e rafforzato per tenere il passo con l'innovazione tecnologica. Ciò implica, ad esempio, l'introduzione di obblighi stringenti e standard condivisi di verifica dell'età per tutte le piattaforme frequentate da minori.

Le sperimentazioni come il regolamento AGCOM sul doppio anonimato sono un buon punto di partenza: tali modelli potrebbero essere estesi oltre i siti vietati ai minori, prevedendo che anche social network e servizi di streaming implementino sistemi di *age assurance* certificati, in grado di distinguere un dodicenne da un maggiorenne senza violare la privacy individuale.

Parallelamente, vanno colmati i vuoti legislativi emersi: ad esempio, criminalizzando esplicitamente la produzione e diffusione di deepfake lesivi della persona e aggiornando la definizione di materiale pedopornografico

per includervi i contenuti di intelligenza artificiale sintetici che sessualizzano minori (come molti ordinamenti già prevedono).

A livello europeo, il *Digital Services Act* e il recente regolamento sull'intelligenza artificiale dovranno essere implementati ponendo particolare attenzione ai diritti dei minori: ad esempio, imponendo valutazioni di impatto specifiche sui rischi per i minori da parte delle grandi piattaforme e vincolando queste ultime a misure di protezione dell'utenza minore (modalità con contenuti adatti all'età, limitazione profilazione pubblicitaria sotto una certa età, etc.).

Inoltre, sarebbe auspicabile recepire nelle normative nazionali ed europee il principio del "superiore interesse del bambino" ("*best interest of the child*") in ogni disciplina attinente al digitale, come raccomandato dal Comitato ONU sui Diritti dell'Infanzia (*General Comment* n. 25/2021).

Questo orientamento aiuterebbe a bilanciare correttamente, in sede interpretativa, le eventuali tensioni tra protezione dei dati, libertà di espressione e tutela dei minori.

In secondo luogo, il settore tecnologico e industriale deve fare la sua parte abbracciando il paradigma della "protezione by design" e "by default" nei confronti degli utenti minori.

Le grandi piattaforme dovrebbero proattivamente implementare sistemi interni di *child safety*: ad esempio, utilizzando l'intelligenza artificiale non solo per profilare a scopi di marketing ma, anche, per individuare e bloccare tempestivamente fenomeni come il grooming, il cyberbullismo reiterato e la diffusione virale di sfide pericolose.

Strumenti di *parental control* efficaci, modalità "under 13" con funzionalità limitate, opzioni di filtro avanzato dei contenuti generati dall'intelligenza artificiale (per impedire output inappropriati ai minori) possono essere tutte innovazioni tecniche a portata di mano che le aziende possono adottare responsabilmente.

Un impegno particolare va richiesto, a nostro avviso, alle società che sviluppano modelli generativi e chatbot: esse dovrebbero integrare dall'inizio nei loro sistemi dei "paletti etici", ad esempio classificando come *adult-only* certi contenuti e fornendo kit che permettano agli sviluppatori terzi di attivare controlli d'età sulle proprie implementazioni.

Inoltre, si auspica una maggiore trasparenza algoritmica: rendere pubbliche – almeno alle autorità garanti e a esperti indipendenti – le logiche di raccomandazione e moderazione aiuterebbe a identificare bias o falle che colpiscono i minori (si pensi agli algoritmi di TikTok che possono aver spinto minori verso contenuti estremi).

In quest'ottica, la creazione di comitati etici con partecipazione anche di esperti di sviluppo infantile, chiamati a supervisionare gli effetti delle piattaforme sui giovani, potrebbe diventare una best practice di responsabilità sociale d'impresa.

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

In terzo luogo, l'asse educativo e culturale è forse il più importante nel lungo periodo. È indispensabile strutturare un programma organico di alfabetizzazione digitale rivolto sia ai minori sia agli adulti di riferimento (Lancini 2025).

La scuola deve consolidare il percorso iniziato: l'educazione civica digitale non deve restare una materia secondaria, ma deve essere trattata con pari dignità delle altre discipline, con verifiche di apprendimento e progetti concreti (Pasta, Rivoltella 2022; Viola 2021).

Contemporaneamente, è utile coinvolgere gli stessi ragazzi come *peer educator*: molti progetti mostrano che quando sono i giovani a farsi portavoce presso i pari dei messaggi di uso responsabile, l'efficacia cresce (Van Zalk, Monks 2020).

Sul fronte familiare, vanno incentivate iniziative di *parental training*: corsi serali per genitori sulla sicurezza online, guide pratiche diffuse attraverso le strutture mediche, campagne sui media che offrano consigli semplici su come attivare protezioni o su come parlare di Internet coi figli.

In generale, servirebbe alimentare una cultura diffusa in cui l'educazione digitale del minore sia percepita come parte integrante della sua educazione tout court, e non come un ambito tecnico riservato agli "esperti di computer".

Un cambio di mentalità è avvenuto in passato su altri temi (educazione stradale, educazione alla salute); allo stesso modo, dovrà diventare naturale occuparsi della "salute digitale" dei figli, con attenzione e senza tabù (Betton, Woollard 2018).

Infine, l'approccio sistemico implica *collaborazione* e *multidisciplinarietà*.

Le sfide digitali riguardanti i minori sono trasversali e richiedono che tutti gli stakeholder cooperino. È auspicabile la creazione di tavoli di lavoro permanenti dove autorità (Garante Privacy, Garante Infanzia, Polizia Postale), aziende tech, mondo della scuola, associazioni genitoriali e magari rappresentanti degli stessi ragazzi s'incontrino per condividere informazioni e coordinare azioni.

Questa rete andrebbe ampliata e resa più operativa, per affrontare prontamente fenomeni emergenti, e anche a livello internazionale la condivisione di best practices diventa fondamentale: Europol e Interpol già cooperano con task force specifiche su crimini online contro minori, scambiando expertise su come rintracciare, ad esempio, autori di adescamento.

In conclusione, costruire un ambiente digitale più giusto e sicuro per i minori significa garantire loro il diritto di navigare senza subire prevaricazioni, sfruttamento o manipolazioni e, al contempo, il diritto di esprimersi, apprendere e partecipare appieno alla vita digitale.

È un equilibrio delicato, che richiede un impegno congiunto – delle istituzioni, del mondo tecnologico, della scuola e della famiglia – nel nome di una generazione che sta crescendo in un contesto mai sperimentato prima dall'umanità.

Bibliografia

Betton, V., Woollard, J., (2018), *Teen Mental Health in an Online World: Supporting Young People around their Use of Social Media, Apps, Gaming, Texting and the Rest*, London, Jessica Kingsley Publishers.

Bianda, E., (2019), Riconoscimento facciale e capitalismo della sorveglianza, in *Problemi dell'informazione*, 2, pp. 400-400, DOI 10.1445/94261.

Biolcati, R., (2010), La vita online degli adolescenti: tra sperimentazione e rischio, in *Psicologia clinica dello sviluppo*, 41 (2), pp. 267-298.

Biolcati, R., Cani, D., Badio, E., (2013), Adolescenti e Facebook: la gestione online della privacy, in *Psicologia clinica dello sviluppo*, 2013, 51 (3), pp. 449-478.

Blake, P., (2019), Age verification for online porn: more harm than good? in *Porn studies*, 6 (2), pp. 228-237.

Caggiano, I.A., (2022) Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law, in *European Journal of Privacy Law & Technologies*, 1, pp. 27-44.

Cantero Gamito, M., (2023), Do Too Many Cooks Spoil the Broth? How EU Law Underenforcement Allows TikTok's Violations of Minors' Rights, in *Journal of consumer policy*, 46 (3), pp. 281-305.

Carr, N. (2025), *Superbloom. Le tecnologie di connessione ci separano?*, Milano, Cortina.

Frigato, P., (20121), Capitalismo della sorveglianza e fallimento del modello di mercato, in *Sociologia del lavoro*, 159, pp. 270-28.

Gallese, V., Moriggi, S., Rivoltella, P.C., (2025), *Oltre la tecnofobia. Il digitale dalle neuroscienze all'educazione*, Milano, Cortina.

Garaci, I., (2023), The child's right to privacy in the family context, in *European Journal of Privacy Law & Technologies*, 1, pp. 84-99.

Ghiglia, A. (2023), *Educazione civica digitale. Abbecedario essenziale*, Rimini, Maggioli.

Lancini, M., (2025), *Chiamami adulto. Come stare in relazione con gli adolescenti,* Milano, Cortina.

Li, J., (2025), Reflection on data right protection for minors in the digital age, in *Children and youth services review*, 170 (5): 108167, DOI: https://doi.org/10.1016/j.childyouth.2025.108167.

Macenaite, M., Kosta, E., (2017), Consent for processing children's personal data in the EU: following in US footsteps?, in *Information & communications technology law*, 26 (2), pp. 146-197.

Murgo, C., (2024), L'identità personale dei minori, tra responsabilità genitoriale e capacità di autodeterminarsi, in *European Journal of Privacy Law & Technologies*, 2, pp. 115-128.

Nagel, D. (2011-12), Beware of the Virtual Doll: ISPs and the Protection of Personal Data of Minors, in *Philosophy & technology*, 24 (4), pp. 411-418.

Pasquale, L., Zippo, P., Curley, C., O'Neill, B., Mongiello, M., (2022), Digital Age of Consent and Age Verification: Can They Protect Children?, in *IEEE software*, 39 (3), pp. 50-57.

Pasta, S., Rivoltella P.C., (2022), a cura di, *Crescere onlife. L'educazione civica digitale progettata da 74 insegnanti-autori*, Brescia, Scholé-Morcelliana.

Pesci, G., (2024), *Educazione civica e cittadinanza digitale. Percorsi educativi nella società dell'informazione*, Milano, Giuffrè.

Savonardo, L., Marino, R., (2021), *Adolescenti always on. Social media, web reputation e rischi online*, Milano, FrancoAngeli.

Scalzaretto, S., (2023), Minori e disabilità nell'era dello sharenting. Il "diritto ad un futuro aperto" come criterio per una valutazione etica, in *Medicina e morale*, 72 (2), pp. 191-206.

Slavtcheva-Petkova, V. (2023), *Young People, Media and Politics in the Digital Age*, Routledge, DOI: 10.4324/9781003201632.

Stardust, Z., Obeid, A., McKee, A., Angus, D., (2024), Mandatory age verification for pornography access: Why it can't and won't 'save the children', in *Big data & society*, 11 (2), DOI: 10.1177/20539517241252129.

Talley, V.A.M., (2021), Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children Under the GDPR, in *Indiana international & comparative law review*, 30 (1), pp. 127-162.

Viola, J.K., (2021), *Young People's Civic Identity in the Digital Age*, Cham, Springer Nature Switzerland AG, 2021.

Yar, M., (2020), Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK, in *Policing : an international journal of police strategies & management*, 43 (1), pp. 183-197.

Zalk, N. van, Monks, C.P., (2020), eds., *Online Peer Engagement in Adolescence: Positive and Negative Aspects of Online Social Interaction*, New York, Routledge.

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

Le rappresentazioni dei bullismi nell'evoluzione della normativa: uno sguardo interdisciplinare

(Cyber)Bullying Representations in the Transformation of Legislation: Interdisciplinary Insights

Anna Rosa Favretto[1], Elena Ferrara[2], Riccardo Michele Colangelo[3]

Sommario[4]

L'articolo intende analizzare il tema degli atti di prevaricazione in Rete tra preadolescenti e adolescenti e la principale normativa che a essi si riferisce.
Dopo aver sottolineato alcune difficoltà teoriche che si incontrano nella definizione dell'oggetto di studio, con la conseguente scarsa accuratezza nella raccolta dei dati, verranno evidenziate le caratteristiche comuni tra le differenti forme di bullismo, così come le loro specificità. Saranno inoltre presentati alcuni dati secondari sul fenomeno oggetto dell'articolo, il cyberbullismo.
L'articolo proseguirà approfondendo alcuni aspetti prettamente giuridici. Verrà esaminata, nell'ambito dei più rilevanti interventi normativi in Europa, la principale normativa italiana sul tema (L. 71/2017), come recentemente integrata dalla L. 70/2024, la quale contribuisce, in modo più ampio, anche a ridisegnare il contesto normativo di riferimento, caratterizzato da una crescente complessità.
Sintetici approfondimenti riguarderanno le problematiche applicative correlate anche alla incompleta attuazione della disciplina vigente, nonché la coesistenza di altre norme potenzialmente rilevanti nell'affrontare le disfunzioni relazionali delle giovani generazioni.

1 Università degli Studi di Torino, Dipartimento di Psicologia. annarosa.favretto@unito.it

2 Senatrice XVII Legislatura, esperta Consiglio Nazionale degli Utenti. elena.ferrara58@gmail.com.

3 Universitas Mercatorum, Facoltà di Scienze Economiche e Giuridiche. riccardomichele.colangelo@studenti.unimercatorum.it.

4 Pur essendo frutto di comune riflessione, Anna Rosa Favretto è autrice del paragrafo 1, Riccardo Michele Colangelo dei paragrafi 2 e 3 ed Elena Ferrara, con Riccardo Michele Colangelo, del paragrafo 4. Le conclusioni sono state formulate congiuntamente.

Data invio: 1 luglio 2025. Data accettazione: 8 agosto 2025.
DOI: https://doi.org/10.54103/1972-5760/30054

Si evidenzieranno, inoltre, alcune costanti e peculiarità delle normative regionali a ora esistenti.
Infine, verranno evidenziati i paradigmi prevalenti utilizzati per prevenire e contrastare il fenomeno in Italia, discutendoli alla luce del mandato normativo della CRC del 1989.

Parole chiave: bullismo; cyberbullismo; normativa; partecipazione; adolescenza

Abstract

This article aims to analyze online abuse among preadolescents and adolescents, along with the key legal frameworks addressing it.
After outlining theoretical challenges in defining the object of study – and the resulting limitations in data accuracy – the study identifies common characteristics and distinctions among different forms of bullying. It also presents secondary data on the focus of this study: cyberbullying.
The discussion then turns to legal dimensions, reviewing the most significant regulatory measures in Europe, with a focus on the key Italian legislation (Law 71/2017), as recently amended by Law 70/2024, which contributes to reshaping an increasingly complex regulatory landscape.
The article briefly explores practical challenges, including gaps in the implementation of current legislation, and the coexistence of other potentially relevant norms in addressing relational dysfunctions among younger generations.
Additionally, it highlights recurring patterns and distinctive features in the Italian regional laws currently in force.
Finally, the article discusses the prevailing paradigms for preventing and combating cyberbullying in Italy, assessing them in light of the 1989 UN Convention on the Rights of the Child (CRC).

Key words: bullying; cyberbullying; legislation; participation; adolescence

1. I bullismi: problemi di definizione e problemi di rilevazione

1.1 La difficile definizione di due fenomeni sociali complessi

Gli atti di prevaricazione tra pari sono fenomeni sociali diffusi (Gazzelloni, Istat, 2023). Essi si ripercuotono non soltanto sulle vittime, sugli aggressori, sui pari e su tutti coloro che assistono, o che indirettamente partecipano, alle prevaricazioni, ma anche sulle famiglie, sui gruppi e sui contesti più ampi in cui si realizzano e, con cerchi concentrici sempre più estesi, anche sulle reti sociali e sulle comunità, di cui possono minare la fiducia interpersonale e sistemica.

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

Desta preoccupazione nell'opinione pubblica e tra gli studiosi anche l'aspetto longitudinale di tali fenomeni. Infatti, le possibili conseguenze di medio e di lungo periodo, rilevate da una consistente letteratura scientifica (si vedano tra gli altri Mark et al., 2019; Brunstein Klomek et al., 2010; Hunter et al., 2014; Wolke et al., 2001) possono incidere sulla vita prossima e futura delle vittime, su quella di coloro che agiscono le prevaricazioni, sui gruppi e sulle comunità di riferimento.

Nelle ultime decadi, a livello mondiale si sta manifestando un aumento dell'attenzione sul tema. Tale incremento è registrabile anche in Italia, considerato il moltiplicarsi di programmi educativi (Elisa, 2023), soprattutto in ambito scolastico, che intendono prevenire e contrastare i bullismi, così come il diffondersi di ricerche condotte non più soltanto su scala locale e circoscritta, ma anche nazionale; infine, appare rilevante il recente affacciarsi sulla scena normativa di interventi legislativi nazionali e regionali.

Dal punto di vista dell'analisi sociologica è interessante, a nostro avviso, innanzitutto interrogarsi sulle ragioni di tale crescente interesse, che frequentemente assume l'aspetto dell'allarme sociale. Si tratta di un incremento d'attenzione che non appare scientificamente imputabile a un documentabile e rilevante aumento degli atti di prevaricazione tra pari. Infatti, come vedremo a breve, la mancanza di dati relativi a tempi risalenti, insieme con la scarsità dei dati recenti e la disomogeneità della loro raccolta, non consentono di compiere fondati raffronti tra passato e presente. È più ragionevole ipotizzare che la mutata sensibilità del mondo occidentale rispetto alla salute e al benessere dell'infanzia e dell'adolescenza, insieme con la stabilizzazione e la diffusione della rappresentazione della pre-adolescenza e dell'adolescenza come periodi della vita "a rischio" – rappresentazione che sta alla base dell'idea moderna di adolescenza, a partire dalla sua individuazione e denominazione secondo criteri contemporanei, a opera di Hall (1904) – giochino un ruolo importante sia nell'individuazione di tali fenomeni, sia nella crescente diffusione delle azioni di prevenzione e di contrasto.

A fronte di tale trasformazione nella percezione e nella costruzione del fenomeno, si impone, innanzitutto, la questione definitoria. Quali caratteristiche specifiche connotano l'oggetto di questa costruzione sociale? Come vengono definiti e caratterizzati gli atti di prevaricazione tra pari, in particolare quando li si denomina "bullismo" e "cyberbullismo"? In secondo luogo, non può sfuggire come per trattare il tema del cyberbullismo, oggetto centrale del presente lavoro, sia necessario ricostruire seppur brevemente il concetto di bullismo, a cui il cyberbullismo stesso è legato sia in termini definitori, sia in termini di applicazione delle politiche e degli interventi educativi.

Come è noto, la storia del concetto di bullismo colloca i suoi inizi negli anni settanta del secolo scorso ad opera di Olweus il quale, nei suoi studi pionieristici, si riferiva agli atti di prevaricazione in ambito scolastico, indi-

viduandone almeno tre caratteristiche connotative che permangono anche nelle sue definizioni successive: l'offesa deliberata, la reiterazione dell'offesa, l'asimmetria di potere tra la vittima e il prevaricatore (Olweus 2001).

Non è possibile, in questa sede, ripercorrere la storia della definizione del bullismo e le sue sfaccettature. Preme, tuttavia, rilevare come alle caratteristiche individuate da Olweus sono state affiancate, e talvolta sostituite, altre caratteristiche ritenute rilevanti. Tra tutte segnaliamo, per la loro peculiarità in ambito minorile, la necessità della percezione che l'atto agito sia abusante, e ciò da parte della vittima, del prevaricatore e degli altri attori o spettatori degli atti di prevaricazione (cfr., tra gli altri, Rigby, 2002; Bacchini, 2007; Belacchi, Biagetti, 2007; Aalsma, 2008; Buccoliero, Maggi, 2018); ancora, appare rilevante la strutturazione del contesto nel quale avvengono le azioni. A proposito di quest'ultimo aspetto, merita sottolineare come il bullismo, già a partire dalla sua prima definizione, sia stato inteso non come un comportamento individuale, una semplice manifestazione di disagio soggettivo, ma come un fenomeno di natura relazionale. Proprio ponendo particolare attenzione alle relazioni, alcuni studiosi (cfr., tra gli altri, Pepler et al., 2008) hanno definito e analizzato il fenomeno in rapporto alle modalità di strutturazione delle relazioni presenti nei contesti nei quali le prevaricazioni vengono attuate, insieme con il differenziale di potere che le sostiene (Iannaccone, 2007). L'attenzione ai contesti ha permesso di riservare considerazione non soltanto agli attori che effettuano e che subiscono le prevaricazioni, ma anche alle dinamiche di potere relative a tutti gli attori presenti negli ambiti in cui avvengono le prevaricazioni, sia che svolgano ruoli attivi, sia che assistano passivamente. E ciò include anche le persone adulte (Horton, 2011; Bacchini, 2007).

Attualmente l'attenzione al contesto inteso in senso ampio rappresenta uno dei pilastri portanti dell'opera di revisione del concetto di bullismo e, congiuntamente, della definizione di cyberbullismo. Questo aspetto è stato ben illustrato dalla Comitato Scientifico del World Anti-Bullying Forum, incaricato dall'UNESCO, tra il 2020 e il 2021, di individuare una nuova definizione di bullismo scolastico da sottoporre a un'analisi consensuale da parte di esperti e di portatori di interesse. La proposta di nuova definizione si è connotata per una concezione del bullismo come insieme di comportamenti prevaricatori che coinvolgono tutti gli attori presenti sulla scena della prevaricazione, in modo strettamente intrecciato al contesto scolastico e al contesto sociale in cui tali attori vivono e agiscono. Nella proposta si evidenzia, dunque, come tali comportamenti possano trovare tanto le ragioni della propria esistenza, quanto le ragioni per il contrasto non soltanto nei soggetti direttamente coinvolti, ma anche nei gruppi sociali primari e nelle comunità di appartenenza. Per questa ragione, il Forum ha invitato gli studiosi, gli educatori e anche i legislatori ad adeguare le definizioni di bullismo e di cyberbullismo, e le conseguenti attività di prevenzione e di contrasto,

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

anche in relazione alle caratteristiche dei contesti sociali e relazionali in cui si manifestano con maggiore frequenza gli atti prevaricanti

Anche le modalità di attuazione delle prevaricazioni cambiano con il mutare dei tempi. L'introduzione massiccia della rete digitale e la facilità del suo accesso hanno stimolato ormai da anni la produzione di nuove forme di sopruso tra pari, a cui è necessario prestare attenzione per comprendere aspetti importanti della vita dei pre-adolescenti e degli adolescenti. Inoltre, il facile accesso ai dispositivi che permettono la connessione alla rete ha amplificato la diffusione e la risonanza degli atti di prevaricazione (De Salvatore, 2012). Tuttavia, nonostante il fiorire di studi sull'argomento, anche per il cyberbullismo non esiste una definizione acclarata e univoca e le caratteristiche che vengono evidenziate dagli studiosi, in quanto ritenute connotative del fenomeno, frequentemente non sono condivise dall'intera comunità scientifica. Anche per il cyberbullismo ci limiteremo a illustrare alcune questioni che riteniamo centrali per la discussione della normativa che proporremo oltre, cominciando con il ricordare che sebbene eminenti studiosi del tema del bullismo, come Olweus e Linber (2018) abbiano ritenuto che i due fenomeni non presentino sostanziali differenze, altri, con visione opposta (cfr. la ricostruzione di Ansary, 2020) hanno individuato caratteristiche così specifiche da considerare gli atti di prevaricazione in rete come fenomeno sociale disgiunto dal fenomeno degli atti di prevaricazione agiti nelle relazioni in presenza.

Tra le molte questioni che creano perplessità in merito alla sovrapposizione completa delle due forme di prevaricazione, riteniamo interessanti quelle connesse al differenziale di potere e alla volontà di procurare danno che, come si ricordava poc'anzi, sono da sempre state considerate caratteristiche imprescindibili per la definizione del bullismo. Nella rete, il differenziale di potere risulta di difficile individuazione; inoltre, il danno procurato alla vittima dal permanere in rete di materiali offensivi può andare ben oltre la volontà di offesa dell'aggressore, soprattutto se di giovane età e ancora troppo inesperto per comprendere appieno le potenzialità di reiterazione nel web di un singolo atto aggressivo. Anche la facilità – fisica e psicologica – con la quale è possibile realizzare aggressioni in rete, spesso sotto la copertura di un vero o presunto anonimato, sembrano rendere il fenomeno del cyberbullismo dotato di una natura propria, soltanto parzialmente sovrapponibile a quella del bullismo.

Il moltiplicarsi degli studi sul cyberbullismo ha offerto anche tentativi di integrazione delle varie definizioni (cfr., come esempio, Peter, Petermann, 2018), ponendo in risalto come il nucleo comune sia rappresentato proprio dalla prevaricazione agita deliberatamente, ossia dalla volontà di danneggiare, ferire, mettere in imbarazzo la vittima degli atti di aggressione perpetrati in rete.

Ansary (2020), con una accurata revisione della letteratura recente, ha trovato serie indicazioni per ritenere che i fenomeni del bullismo e del cyberbullismo siano correlati ma distinti, e come di questa non identità si debba tenere lucidamente conto quando si tratti di progettare politiche e interventi educativi. L'autore sottolinea come allo stato attuale i lavori sul cyberbullismo siano ancora largamente descrittivi e come manchino modelli teorici di riferimento che permettano di studiare e di interpretare correttamente gli atti di prevaricazione in rete.

Un'efficace proposta arriva da Thomas et al. (2015) che, con lo scopo di arrivare a definire in modo specifico bullismo e di cyberbullismo, soprattutto in vista della loro corretta misurazione, ritengono che si debbano integrare alle tre caratteristiche proposte da Olweus (Olweus, Limber, 2018) nella sua riproposizione più recente della definizione di bullismo, ossia l'intenzione, la reiterazione e la presenza di un differenziale di potere, due caratteristiche del cyberbullismo molto presenti negli studi sul tema, ossia l'anonimato e l'ampia diffusione in rete.

Come appare chiaro la questione definitoria non è un mero esercizio fine a sé stesso. Infatti, dalla definizione adottata discendono le modalità di misurazione dei due fenomeni, così come le politiche di prevenzione e di contrasto e i percorsi educativi (Beltran-Catalan, Cruz-Catalan, 2020). Arrivare a definizioni stabilizzate e condivise è necessario per individuare indicatori scientificamente fondati e condivisi dalla comunità scientifica. Diversamente, sarà difficile conoscere in modo adeguato l'estensione e le caratteristiche di questi fenomeni, al fine di contrastarli.

1.2 Definizione dei bullismi secondo il principio della Participation

Tra le critiche più frequenti mosse alle definizioni di bullismo e di cyberbullismo troviamo almeno due argomenti rilevanti per la comprensione dei due fenomeni. Il primo riguarda la critica alla sistematica mancanza di attenzione ad alcune variabili che potrebbero influenzare in modo preminente sia gli atti prevaricanti, sia i contesti nei quali tali atti si realizzano. In particolare, gli studiosi si riferiscono alla mancanza di attenzione per la classe sociale, per le differenti culture di appartenenza, per le strutture di genere, per la struttura del contesto a cui appartengono gli attori sulla scena della prevaricazione.

Si ritiene, infatti, che conoscere le dinamiche e la strutturazione dei contesti possa cogliere più compiutamente la dinamicità dei fenomeni di bullismo e di cyberbullismo, i quali non sono statici, ma fluidi, soggetti a modificazioni costanti e in itinere, sollecitati ininterrottamente dall'ambiente sociale in cui si manifestano.

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

Inoltre, e questa è la critica su cui vogliamo qui appuntare la nostra attenzione, le definizioni più diffuse di bullismo e cyberbullismo, e le politiche e le pratiche conseguenti, non tengono conto dell'importanza di considerare come centrali i significati attribuiti dai bambini, dai pre-adolescenti e dagli adolescenti ai termini "bullismo" e "cyberbullismo". Come rilevano alcuni autori (cfr., tra gli altri, Canty et al., 2016; Thornberg, 2015) l'adozione di una postura che solleciti la partecipazione delle persone di minore età a tutte le questioni che li riguardino, così come l'espressione del loro punto di vista, richiesta dalla Convenzione dei diritti dell'Infanzia e dell'Adolescenza (in particolare all'articolo 12) hanno spinto un numero crescente di studiosi a costruire piani di rilevazione del fenomeno che tengano in considerazione la voce delle nuove generazioni. Questa mutata considerazione ha condotto allo svilupparsi di percorsi di ricerca che, da un lato, hanno inteso abbandonare definizioni predefinite dei due fenomeni da utilizzare come lente per studiarne caratteristiche e diffusione; d'altro lato, hanno curato la rilevazione di tali caratteristiche secondo l'opinione di tutti gli attori presenti sulla scena in cui si realizzano gli atti di prevaricazione: gli aggressori, le vittime, le loro reti sociali, gli adulti significativi (Mishna et al., 2020). È stato così possibile anche ampliare la conoscenza dei due fenomeni secondo il punto di vista e la definizione che ne danno le persone di minore età vittima di prevaricazione (Vallaincourt et al. 2008). Dredge et al. (2014), per esempio, hanno rilevato soltanto una parziale convergenza tra le definizioni del fenomeno offerte dai ricercatori e quelle espresse da vittime di cyberbullismo, per i quali il primo criterio per individuare questo tipo di sopraffazione era un criterio soggettivo, ossia l'impatto negativo sulla vittima, criterio non così centrale nelle tradizionali definizioni di cyberbullismo rintracciabili nella letteratura scientifica e nelle ricerche.

Per l'ambito italiano è ancora oggi interessante il lavoro di Menesini et al. (2011) i quali, raccogliendo il punto di vista di un gruppo di adolescenti sulla definizione di cyberbullismo e sulle sue caratteristiche, hanno rilevato nei ragazzi e nelle ragazze coinvolti nella ricerca anche l'attribuzione di caratteristiche specifiche e di gravità differenziate delle prevaricazioni in rete e in presenza.

Secondo questa linea di pensiero attenta al dettato della CRC relativo alla Participation, dunque, soltanto riservando attenzione alla partecipazione delle giovani generazioni alla definizione dei due fenomeni e all'individuazione delle loro caratteristiche, ponendo contemporaneamente attenzione al contesto nel quale avvengono gli atti di prevaricazione e all'influenza di alcune variabili centrali si potranno fornire spunti efficaci per rendere la conoscenza scientifica più capace di comprendere gli atti di prevaricazione tra pari e per costruire politiche e interventi educativi più adeguati alla loro prevenzione e al loro contrasto (Favretto, Torre, 2024).

1.3 Le dimensioni del bullismo e del cyberbullismo

Un problema rilevante per la conoscenza degli atti di prevaricazione tra pari di minore età è la disomogeneità delle metodologie di rilevazione insieme con la disomogeneità delle definizioni di riferimento. Ciò vale in modo accentuato anche per il nostro Paese, per il quale soltanto recentemente sono disponibili dati raccolti in modo sistematico, sebbene ancora largamente improntati a una visione soltanto parzialmente partecipativa. La mancanza di raccolte sistematiche riguardanti il passato permette di arrivare a valutare soltanto parzialmente la diffusione e le caratteristiche del bullismo e del cyberbullismo secondo variabili sufficientemente condivise dai ricercatori.

Nell'economia del presente lavoro ci limiteremo a individuare e a segnalare alcune tendenze significative che provengono da ricerche nazionali realizzate negli ultimi anni, concentrandoci, laddove possibile, sugli aspetti che riguardano il cyberbullismo, oggetto del presente lavoro.

Nel nostro Paese, la prima ricerca nazionale di riferimento sul bullismo e il cyberbullismo è stata realizzata dall'Istat (2014) che aveva rilevato in un'indagine campionaria annuale la presenza apprezzabile di entrambi i fenomeni nella popolazione di ragazzi e ragazze di età compresa tra gli 11 e i 17 anni. Una ricerca successiva aveva evidenziato come il bullismo e il cyberbullismo fossero più accentuati per i ragazzi di origine straniera (ISTAT, 2015), dimostrando ancora una volta che alcune variabili modulano in modo rilevante questi fenomeni.

L'ISTAT ha poi dato avvio a raccolte sistematiche. La prima di queste riguarda il 2021, di cui sono a oggi disponibili i dati (presto saranno disponibili anche i dati della rilevazione 2023) che risultano particolarmente interessanti perché riguardano il periodo immediatamente successivo alla pandemia di Covid-19. Innanzitutto, questa indagine testimonia come le variabili di genere e di cittadinanza siano in grado di influenzare il fenomeno, o la percezione di esso. Sono le ragazze, in misura lievemente maggiore (12,5% contro il 10,3%), a dichiarare di essere state vittima di atti di offesa, di derisione, di diffamazione, di persona e on line, e di violenza fisica, così come sono soprattutto i ragazzi e le ragazze stranieri, per i quali l'essere stati vittima riguarda il 18,2%, contro il 12,5% degli italiani. Anche la variabile dell'età conferma la propria rilevanza: nelle scuole secondarie di primo grado quasi il 14% ha dichiarato di avere subito questi atti di prevaricazione, contro il 9,8% degli studenti e delle studentesse delle secondarie di secondo grado.

Merita di ricordare l'influenza di un'altra importante variabile rilevata dall'ISTAT: la classe sociale di appartenenza. Il bullismo e il cyberbullismo appaiono tanto più diffusi quanto più si manifestano in un quadro di disagio sociale. Come sottolineato dalla ricerca, i ragazzi che ritengono di appartenere a famiglie povere o molto povere dichiarano di avere subito prevarica-

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

zioni nel 16,2% dei casi, mentre coloro che ritengono di appartenere a una famiglia né ricca e né povera sono l'8,1% dei casi e coloro che dichiarano di appartenere a una famiglia ricca sono il 7,9% dei casi. In aggiunta, coloro che dichiarano di non essere bravi a scuola dichiarano di essere stati vittima di prevaricazioni nel 14,8% dei casi, mentre coloro che dichiarano di essere bravi o molto bravi a scuola sono state vittime nell'8% dei casi. Merita ricordare che la classe sociale di appartenenza influenza il successo o l'insuccesso scolastico, come dimostrato da un'ampissima letteratura.

L'influenza di queste variabili induce l'ISTAT a dichiarare che "lo studio del bullismo e del cyberbullismo debba avvenire all'interno d rilevazioni strutturate, che consentono di avere allo stesso tempo informazioni approfondite sul background sociale e scolastico dei ragazzi" (Gazzelloni, ISTAT, 2023, 8).

I dati raccolti da questa ricerca, insieme con quelli del 2014 e del 2015, rendono chiaro come il bullismo e il cyberbullismo rispondano anche a questioni di carattere sociale sulle quali è doveroso intervenire.

Il Ministero dell'Istruzione, accogliendo anche l'impulso al monitoraggio degli atti di prevaricazione in rete dato dalla legge n.71 del 2017, che ha istituito la figura del docente scolastico di riferimento per il cyberbullismo, ha promosso da alcuni anni l'utilizzo della Piattaforma Elisa per il monitoraggio costante del bullismo e del cyberbullismo. Allo stato attuale sono disponibili i dati delle rilevazioni attuate dall'anno scolastico 20/21 a quello 22/23. In sintesi, a fronte di un numero elevato di studenti e di studentesse che hanno partecipato alla rilevazione, e che si è ridotto di un terzo nel corso dei tre anni (185.063 per l'ultima raccolta), i dati segnalano che il 25% degli studenti rispondenti hanno dichiarato di essere stati vittima di bullismo almeno una volta nei mesi immediatamente precedenti alla rilevazione. Il 18% ha dichiarato di aver preso parte ad atti di bullismo. Per quanto riguarda il cyberbullismo, l'8% dei rispondenti ha dichiarato di esserne stato vittima, mente il 7% ha dichiarato di aver preso parte a episodi di prevaricazione in rete. Il monitoraggio 2023 si conclude affermando che mentre si assiste a un aumento di forme sistematiche di vittimizzazione nel corso dei tre anni, il bullismo e il cyberbullismo dichiarati rimangono complessivamente stabili, con un lieve aumento delle forme sistematiche e una lieve diminuzione di quelle occasionali.

Come appare evidente, esiste una apprezzabile differenza tra i dati ISTAT e i dati della Piattaforma Elisa, che rilevano ampiezze e caratteriste dei fenomeni in modo soltanto parzialmente congruente. Tale differenza ben esemplifica quanto dicevamo in apertura a proposito della disomogeneità della raccolta dei dati, delle definizioni adottate e delle caratteristiche attribuite ai fenomeni.

A medesime considerazioni ci conduce il lavoro sul tema condotto da altre serie istituzioni sulla base di campioni importanti, come la wave HBSC

(Health Behaviour in School-aged Children – Comportamenti collegati alla salute in ragazzi di età scolare) rilasciata nel 2024 e relativa al 2022 (campione di ragazzi di 11,13,15, 17 anni, numerosità finale 89.321 relativa a tutto il territorio italiano) che ha rilevato dati più vicini a quelli dell'ISTAT. Infatti, i ragazzi e le ragazze che hanno dichiarato di essere state vittima di bullismo e di cyberbullismo ammontano a circa il 15% per entrambi i fenomeni, con la variabile età che diviene il modulatore principale. È interessante sottolineare che proprio nella fascia d'età 11-13, indipendentemente dal genere, si è assistito a un aumento del cyberbullismo rispetto alle raccolte HBSC precedenti. Così come rilevato dall'ISTAT, infine, il bullismo e il cyberbullismo paiono essere diffusi in tutte le regioni del nostro Paese.

Potremmo illustrare i fenomeni con altri dati ancora, ma la sostanza dell'immagine che se ne ricava non cambierebbe. Continua a non essere possibile, ad oggi, comporre un quadro stabile del bullismo e del cyberbullismo nella loro estensione e nelle loro caratteristiche a livello nazionale.

Oltre alla mancanza di univocità delle definizioni di bullismo e di cyberbullismo e degli strumenti di raccolta, già evidenziate, desideriamo, in conclusione di questa breve disamina, sottolineare come il principio della Participation dei ragazzi e delle ragazze sia ancora poco e per nulla assunto come cardine nella costruzione delle ricerche sul tema. In altre parole, non è semplice trovare ricerche che definiscano i due fenomeni e le loro caratteristiche, e gli strumenti di rilevazione che da esse discendono, sulla base di un lavoro istruttorio compiuto dai ricercatori con ragazzi e ragazzi per cogliere il loro punto di vista, secondo il dettato dell'art. 12 della CRC del 1989.

Inoltre, i dati possono variare anche per l'influenza del contesto di riferimento e di raccolta. Come abbiamo rilevato, molte ricerche riguardano l'ambito scolastico, mentre sarebbe interessante riferirsi anche a contesti extra-scolastici, tenendo presente la loro importanza soprattutto a riguardo del cyberbullismo.

Nonostante ciò, desideriamo, in conclusione, rilevare che, sebbene il quadro conoscitivo degli atti di prevaricazione tra pari pre-adolescenti e adolescenti sia ancora inadeguato e frammentato, la mutata sensibilità dell'opinione pubblica e gli impulsi provenienti da disposizioni normative europee, nazionali e regionali hanno creato le condizioni per un radicale mutamento di rotta.

Ed è proprio sulla normativa di riferimento riguardanti il tema che dedicheremo i nostri approfondimenti successivi.

2. Cenni all'approccio eurounitario al fenomeno del cyberbullismo

Prima di approfondire il quadro normativo italiano in tema di bullismi e, segnatamente di cyberbullismo, risulta opportuno scattare una fotografia dei tratti fondamentali dell'approccio dell'Unione Europea in relazione alla

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

prevenzione ed al contrasto del cyberbullismo, a completamento dei riferimenti sovranazionali sinora evidenziati.

A tal fine, si rileva una sostanziale inerzia del legislatore unionale, laddove non è stato ad oggi compiuto un passo definitivo volto a creare – a livello di fonti secondarie del diritto dell'Unione Europea una disciplina vincolante e direttamente concernente tale fenomeno complesso, volta a perseguire una significativa uniformità in tutti gli Stati membri.

In argomento, se da un lato, guardando ai ragazzi ed alle ragazze coinvolte, non pare assumere carattere predominante la natura transnazionale del fenomeno complesso del cyberbullismo, dall'altro, considerando in modo più ampio anche gli ambienti digitali utilizzati e la relativa governance, emerge *ictu oculi* come il ricorso a strumenti informatici e l'utilizzo, ad esempio, di social network potrebbero giustificare una disciplina comune o, quantomeno, l'individuazione di principi condivisi che – ferme le peculiarità del fenomeno in questione – rendano più incisivo tanto il profilo della tutela, quanto quello dell'effettività degli strumenti che la normativa di settore mette a disposizione dei soggetti coinvolti.

La sostanziale assenza di fonti vincolanti specificamente relative al fenomeno non significa, tuttavia, che a livello unionale esso non sia stato attenzionato e non siano emerse preziose indicazioni.

Nel contesto di una tendenziale attenzione sovranazionale al fenomeno (si pensi, a tal proposito, anche all'*International Day against Violence and Bullying at School, Including Cyberbullying*, stabilito dall'UNESCO), è in particolare la Commissione Europea ad aver predisposto alcuni interessanti documenti.

Senza pretesa di completezza, ed escludendo riferimenti a progettualità specifiche, è questo il caso della "Strategia dell'UE sui diritti dei minori" (Comunicazione della Commissione del 24 marzo 2021), che contempla anche il bullismo on line, così come del documento intitolato "Un decennio digitale per bambini e giovani: la nuova strategia europea per un'internet migliore per i ragazzi (BIK+)" (Comunicazione della Commissione del giorno 11 maggio 2022), che, seppur in puntiformi passaggi, contempla l'importanza del supporto alle vittime (per via telefonica), di attività educative e di sensibilizzazione, nonché della condivisione di quanto elaborato da un apposito gruppo di esperti.

Particolarmente rilevante risulta anche la "Strategia dell'Unione europea per la gioventù 2019-2027" (Risoluzione del Consiglio dell'Unione europea e dei rappresentanti dei governi degli Stati membri del 2018), in quanto, proprio per dare concreta attuazione all'EU Youth Strategy, è stato pensato l'attesissimo "Piano di azione contro il cyberbullismo"[5] che, a livello eu-

5 Tale Piano di azione risulta preconizzato nel recentissimo "Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the implementation of the EU Youth

rounitario, si configurerà presto quale intervento di coordinamento nella prevenzione e nel contrasto del fenomeno.

3. Gli strumenti introdotti dalla normativa italiana, tra legge 71 e legge 70

3.1 L'evoluzione della disciplina e i profili definitori

Il quadro normativo nazionale in materia di cyberbullismo, considerato in un'ottica diacronica, si è andato arricchendo, a partire dalla legge 29 maggio 2017, n. 71, in origine dedicata al solo cyberbullismo e recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo".

Richiamando quanto evidenziato nel paragrafo precedente, con la legge 71 il legislatore italiano non ha recepito o attuato una direttiva europea, né ha operato in un'ottica di adeguamento dell'ordinamento nazionale ad uno specifico regolamento unionale.

Si è trattato, in sostanza, di un primato in ambito italiano, che ha arricchito lo sforzo definitorio attestato in letteratura ed in dottrina (Ziccardi 2024, pp. 283-284) mediante una definizione normativa del fenomeno, capace di evidenziarne le plurime sfaccettature, non sempre caratterizzate da una rilevanza penalistica (Colangelo 2017, p. 399), e le peculiarità, legate all'uso del digitale, che lo differenziano dal bullismo (Senigaglia 2023, pp. 1571-1572) principalmente per il fatto che i soggetti coinvolti si trovano "altrove" (Pessina 2023, p. 114).

Tale definizione normativa risulta recentemente affiancata da quella di bullismo, ad opera della legge 17 maggio 2024, n. 70, la quale ha in più parti novellato il testo originario. L'integrazione definitoria, pur innovativa rispetto al testo previgente della legge 71, evidenzia la contiguità tra i bullismi, riconoscendone al contempo le peculiarità; parimenti, guarda in modo condivisibile alla natura essenzialmente giovanile di tali fenomeni (Ziccardi 2016, p. 205), evitando di cedere alla tentazione, emersa nell'iter di approvazione della legge 71, di non considerare il fattore anagrafico come elemento ontologicamente connaturato a siffatti fenomeni complessi (Colangelo 2016, pp. 198-199).

Di conseguenza, i riferimenti precedentemente operati al cyberbullismo risultano ora sostanzialmente estesi anche ai casi di bullismo, similmente a

Strategy (2022-2024)" del 24 marzo 2025, nonché nella Comunicazione della Commissione "Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065", in corso di pubblica consultazione alla data di chiusura del presente articolo.

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

quanto emerge dalle linee guida in materia del Ministero dell'istruzione, che contemplano, ormai da anni, entrambi i distinti fenomeni.

3.2 Gli strumenti introdotti dal legislatore

L'importanza della legge 71 trascende l'ambito definitorio, strutturando una disciplina che non solo prevede il coinvolgimento delle istituzioni nella prevenzione del fenomeno[6], ma soprattutto si focalizza sull'esigenza di una piena e proattiva consapevolezza in ambito scolastico, grazie a ruoli e procedure per la corretta e tempestiva gestione dei casi[7], della cui attuazione verrà dato conto nel paragrafo che segue.

La legge 71 ha infatti introdotto alcuni strumenti a beneficio dei soggetti coinvolti e dei rispettivi genitori, direttamente attivabili dagli stessi: tra essi spiccano la procedura di oscuramento, rimozione o blocco e la procedura di ammonimento.

Per quanto attiene alla procedura, invero non ancora compiutamente implementata, l'art. 2, comma 1, dispone:

> Ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'articolo 1, comma 2, della presente legge, può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet, previa conservazione dei dati originali, anche qualora le condotte di cui all'articolo 1, comma 2, della presente legge, da identificare espressamente tramite relativo URL (Uniform resource locator), non integrino le fattispecie previste dall'articolo 167 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, ovvero da altre norme incriminatrici.

Con tale innovativa procedura, la legge 71 "sembra voler responsabilizzare l'utente ultraquattordicenne affidandogli un ruolo attivo nel combattere il fenomeno" (Battelli 2021, p. 1273), riconoscendolo "sufficientemente maturo" e legittimato (La Spina 2024, p. 937).

Il successivo comma 2 prevede la possibilità di rivolgersi all'Autorità Garante per la protezione dei dati personali, che è tenuta a provvedere entro 48 ore; essa ha predisposto un modello editabile ed ha attivato varie collaborazioni istituzionali per la pronta gestione delle istanze.

---

6 Il riferimento va principalmente all'art. 3 (piano di azione integrato), legge 71/2017.

7 Cfr. artt. 4 (Linee di orientamento per la prevenzione e il contrasto in ambito scolastico), 4-bis (Servizio di sostegno psicologico agli studenti) e 5 (Informativa alle famiglie, sanzioni in ambito scolastico e progetti di sostegno e di recupero), legge 71/2017.

Tale facoltà è subordinata all'assenza di conferma di presa in carico dell'istanza, entro 24 ore, da parte del "soggetto responsabile", che deve provvedere entro le successive 48 ore, così come è esercitabile in caso di irreperibilità del titolare del trattamento o del "gestore del sito internet o del social".

Mentre si perpetua a tutt'oggi l'assenza di "procedure e formati standard" (art. 3, comma 3, l. 71/2017) e quindi di un canale di segnalazione specificamente rispondente al dettato normativo (Colangelo 2020, p. 232), per via della mancata attuazione del codice di coregolamentazione previsto dal medesimo articolo, risulta degno di nota l'impegno dell'Autorità Garante, finalizzato – seppur a margine di consuete procedure di *notice and takedown* – a garantire la rapidità dell'intervento a beneficio delle vittime (Mattarella 2025, p. 250).

In merito all'ammonimento, esso ricalca in parte quello previsto per il c.d. stalking ed è stato introdotto dall'art. 7, l. 71/2017 per quegli atti di cyberbullismo integranti l'ingiuria o i reati di diffamazione, minaccia e trattamento illecito dei dati personali. Il disposto del medesimo articolo, come modificato dalla l. 70/2024, ricomprende anche l'art. 612-ter c.p.[8] tra i reati presupposto e, nei limiti delle condotte effettuabili offline, è caratterizzato dall'estensione dello specifico istituto anche ai casi di bullismo:

> 1. Fino a quando non è proposta querela o non è presentata denuncia per taluno dei reati di cui agli articoli 594, 595, 612 e 612-ter del codice penale e all'articolo 167 del codice per la protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, commessi, anche mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento di cui all'articolo 8, commi 1 e 2, del decreto-legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38, e successive modificazioni.
> 2. Ai fini dell'ammonimento, il questore convoca il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale.
> 3. Gli effetti dell'ammonimento di cui al comma 1 cessano al compimento della maggiore età.

La dottrina guarda con favore all'istituto dell'ammonimento, nelle sue varie declinazioni, auspicandone anche un rafforzamento (Marandola 2023, p. 1428); l'unico strumento con diretta rilevanza penalistica all'interno della l. 71/2017 è stato ritoccato, anche ampliandone la portata applicativa, senza stravolgimenti, in particolare mantenendo il vincolo anagrafico relativo alla vittima, rimanendo la procedura limitata ai casi in cui anche la persona offesa sia minorenne.

Guardando più nel dettaglio alle modifiche apportate dalla l. 70/2024, in materia di prevenzione e contrasto del bullismo e del cyberbullismo (riman-

8 Si tratta del reato di diffusione illecita di immagini o video sessualmente espliciti.

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

dando a quanto argomentato *infra*, nonché a Zanovello 2024), occorre evidenziare come all'ampliamento della disciplina speciale anche al bullismo, risulti abbinata la conservazione, tra le finalità, del rilevante riferimento a "azioni di carattere preventivo", mentre viene esplicitata la rilevanza della "strategia di attenzione e tutela nei confronti dei minori, sia nella posizione di vittime sia in quella di responsabili di illeciti, privilegiando azioni di carattere formativo ed educativo", così come trova ora espressa visibilità nell'art. 1 la sinergia tra scuola, enti locali e realtà sportive e del terzo settore "che svolgono attività educative, anche non formali". La riforma ha altresì evidenziato il ruolo degli esercenti la responsabilità genitoriale, sottolineando, sempre al medesimo articolo, il relativo "obbligo di orientare i figli al corretto utilizzo delle tecnologie e di presidiarne l'uso", peraltro già colto da autorevole dottrina (Cassano 2020, pp. 636-637).

In estrema sintesi, ed avendo particolare riguardo agli "strumenti" sopra analizzati, per quanto attiene alla procedura di oscuramento, rimozione o blocco, la legge 70 ha lasciato invariato il disposto, perpetuando quel *vulnus* attuativo – ormai quasi decennale – cui si è fatto poc'anzi riferimento.

Con riguardo all'ammonimento del questore, la procedura di ammonimento prevista dalla legge 71 è divenuta applicabile a quegli atti di non solo di cyberbullismo, ma anche di bullismo, purché integrino in concreto le fattispecie previste dall'art. 7 con condotte poste in essere "*anche* mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne".

La disciplina novellata, tuttavia, va contestualizzata alla luce degli ulteriori interventi normativi del legislatore, in particolare del c.d. "Decreto Caivano", d.l. 15 settembre 2023, n. 123 - "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale" convertito in l. 13 novembre 2023, n. 159 (Panebianco 2023), ma anche della stessa l. 70/2024, anche in parti non direttamente concernenti modifiche alla legge 71.

Tali interventi, infatti, possono incidere sul complessivo quadro normativo di riferimento, implicando difficoltà applicative e di coordinamento, tratteggiate nel paragrafo seguente.

4. L'implementazione difficile tra disarmonie normative e ritardi attuativi

4.1 Cenni alla ritardata attuazione della legge 71

Il passaggio alla XVIII legislatura, a pochi mesi dall'entrata in vigore della legge 71, ha registrato la necessità di implementare la norma includendo il fenomeno del bullismo e inserendo misure eminentemente sanzionatorie.

Il dibattito parlamentare ha investito due legislature ed ha portato a una sostanziale conferma della finalità preventiva evidenziando, però, differenti approcci ai fenomeni prevaricatori.

Ciò emerge, in via generale, considerando come, nei sette anni esatti intercorsi tra l'approvazione della l. 71/2017 e le modifiche apportate dalla l. 70/2024, siano state promulgate, tra le altre, due leggi: la n. 92/2019 in materia di educazione civica e la n. 159/2023, la quale ha convertito con modificazioni il noto d.l. 15 settembre 2023, n. 123 ("decreto Caivano"). Se l'una risulta incentrata sull'azione formativa, l'altra è caratterizzata da un preminente approccio sanzionatorio.

Prima di analizzare tali profili, tuttavia, è fondamentale approfondire alcuni aspetti del perdurante stato di parziale attuazione della legge sul cyberbullismo.

Una delle misure ancora disattese è il Piano d'azione integrato, alla cui redazione è preposto il Tavolo tecnico per la prevenzione e il contrasto (del bullismo) e del cyberbullismo; insediato una prima volta nel febbraio 2018 e una seconda nel febbraio 2025, il Tavolo non ha finora raggiunto adeguatamente le previsioni oggetto dell'art. 3 della legge 71. La sollecitazione alla sua piena attuazione da parte del Comitato ONU per i diritti dei bambini e degli adolescenti, fin dal 2019, ne ha rimarcato l'importanza. Come già ricordato nel precedente paragrafo, il codice di co-regolamentazione e il Comitato di monitoraggio a garanzia dell'efficacia della misura di tutela della dignità dei minori (art. 2) restano adempimenti inevasi, incidendo direttamente anche su uno dei due principali strumenti di tutela introdotti dalla legge 71.

Una maggiore attenzione è invece stata indirizzata alla formazione dei referenti per la prevenzione dei bullismi mediante la piattaforma di formazione e-learning denominata ELISA, in grado di fornire anche rilevazioni circa i fenomeni.

Le modifiche apportate dalla l. 70/2024, in aggiunta a quanto già tratteggiato, vanno ad incidere anche sui ruoli di responsabilità dell'organo di coordinamento nazionale, la cui presidenza viene affidata al Dipartimento per le politiche della famiglia, sottraendo al contempo il coordinamento al Ministero dell'Istruzione e del Merito. Quest'ultimo ministero vede altresì ristretta al solo ambito scolastico la competenza nella promozione di campagne di sensibilizzazione.

4.2 In cerca dell'armonia nell'ipertrofia normativa

Lo strumento delle campagne di informazione promosso dalla Presidenza del Consiglio dei ministri – Dipartimento per le politiche della famiglia e dal Ministero delle imprese e del made in Italy è previsto anche dall'articolo

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

14 della l. 159/2023, al Capo IV – Disposizioni per la sicurezza dei minori in ambito digitale[9]. Esso è indirizzato più direttamente alla diffusione dell'uso del controllo parentale, ossia a quei "mezzi di prevenzione dall'accesso a contenuti potenzialmente nocivi per lo sviluppo armonioso dei minori". Anche in questo caso non è coinvolto il Ministero dell'Istruzione e del merito, ma sono molto valorizzati i Centri per la famiglia (art. 14), individuati come le strutture idonee per l'alfabetizzazione digitale e mediatica di minori e dei loro genitori. Sembra nuovamente di cogliere una sottrazione o, quantomeno, una diminuzione di competenze fino a oggi riconosciute alla scuola quale cuore generativo di cultura – e cittadinanza – digitale nei territori, in rete con i servizi utili ad affrontare la complessità dei fenomeni in oggetto.

Questa visione sinergica e strutturale non trova spazio nella l. 159/23, di cui è evidente l'approccio sanzionatorio correlato ad esigenze di ordine pubblico; i giovani sono avvertiti come la causa di un degrado più o meno marcato a seconda dei contesti, potenziali attori di illeciti in danno di coetanei e dell'intera comunità. Per contrastare la violenza minorile si applica l'avviso orale al soggetto ultraquattordicenne nel caso risulti condannato per uno o più delitti contro la persona. Se la condotta delittuosa viene realizzata con strumenti informatici, il minore subirà la proibizione al possesso e all'uso di telefoni cellulari o altri dispositivi di comunicazione. La norma prevede anche l'introduzione di un'ulteriore variante dell'ammonimento del questore – approfondito nel precedente paragrafo per come configurato nella legge 71 – nei confronti del minore ultraquattordicenne per reati di percosse, lesioni personali, violenza privata, minacce e danneggiamento, risultando caratterizzata da una significativa estensione della misura anche al minore di età compresa tra i dodici e i quattordici anni – ad oggi assente nell'ammonimento del questore disciplinato dalla legge 71 – quando il fatto commesso possa configurare una fattispecie di reato per cui è prevista la reclusione non inferiore a cinque anni. Si prevede, in tali casi, anche una sanzione amministrativa pecuniaria per i genitori, da 200 a 1.000 euro, salvo che questi provino di non aver potuto impedire il fatto. Nei casi meno gravi, cioè con pena non superiore a un massimo di cinque anni, è previsto il ricorso a un percorso di rieducazione, che costituisce una forma di definizione anticipata del procedimento penale. Essa è avviata su iniziativa del pubblico ministero e subordinata "alla condizione che il minore acceda a un percorso di reinserimento e rieducazione civica e sociale sulla base di un programma rieducativo che preveda lo svolgimento di lavori socialmente utili o la collaborazione a titolo gratuito con enti no profit o lo svolgimento

9 Del Capo IV "Disposizioni per la sicurezza dei minori in ambito digitale" in particolare risultano interessanti alla presente analisi i seguenti articoli: Applicazione del controllo parentale nei dispositivi di comunicazione elettronica (art. 13), Disposizioni per la verifica dell'età per l'accesso a siti pornografici (art. 13/bis), Alfabetizzazione digitale e mediatica a tutela dei minori e campagne informative (art. 14).

di altre attività a beneficio della comunità di appartenenza, per un periodo compreso da uno a sei mesi".

Tali misure, seppur dettate in relazione alla c.d. delinquenza minorile e non direttamente rivolte ai bullismi, sono già state applicate in casi di bullismo e cyberbullismo. Inoltre, vanno ulteriormente contestualizzate in relazione a quanto previsto all'art. 2 della l. 70/2024, che dispone la modifica l'art. 25 del regio decreto-legge 1404/1934, convertito con modificazioni dalla l. 835/1935, relativamente alle specifiche procedure della procura minorile. La novella, sul punto, ha ricadute anche nell'ambito scolastico, laddove, a fronte di condotte recidivanti per le quali a nulla siano valsi interventi di tipo educativo, sarà la segnalazione del dirigente scolastico a mettere in moto le procedure stesse.

Ciò posto, è lecito l'auspicio che la progettazione ed il monitoraggio degli interventi di prevenzione e responsabilizzazione vengano in futuro caratterizzati da un maggior coordinamento tra gli operatori coinvolti; una formazione integrata, anche con il personale delle autonomie scolastiche, sarebbe di grande supporto in particolare nella progettazione delle attività sanzionatorie ispirate alla giustizia riparativa.

Un utile apporto potrà derivare dalla fattiva collaborazione tra il Tavolo tecnico della l. 71/2017 e la Consulta dei diritti e dei doveri del bambino e dell'adolescente digitale, prevista dalla l. 92/2019: si auspica, sul punto, quel "coordinamento" tra Tavolo tecnico e Consulta sancito *ex* art. 5, comma 6, l. 92/2019. Pur nella formale autonomia dei consessi, essi sono posti in parallelo dal 5° Piano nazionale di azione e di interventi per la tutela dei diritti e lo sviluppo dei soggetti in età evolutiva - Educazione, Equità, Empowerment10.

Con apposito inserimento del nucleo concettuale "Cittadinanza Digitale", la l. 92/2019 sviluppa coerentemente l'art. 4, comma 5 della l. 71/2017: la promozione dell'uso consapevole di Internet deve essere un obiettivo trasversale nelle diverse discipline curricolari e richiedere una progettualità verticale che coinvolge tutti gli ordini di scuola. In una prospettiva sistemica e interdisciplinare, i fenomeni del bullismo e del cyberbullismo vengono confermati come rischi da minimizzare e da gestire correttamente – abbandonando logiche di contingente emergenza – per il benessere psicofisico individuale e collettivo, per l'inclusione sociale e la legalità. Le Linee guida relative alla Legge 92/2019 emanate nel 2020 e nel 2024 considerano ampiamente i fenomeni di prevaricazione tra pari, articolando le azioni e gli obiettivi specifici [11].

10 https://www.minori.gov.it/sites/default/files/idi_quintopianoazione_220725-2.pdf

11 "Le Linee guida si configurano come strumento di supporto e sostegno ai docenti anche di fronte ad alcune gravi emergenze educative e sociali del nostro tempo quali, ad esempio, l'aumento di atti di bullismo, di cyberbullismo e di

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

L'alleanza educativa, fondamentale nella scuola, viene fortemente valorizzata nelle Linee di orientamento 2017[12] e nel 2021[13] per la prevenzione e il contrasto dei bullismi (purtroppo emanate con cadenza più lunga e sostanzialmente raddoppiata rispetto alla previsione normativa).

Tutte le componenti della scuola sono chiamate a occuparsi dei fenomeni di prevaricazione tra pari e certamente in tal senso il progetto europeo – attivo da 15 anni – Generazioni connesse[14] e la formazione e-learning tramite la piattaforma ELISA[15], attiva dal 2018, offrono utilissimi strumenti per far crescere le competenze di educazione alla cittadinanza digitale e gestire le politiche anti-bullismo dentro e fuori la Rete, nonché dentro e fuori le scuole.

In questo contesto, la partecipazione degli studenti è fondamentale, per l'appropriazione dei diritti, per l'assunzione di responsabilità, per percepirsi protagonisti consapevoli nella dimensione *onlife*.

Le norme non si sono dimenticate della componente studentesca, che è rappresentata al Tavolo tecnico nazionale e al Tavolo permanente per il monitoraggio dei fenomeni di bullismo e cyberbullismo costituito in ogni istituto. Tra le metodologie partecipative emerge la *peer education* che, nell'ottica del legislatore, può coinvolgere anche gli ex studenti che abbiano svolto quel ruolo, sta ottenendo risultati molto importanti nelle scuole italiane.

4.3 Cenni alle leggi regionali in materia

I numerosi progetti attivati in questi anni hanno anche potuto attingere a canali di finanziamento previsti da normative specifiche promulgate dal 2016 da parte delle Regioni. Le previsioni disposte dai governi regionali rispondono correttamente alla programmazione degli interventi dei servizi sanitari, assistenziali e educativi per offrire servizi di supporto nel prevenire e contrastare i bullismi.

In dottrina (Foschino, Barbaro, Russo, 2019) viene evidenziato il ruolo delle Regioni, che hanno costituito organismi di governance per condividere i piani progettuali con gli Uffici scolastici regionali e soggetti istituzionali operanti in ambito regionale, come le Autorità Garanti dell'infanzia e adolescenza e i CoReCom. Sono inoltre attivi a livello regionale e/o provinciale

violenza contro le donne, la dipendenza dal digitale, il drammatico incremento dell'incidentalità stradale": https://www.mim.gov.it/documents/20182/0/Linee+guida+Educazione+civica.pdf/9ffd1e06-db57-1596-c742-216b3f42b995?t=1725710190643

12 https://www.mim.gov.it/documents/20182/0/Linee+Guida+Bullismo+-+2017.pdf/4df7c320-e98f-4417-9c31-9100fd63e2be?version=1.0

13 https://shorturl.at/FX1KQ

14 https://www.generazioniconnesse.it/site/it/home/

15 https://www.piattaformaelisa.it/

significativi protocolli d'intesa con le Prefetture, le forze dell'ordine, i servizi territoriali (operatori di giustizia, socio-sanitari e socio-assistenziali) e associazioni del terzo settore specializzate nella mediazione dei conflitti e nelle attività riparative.

È possibile interpretare come potenziamento della disciplina nazionale sui bullismi i richiami espliciti operati nelle leggi regionali di Piemonte, Calabria, Marche, Toscana, Puglia, Sardegna, Campania, Sicilia alla *peer education* "per potenziare il senso di responsabilità, la partecipazione e l'autostima dei ragazzi, nonché favorire modalità corrette di gestione dei conflitti, di confronto e di comunicazione tra pari"[16] o alla funzione di "studenti in veste di mediatori scolastici che, con il supporto di un docente, svolgano un ruolo attivo nella gestione di episodi di bullismo e cyberbullismo"[17].

Alcune leggi regionali, quali quelle emanate dalle Regioni Lazio e Lombardia, prevedendo - con formulazioni simili - l'utilizzo di "idonee tecniche psico-pedagogiche e di pratiche educative per attuare un'efficace azione, soprattutto preventiva, del fenomeno del bullismo"[18], rimandano a attività partecipative delle scolaresche. Considerando le attività finanziate dalle Regioni in questi anni, il protagonismo delle giovani generazioni assurge a criterio normalmente valorizzato nell'assegnazione dei fondi[19].

Più limitata risulta invece la partecipazione delle giovani generazioni in relazione alla scrittura delle norme regionali sul tema[20] o alla co-progettazione con partecipazione diretta alla governance e ai tavoli programmatici.

Diverse regioni, infine, sostengono l'attuazione di sportelli d'ascolto e di sportelli psicologici oltre alla creazione di strutture sanitarie specializzate nella presa in carico di vittime e autori di bullismo e cyberbullismo[21].

Richiamato proprio il principio di sussidiarietà Stato-Regione, la l. 70/2024 inserisce nella legge 71 l'art. 4 bis, dando rilievo ad una specifica indicazione: la fornitura di "un servizio psicologico agli studenti per favorire lo sviluppo e la formazione della personalità degli studenti nonché prevenire fattori di rischio o situazioni di disagio, anche attraverso il coinvolgimento delle famiglie". Questo nuovo articolo, elaborato dalla commissione ristretta

16 Art. 2, comma 4, lett. g), legge regionale della Regione Piemonte 5 febbraio 2018, n. 2.

17 Art. 3, comma 1, lett. e), legge regionale della Regione Marche 6 agosto 2018, n. 32.

18 Art. 2. comma 3, lett. c), legge regionale della Regione Lazio 24 Marzo 2016, n. 2.

19 Il monitoraggio sulle buone pratiche realizzato da Piattaforma Elisa con il progetto SIA risultano attive e diffuse buone pratiche che valorizzano il protagonismo fin dalla scuola dell'infanzia.

20 La legge regionale Toscana ha fatto sua una proposta di legge di prevenzione e contrasto ai bullismi elaborata dal Parlamentino della Regione e ha previsto la partecipazione al tavolo di coordinamento della Consulta degli studenti

21 La Regione Piemonte prevede la realizzazione Centri regionali specializzati nella cura dei disturbi derivanti dal bullismo e dal cyberbullismo dotati di equipe multidisciplinari.

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

e approvato in prima lettura, conteneva la previsione di un secondo comma relativo alla fornitura di un servizio di coordinamento pedagogico "al fine di promuovere e contribuire al pieno sviluppo delle potenzialità di crescita personale, di inserimento e partecipazione sociale, agendo in particolare sulle relazioni interpersonali e sulle dinamiche di gruppo". Tale misura è stata cassata in seconda lettura al Senato, suscitando un dibattito politico circa la penalizzazione di una visione pedagogica a vantaggio di una eccessiva "sanitarizzazione" dell'intervento di presa in carico di vittime, bulli e spettatori.

Parrebbe quindi consolidarsi da una parte l'approccio rieducativo/sanzionatorio che guarda agli autori di bullismo e cyberbullismo come "devianti", dall'altra la tendenza a attribuire tali fenomeni esclusivamente a aspetti caratteriali o alla salute mentale degli adolescenti.

Non meno preoccupante, risulta una certa tendenza al proibizionismo digitale ed alla sorveglianza, che non rappresenta una risposta ai bisogni di *agency* delle giovani generazioni. Strumenti abilitanti come la Patente per l'uso consapevole dello smartphone, adottata dalla Regione Piemonte, risultano vincenti anche per la dimensione "comunitaria" in grado di coinvolgere un'ampia alleanza educativa (Croce, Paracchini, 2025).

5. Alcune riflessioni di sintesi

Considerate la complessità dei due fenomeni e le difficoltà di definizione e di rilevazione omogenee, non stupisce che le attuali normative e politiche nazionali appaiano fondate su visioni soltanto parzialmente convergenti. Anche gli sforzi in ambito eurounitario non sembrano riuscire a stimolare una vera integrazione tra le differenti visioni. Infatti, nelle normative a livello nazionale e regionale si passa dal considerare bullismo e cyberbullismo come problemi di natura psicologica individuale, che necessitano di interventi medicalizzanti, a letture completamente sbilanciate verso la rilevazione degli aspetti devianti, se non francamente criminali, degli atti di prevaricazione, per i quali si ritiene necessario l'intervento punitivo sul perpetratore o, di riflesso, sulla sua famiglia.

Inoltre, la normativa e le politiche richiamano anche la visione pedagogico-educativa, secondo la quale i comportamenti prevaricanti possono rientrare tra quelli che meritano l'attivazione di percorsi educativi a fini preventivi e rieducativi.

A proposito di quest'ultima visione, merita ricordare quanto sottolineato nel quarto paragrafo a proposito dello spostamento dalla scuola alla famiglia delle competenze educative principali riferite al bullismo e al cyberbullismo. Come abbiamo visto, sebbene la scuola mantenga una propria riconosciuta funzione, l'attuale quadro normativo affida la regia degli interventi al Dipartimento per le politiche della famiglia e le famiglie di coloro che

commettono atti di prevaricazione sono chiamate direttamente in causa in termini di responsabilizzazione e di possibile punizione. Se, a prima vista, si tratta di una semplice riaffermazione della primazia delle funzioni educative dei genitori, in realtà si tratta di un interessante spostamento di campo in merito all'interpretazione dei due fenomeni.

Come è noto, non tutte le famiglie sono in grado di essere "educanti" e non tutti i contesti sociali sono in grado di offrire le risorse strutturali e culturali necessarie per apprendere ad agire costantemente quelle pratiche di espressione delle emozioni e delle tensioni, di gestione dei conflitti, di rispetto reciproco necessarie per il vivere associato senza prevaricazioni. La scuola è e rimane l'unica istituzione universalista che dovrebbe essere in grado di rivolgere la propria attenzione in modo uguale a tutti coloro che la frequentano e questo suo universalismo, insieme con la primaria funzione educante che la connota, è garanzia che tutte le persone giovani in formazione possano avere accesso alla "cassetta degli attrezzi" necessaria per sviluppare capacità e modalità relazionali non prevaricanti. Ciò nulla toglie alla responsabilità educativa e di sorveglianza che fa capo ai genitori, ma la realtà delle disuguaglianze economiche, sociali, culturali che connotano la vita delle giovani generazioni del nostro paese, indicano che le risposte al bullismo e al cyberbullismo non possono essere primariamente allocate nelle singole famiglie (Menesini, 2000). Inoltre, potrebbe essere disfunzionale non riconoscere la centralità della scuola, anche in virtù della sua funzione di possibile primo aggancio istituzionale di quelle famiglie che necessitano di ausilio per compiere la loro funzione educativa.

Sarebbe peraltro disfunzionale non valorizzare il ruolo della scuola in termini di prevenzione, intendendosi soltanto come ancillare alla famiglia, proprio in relazione non solo all'erogazione di pacchetti formativi rivolti al bullismo e al cyberbullismo, ma anche, e soprattutto, nel costante impegno a fornire a tutti gli studenti e a tutte le studentesse quella cassetta degli attrezzi necessaria a tutti gli aspetti della vita sociale, menzionata poc'anzi.

Un'ultima riflessione riguarda la partecipazione attiva dei bambini, delle bambine, degli e delle adolescenti all'individuazione dei fenomeni in oggetto, alla produzione normativa che li previene e che li contrasta, alla costruzione e all'attuazione delle attività che hanno il bullismo e il cyberbullismo come bersaglio. Accanto ad aperture normative importanti – quali, per esempio, la disposizione che ha inteso riconoscere e valorizzare le capacità dei ragazzi e delle ragazze di segnalare autonomamente alle istituzioni, già a partire dai 14 anni, gli atti di prevaricazione subiti sul web e di richiedere la rimozione dei relativi contenuti postati – e accanto alle non ancora molto diffuse, sebbene presenti, pratiche di co-costruzione di percorsi normativi ed educativi, ancora oggi appare sottovalutata l'importanza della partecipazione attiva, legittimata e riconosciuta, delle nuove generazioni ad azioni per la prevenzione e il contrasto ai due fenomeni. Parimenti, è poco diffusa la

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

consapevolezza degli adulti circa l'importanza di costruire ambienti sociali che insegnino – anche attraverso l'esempio e l'organizzazione più paritaria dei contesti di vita comune – a praticare il rispetto reciproco.

In conclusione, come insegnano la letteratura pedagogica e nuove e illuminate pratiche educative per il contrasto degli atti di prevaricazione tra pari (cfr., per esempio, Croce, Paracchini, 2025) e come indicano le istituzioni più attente al tema della partecipazione, i ragazzi e le ragazze, quando ascoltati, coinvolti e legittimati come interlocutori competenti, hanno dimostrato di saper agire come valido motore per il cambiamento. Sono loro, dunque, i primi interlocutori a cui pensare nella costruzione di efficaci percorsi di prevenzione e di contrasto ai bullismi.

Bibliografia

Aalsma, M.C., (2008), What Is Bullying?, *Journal of Adolescent Health*, vol. 43, 2, pp. 101-102.

Ansary, N.S., (2020), Cyberbulling: Concepts, theories, and correlates in-forming evidence-based best practices for prevention, *Aggression and violent Behavior*, vol. 50, Article 101343.

Bacchini, D., (2007), Le relazioni del bullismo con il clima sociale e scolastico, *Minorigiustizia*, vol. 4, pp. 142-150.

Battelli, E., (2021), Minori e social network: cyberbullismo e limiti della *parental responsibility*, *Il Corriere giuridico*, 10, pp. 1269-1277.

Belacchi, C., Biagetti, G., (2007), I ruoli dei partecipanti nel bullismo: oltre lo stereotipo bullo-vittima, *Minorigiustizia*, vol. 4, pp. 163-175.

Beltran-Catalan, M., Cruz-Catalan, E. (2020), How long bullying last? A comparison between a self-reported general bullying-victimization question and specific bullying-victimization questions, *Children and Youth Services Review*, vol. 111, Article 104844.

Brunstein Klomek, A., Sourander, A., Gould, M. (2010), The Association of Suicide and Bullying in Childhood to Young Adulthood: A Review of Cross-Sectional and Longitudinal Research Findings, *La Revue canadienne de psychiatrie*, vol. 55, n. 5, pp. 282-288.

Buccoliero, E., Maggi, M., (2018), *Bullismo, Bullismi*, Milano, Franco Angeli.

Canty, J., Stubbe, M., Steers, D., Collings, S., (2016), The trouble with bullying–deconstructing the conventional definition of bullying for a child-centred investigation into children's use of social media, *Children & Society*, vol. 30, n. 1, pp. 48-58.

Cassano, G., (2020), La responsabilità genitoriale nell'uso dell'odierna tecnologia telematica, *Famiglia e diritto*, 6, pp. 631-637.

Colangelo, R.M., (2016), Cyberbullismo e responsabilità: Internet è veramente un mondo virtuale?, in Passaglia, P., Poletti, D., eds., Nodi virtuali, legami informali: Internet alla ricerca di regole, Pisa, Pisa University Press, pp. 193-206.

Colangelo, R.M., (2017), La legge sul cyberbullismo. Considerazioni informatico-giuridiche e comparatistiche, *Informatica e diritto*, XXVI, 1-2, pp. 397-418.

Colangelo, R.M., (2020), La normativa sul cyberbullismo: per un bilancio a due anni dall'entrata in vigore della l. 29 maggio 2017, n. 71, *Diritto ed economia dell'impresa*, 2, pp. 227-252.

Croce, M., Paracchini, F., (2025) *La patente per lo smartphone*, *Proposte e strumenti per il benessere digitale in adolescenza,* Milano, Franco Angeli.

De Salvatore, F. (2012), Bullismo e cyberbullying, dal reale al virtuale tra media e new media, *Minorigiustizia*, vol. 4, pp. 94- 101.

Dredge, R., Gleeson, J., De la Piedad Garcia, X., (2014), Cyberbullying in social networking sites: An adolescent victim's perspective*, Computers in human behavior*, vol. 36, pp. 13-20.

Elisa, 2023, https://www.piattaformaelisa.it/risultati-monitoraggio-a-s-2022-2023/ (consultato il 15 ottobre 2025)

Favretto, A.R., Torre, E.M.T, (eds.) (2024), *Secondo il mio punto di vista. Bullismo e cyberbullismo esplorati con gli occhi degli adolescenti*, Il mulino, Bologna.

Foschino Barbaro, M.G., Russo, P., (2019), *Bulli, cyberbulli e vittime*, Milano, Franco Angeli.

Gazzelloni, S., Esame delle proposte di legge in materia di contrasto del fenomeno del bullismo, https://www.istat.it/audizioni/esame-delle-proposte-di-legge-c-536-dori-c-891-pittalis-e-c-910-maschio-recanti-disposizioni-in-materia-di-prevenzione-e-contrasto-del-fenomeno-del-bullismo-del-cyberbullismo-e-di-misure-ried/ (consultato il 15 ottobre 2025)

Hall, G.S., (1904). Adolescence: Its psychology and its relations to physiology, anthropology, sociology, sex, crime, religion and education, Vol. 1., New York, D Appleton & Company.

Horton, P., (2011), School bullying and social and moral orders, *Children & Society*, vol. 25, 4, pp. 268-277

Hunter, S.C., Durkin, K., Boyle, J.M.E., Booth, J.N., Rasmussen, S., (2014), Adolescent Bullying and Sleep Difficulties, *Europe's Journal of Psychology*, vol. 10, 4, pp. 740-755.

Iannaccone, N., (2014), *Né vittime, né prepotenti. Una proposta didattica di contrasto al bullismo*, Bari, La meridiana.

ISTAT, *Il bullismo in Italia: comportamenti offensivi e violenti tra i giovanissimi*, 2014

ISTAT, *Indagine conoscitiva su bullismo e cyberbullismo*, 2015

La Spina, A., (2024), L'identità del minore nella realtà *on-life* tra protezione e autodeterminazione, *Famiglia e diritto*, 10, pp. 920-942.

Marandola, A., (2023), Codice Rosso rafforzato, *Diritto penale e processo*, 11, 1420-1430.

Mark, L., Värnik, A., Sisask M. (2019), Who Suffers Most From Being Involved in Bullying - Bully, Victim, or Bully-Victim?, «Journal of School Health», vol. 89, n. 2, pp. 136-144.

Mattarella, A., (2025), Diritto penale e nuove tecnologie: dalla Convenzione Onu contro i reati informatici alle sfide dell'intelligenza artificiale, *Diritto penale e processo*, 2, pp. 250-271.

Menesini, E., (2000), Il bullismo. Che fare? Prevenzione e strategie di intervento nella scuola, Giunti, Firenze.

Menesini, E., Nocentini, A., Calussi, P., (2011), The measurement of cyberbullying: Dimensional structure and relative item severity and discrimination, *Cyberpsychology, behavior, and social networking*, vol. 14, 5, pp. 267-274.

Mishna, F., Sanders, J.E., McNeil, S., Fearing, G., Kalenteridis, K., (2020), "If Somebody is Different": A critical analysis of parent, teacher and student perspectives on bullying and cyberbullying, *Children and Youth Services Review*, vol. 118, 105366.

Olweus, D., (2001), *Bullismo a scuola. Ragazzi oppressi ragazzi che opprimono*, Firenze, Giunti Editore.

Olweus, D., Limber, S.P., (2018), Some problems with cyberbullying research, *Current opinion in psychology*, 19, pp. 139-143.

Panebianco, G., (2023), Sicurezza, criminalità minorile e urgenza a fronte del c.d. decreto "Caivano", *Diritto penale e processo*, 12, pp. 1554-1586.

Pessina, A., (2023), *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, Milano-Udine, Mimesis.

Pepler, D., Jiang, D., Craig, W., Connolly, J., (2008), Developmental Trajec-tories of Bullying and Associated Factors, *Child Development*, vol. 79, 2, pp. 325-338.

Peter, I-K., Petermann, F., (2018), Cyberbulling: A concept analysis of defining attributes and additional influencing factors, *Computers in Human Behavior*, vol. 86, pp. 350-366.

Rigby, K., (2002), *New Perspectives on Bullying*, London, Jessica Kingsley Publishers.

Senigaglia, R., (2023), L'identità personale del minore di età nel cyberspazio tra autodeterminazione e *parental control system*, *Le nuove leggi civili commentate*, 6, pp. 1568-1602.

Thomas, H.J., Connor, J.P., Scott, J.G., (2015), Integrating traditional bullying and cyberbullying: challenges of definition and measurement in adolescents – a review, *Educational psychology review,* vol. 27, 1, pp. 135-152.

Thornberg, R., (2015), The social dynamics of school bullying: The necessary dialogue between the blind men around the elephant and the possible meeting point at the social-ecological square, Confero: *Essays on Education, Philosophy and Politics*, vol. 3, 2, pp. 161-203.

Vaillancourt, T., McDougall, P., Hymel, S., Krygsman, A., Miller, J., Sti-ver, K., Davis, C., (2008), Bullying: Are researchers and children/youth talking about the same thing?, *International Journal of Behavioral Development*, vol. 32, 6, pp. 486-495.

Wolke D.,Woods S., Stanford K., Schulz H., (2001), Bullying and victimization of primary school children in England and Germany: Prevalence and school factors, *British Journal of Psychology*, Vol. 92, 4, pp. 567-696.

Zanovello, F., (2024), Prevenzione e contrasto del bullismo e del cyberbullismo. Tra novità e criticità della l. n. 70/24, *Le nuove leggi civili commentate*, 4, pp. 826-850.

Ziccardi, G., (2016), *L'odio on line. Violenza verbale e ossessioni in rete*, Milano, Raffaello Cortina Editore.

Ziccardi, G., (2024), *Dati avvelenati. Truffe, virus informatici e falso online*, Milano, Raffaello Cortina Editore.

Patti educativi digitali: una possibile risposta alle sfide tecnologiche?

Digital Educational Pacts: A Possible Response to Technological Challenges?

Thomas Casadei[1]

Sommario

Il contributo mira ad approfondire il ruolo dei Patti educativi digitali come strumenti capaci di implementare l'alleanza educativa tra scuola, famiglie, istituzioni e territorio, in un contesto segnato dalla pervasiva presenza delle tecnologie digitali nella vita quotidiana, soprattutto in quella delle giovani generazioni.

In un siffatto scenario, i Patti educativi – nella loro accezione più ampia – si configurano come risposte generative alla necessità di ricostruire forme di dialogo tra generazioni e un tessuto di corresponsabilità educativa, capace di interpretare i mutamenti in atto nelle forme del sapere, della relazione e della cittadinanza attiva.

La società iperconnessa richiede, infatti, nuovi paradigmi educativi, che non si limitino a interventi emergenziali o repressivi (o comunque di carattere meramente regolatorio), ma siano in grado di accompagnare bambini e adolescenti nella costruzione di un rapporto equilibrato, consapevole e critico con la rete.

I Patti educativi digitali si collocano in questa cornice come strumenti con implicazioni sia sul versante pedagogico-educativo, sia sul versante del diritto, in grado di favorire il dialogo tra attori diversi del mondo educante (ma anche tra generazioni), promuovendo un approccio fondato sulla corresponsabilità, sull'ascolto e sulla costruzione condivisa di regole e obiettivi educativi.

Parole chiave: patti educativi; corresponsabilità; educazione digitale; diritti; benessere digitale

1 Università degli Studi di Modena e Reggio Emilia, Dipartimento di Giurisprudenza; Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità – CRID. thomas.casadei@unimore.it.

Data invio: 1 luglio 2025. Data accettazione: 1 settembre 2025.
DOI: https://doi.org/10.54103/1972-5760/30055

Abstract

The contribution aims to explore the potential of Digital Educational Pacts to strengthen the educational alliance between schools, families, institutions, and the wider community, in a context that is increasingly shaped by the pervasiveness of digital technologies in everyday life, particularly among younger generations.

In this scenario, Educational Pacts – in their broadest sense – emerge as a generative response to the need to rebuild forms of intergenerational dialogue and shared educational responsibility, capable of interpreting the ongoing transformations in knowledge, relationships, and active citizenship.

Indeed, a hyperconnected society calls for new educational paradigms that go beyond emergency or repressive measures, as well as merely regulatory approaches, in order to support children and adolescents in developing a balanced, conscious, and critical relationship with the digital world.

Within this framework, Digital Educational Pacts serve as tools with both pedagogical-educational and legal implications. They foster dialogue among the various actors in the educational ecosystem (as well as between generations), promoting an approach grounded in shared responsibility, active listening, and the co-construction of rules and educational goals.

Keywords: Educational Agreements; Co-responsibility; Digital Education; Rights; Digital Wellbeing

1. Contesto: impatto del digitale e giovani generazioni

In un mondo in cui la crescente digitalizzazione sta trasformando profondamente ogni aspetto della quotidianità, nelle sue molteplici pratiche[2] ed entro i suoi vari ambienti (e assai opportuna è dunque la segnalazione di una sua notevole "ristrutturazione"[3]), diventa sempre più urgente analizzare il suo *impatto*, non solo in termini di opportunità e criticità, ma anche rispetto alle implicazioni relazionali, sociali ed educative che essa comporta (cfr. Lupton 2015; Longo, Scorza 2020; Han 2022; nello specifico dell'aspetto educativo, cfr. Campagnoli 2024; Casadei 2021)[4].

2 Come è stato rilevato, non c'è ormai ambito della vita personale e collettiva che non sia toccato dalla "digitalizzazione": "ricerca, sanità, mobilità, logistica, pubblica amministrazione, scuola, moneta, produzione, lavoro; e poi tracciamento, videosorveglianza, robotica, riconoscimento facciale, regolamentazione algoritmica, intelligenza artificiale, ecc." (Giaccardi, Magatti 2022, p. 65 e, più ampiamente, pp. 64-79).

3 Lo spiega molto bene Michele Martoni nelle battute iniziali del suo contributo a questo dossier.

4 Sono state queste alcune delle tematiche al centro della I Semana internacional "El impacto social y normativo de la inteligencia artificial", che si è svolta dal 13 al 16 maggio 2025, presso l'Universidad de Oviedo su iniziativa di Roger Campione e Miguel A. Presno Linera e alla

In questo contesto, una specifica attenzione meritano le giovani generazioni, il cui rapporto con le tecnologie digitali si intreccia con i processi di apprendimento e – più ampiamente – con quelli di crescita, di formazione dell'identità e di interazione sociale[5], aspetto che comporta anche il prendere sul serio i rischi di questi problemi sul piano psicologico (Lavenia 2018).

Invero, una siffatta riflessione si rende ancora più necessaria dal momento in cui i dispositivi digitali vengono utilizzati non solo a scopo ludico, ricreativo, di intrattenimento bensì anche nell'ambito scolastico, a fini didattici e formativi (Amato Mangiameli, Campagnoli 2020; Martoni 2025).

Tali contesti, un tempo considerati separati rispetto alla dimensione digitale, sono ormai profondamente permeati dalla tecnologia, che si presenta come elemento che influenza abitualmente le pratiche educative quotidiane, oltre che i molteplici ambiti della comunicazione e del diritto (da ultimo, Moro 2025). A partire dalla pandemia da Covid-19 e dall'estensione della didattica a distanza (Bruschi, Perissinotto 2020; Casadei 2021), la presenza del digitale si è intensificata, diventando una componente ordinaria della relazione educativa: ciò ha determinato nuove pratiche, nuove abitudini, nuove attitudini, nuove aspettative, ma anche nuove criticità.

Se, da un lato, è vero che l'uso del digitale in questi ambiti può apportare significative opportunità – si pensi all'accesso a contenuti aggiornati, alla personalizzazione dei percorsi di apprendimento, o all'inclusione di alunni e alunne con bisogni educativi speciali[6] – dall'altro, non è possibile esimersi dall'interrogarsi sugli effetti problematici o negativi che un uso precoce, intensivo, non pienamente consapevole e regolato degli strumenti digitali può avere su individui la cui personalità è in piena fase di sviluppo e cambiamento, quali le persone di minore età, gli adolescenti e, in generale, i giovani.

---

quale ho preso parte mercoledì 14 maggio 2025 nell'ambito di un panel specificamente dedicato: "Educación e IA". Per un primo resoconto: https://retina-der.uniovi.es/index.php/2025/05/29/limpatto-sociale-e-normativo-dellintelligenza-artificiale-1a-settimana-internazionale/.

5 M. Paola Mittica, nel suo contributo in questo forum dal titolo "Corpi digitalmente modificati. *Law and Humanities* per adolescenti nell'epoca della trasformazione digitale" spiega – facendo riferimenti a una serie di studi scientifici e psicologici – che l'immersione nell'ambiente digitale in cui nascono e crescono i c.d. "nativi digitali" ha conseguenze negative sui processi primari, limitando il loro sviluppo della soggettività, e si interroga su quali possano essere metodologie e pratiche la prevenzione del disagio di persone di minore età e giovani, individuando la proposta educativa di *Law and Humanities* come molto feconda.

6 Commissione Europea 2020 (pp. 1-2): "La tecnologia digitale, se impiegata in modo capace, equo ed efficace dagli educatori, può sostenere pienamente l'agenda per un'istruzione e una formazione inclusive e di elevata qualità per tutti i discenti. Può facilitare un apprendimento maggiormente personalizzato, flessibile e incentrato sullo studente, in tutte le fasi e gli stadi dell'istruzione e della formazione. La tecnologia può rappresentare uno strumento potente e coinvolgente per l'apprendimento collaborativo e creativo. Può aiutare i discenti e gli educatori ad accedere a contenuti digitali, a crearne e a condividerli. […] L'apprendimento può avvenire interamente online oppure in modalità mista, seguendo tempi, luoghi e ritmi adeguati alle esigenze del singolo discente".

Numerosi studi segnalano infatti criticità connesse alla dimensione del c.d. *screen time* e, più specificamente, alla qualità del sonno, alla regolazione emotiva, all'attenzione e alla concentrazione scolastica (cfr. Gui *et al*. 2020)[7]. L'esposizione prolungata agli schermi[8] (Carbone, Lingua 2024; cfr. Pezzano 2024), soprattutto in assenza di un accompagnamento educativo stabile e coerente, può interferire con lo sviluppo cognitivo e relazionale, incidendo negativamente sull'apprendimento e sul benessere psicologico.

Le evidenze scientifiche confermano infatti che dall'età di accesso al primo smartphone dipendono fortemente gli effetti – misurabili nel tempo – sulla qualità delle relazioni, sull'apprendimento scolastico e sull'emersione di usi problematici della rete (Gui *et al*. 2020); inoltre, numerosi studi provano che l'uso intensivo dei social network in età evolutiva contribuisce all'incremento di ansia, isolamento e disagio psicologico tra preadolescenti (Haidt 2024).

Le conseguenze dell'isolamento possono sfociare in forme di manifestazione del disagio anche estreme, ma anche in forme di anomie. Un caso emblematico è quello dei cosiddetti "hikikomori", un fenomeno di ritiro sociale volontario, che può essere inteso come una vera e propria "autoreclusione" (Bagnato 2023; cfr. Furuhashi *et alii* 2023; Sagliocco 2011; Verza 2016; Mignolli 2023; e, da ultimo, Rossi 2025)[9].

---

7 Federazione Italiana Medici Pediatri 2023: https://www.fimp.pro/images/guide/digitale.pdf.

8 Si tratta di un fenomeno che sta generando profonde mutazioni anche sul piano antropologico. Nella letteratura internazionale è importante il lavoro recente di Degen (2024), *Swipe, like, love. Intimität und Beziehung im digitalen Zeitalter*, Giesen, Psychosozial-Verlag. Da quest'opera ha tratto spunto il progetto "Swipe Like Love – Sguardi di genere su digitale e uso di TikTok". Quest'ultimo, nato dalla collaborazione tra OGEPO – Osservatorio interdipartimentale per gli Studi di Genere e le Pari Opportunità dell'Università degli Studi di Salerno e CRID – Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità dell'Università degli Studi di Modena e Reggio Emilia, mira a sensibilizzare e prevenire il sessismo online, fenomeno sempre più diffuso nelle piattaforme digitali, concentrandosi sull'analisi delle dinamiche violente e discriminatorie che si verificano sui social media, luoghi virtuali in cui gli stereotipi sessisti e la misoginia si manifestano in modo virulento, e in particolare su TikTok. Per maggiori informazioni: https://www.crid.unimore.it/site/home/archivio-progetti/articolo1065068574.html. Nell'ambito di questa più ampia progettualità si è sviluppato anche il Progetto di Public Engagement (2024) *TikTok e dintorni: buone pratiche per una cittadinanza digitale 'sicura' nell'era dei social network*, da me coordinato: https://www.crid.unimore.it/site/home/progetti/articolo1065068574.html. Per un'analisi in chiave giusfilosofica e, al contempo, sociologico-giuridica delle questioni: Casadei (2025a).

9 Il fenomeno è in crescita, anche in Italia, spingendo a riflettere sul ruolo cruciale di famiglia, scuola e rete digitale nella sua prevenzione. Secondo un indagine dell'Istituto Superiore di Sanità del 2023, dal titolo "Dipendenze comportamentali nella Generazione Z: uno studio di prevalenza nella popolazione scolastica (11-17 anni) e focus sulle competenze genitoriali" (https://www.iss.it/-/rapporto-istisan-23/25-dipendenze-comportamentali-nella-generazione-z-uno-studio-di-prevalenza-nella-popolazione-scolastica-11-17-anni-e-focus-sulle-competenze-genitoriali-claudia-mortali-luisa-mastrobattista-ilaria-palmi-rena-

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

La questione è certamente complessa, poiché si tratta di una questione multifattoriale, influenzata da determinanti individuali, familiari e sociali. Spesso scaturisce da episodi di bullismo o cyberbullismo[10], sommati a pressioni legate alle aspettative di successo, sia scolastiche, sia relazionali (Viggiani 2022; Campagnoli 2023; Lodevole 2023; Barbuzzi 2024; da ultimo, Mondello 2025).

Per tentare di offrire risposte a questi processi sono maturate diverse iniziative cui sono connesse forme di elaborazione, a cui si farà diretto riferimento in queste pagine, finalizzate al *benessere digitale*[11].

Il concetto di *benessere digitale* è al centro delle attività del Centro di Ricerca dell'Università di Milano-Bicocca[12]: ad orientare le attività di questo centro universitario, come si vedrà nel prosieguo, è la profonda convinzione che l'uso della tecnologia debba essere accompagnato e governato da competenze sociali e culturali le quali permettano ai soggetti di orientarsi in un ambiente digitale sovraccarico di stimoli (Gui *et al*. 2017).

In un simile scenario, alla luce anche di una serie di progetti scientifici e iniziative in cui si dà conto in vari passaggi di questo contributo, si ritiene necessaria una strategia su più livelli, non solo impostata su forme di regolazione, ma su pratiche coordinate che facilitano relazioni e condivisione, e dunque non solo a partire dalle istituzioni, ma anche da forme di partecipazione per così dire "dal basso": ciò implica il saper coniugare la scelta di regole condivise tra scuola, famiglie e giovani con forme di confronto e di

ta-solimini-roberta-pacifici-), infatti, sono circa 66.000 gli adolescenti tra gli 11 e 17 anni potenzialmente affetti da ritiro sociale: cifre simili sono state rilevate dal CNR (https://www.gruppoabele.org/documenti/schede/report_hikikomori_rev_aggiornamento16_01.pdf), che ha individuato circa 54.000 casi tra i 15 e i 19 anni. Un dato significativo, su cui riflettere, è che contrariamente ai luoghi comuni, molte più ragazze – fino a tre volte il numero dei coetanei maschi – vivono un ritiro sociale, seppur moderato; tuttavia, negli stadi più cronici, i maggiori numeri restano tra i ragazzi. Per approfondimenti su queste tematiche si rinvia a Rossi (2025).

10 Si veda, in proposito, il contributo di Anna Rosa Favretto, Elena Ferrara, Riccardo Michele Colangelo.

11 Un progetto certamente interessante è "Custodi Digitali": sorto nel 2020 in Friuli-Venezia Giulia, esso, mettendo in dialogo pediatri, genitori, insegnanti e comunità territoriali, evidenzia quanto sia necessario iniziare fin dai primi anni di vita a costruire un rapporto consapevole e sicuro con la tecnologia, attraverso indicazioni specifiche differenziate per fasce d'età e una responsabilizzazione delle figure adulte di riferimento: il fine è quello del *benessere digitale* (Fasoli 2019; Gui 2019).

12 Sul portale del Centro, nato nel 2016, https://www.benesseredigitale.eu/, oltre ad una presentazione e alla dettagliata mappa dei diversi progetti e attività (che riguardano "le competenze cognitive, il comportamento, le performance scolastiche, la proposta di modelli educativi per le età dell'infanzia e dell'adolescenza") si trovano anche pubblicazioni, articoli scientifici e report che "hanno come focus l'analisi dell'impatto sulla società dei media digitali e le conseguenze legate all'uso e abuso dei device".

iniziativa dei vari attori coinvolti, cercando anche di accorciare le distanze generazionali.

In tal senso, negli ultimi anni, i Patti educativi digitali che sono al centro di questo contributo possono rappresentare un significativo esempio nella promozione di un uso consapevole e responsabile della tecnologia con riguardo alle persone di minore età e agli adolescenti, e che possa essere di buon esempio anche per gli adulti[13].

Intesi come *patti di corresponsabilità* che prendono avvio dalle famiglie e si aprono alla collaborazione con altri soggetti coinvolti nell'educazione (quali scuola, istituzioni e mondo del terzo settore) essi traggono origine dall'idea dei patti educativi e costituiscono un caso di studio interessante sia sotto il profilo della *regolazione* sia, al contempo, sotto il profilo della *partecipazione e della cittadinanza attiva*. Più in generale, essi possono costituire la concreta attuazione di un approccio che, rifuggendo dalle contrapposizioni tra tecno-ottimisti (e tecno-entusiasti) e tecno-pessimisti (e tecno-angosciati), tra tecno-maniacali e tecno-fobici, ossia tra trionfalisti e apocalittici, sappia affrontare le sfide della *civiltà tecnologica* e delle sue *trasformazioni*[14].

Dopo aver descritto i tratti salienti dei Patti educativi e l'orizzonte entro cui si sviluppano (§ 2), ci si soffermerà dunque sui Patti educativi digitali, mettendo in relazione teoria e narrazione di esperienze pratiche (§ 3), per evidenziarne le potenzialità e delinearne alcune ulteriori prospettive (§ 4).

2. I Patti educativi: principi, finalità, prospettive

I Patti educativi rappresentano strumenti di cosiddetta "*governance* collaborativa" attraverso cui una pluralità di soggetti – a titolo meramente esemplificativo: istituzioni scolastiche, enti del Terzo Settore, amministrazioni locali, famiglie, studenti e gruppi informali – progettano congiuntamente e insie-

13 Come è stato puntualmente rilevato da Lodevole 2024, pp. 287-291, "[…] i minori sono oggetto di speciale attenzione anche da parte delle recenti normative europee in tema di comunicazioni elettroniche e servizi della società dell'informazione (considerando 71 e art. 28 del Digital Services Act o Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE), in quanto essi sempre più frequentemente sono utenti di servizi digitali e, ad esempio, possono disporre dei propri dati personali (art. 8 GDPR), prima del raggiungimento della maggiore età, nonostante questo appaia in palese contrasto con l'assenza di capacità di agire. Queste normative scontano ancora un deficit di armonizzazione con le normative nazionali e rendono evidente il difficile coordinamento tra leggi del mercato e protezione dei minori nel mondo digitale". Ma a questa attenzione sul piano regolatorio non corrispondono una visione e sistematica strategia sul piano pedagogico, e su come il diritto possa favorire determinante pratiche di responsabilità sociale.

14 Come suggerisce con molto equilibrio e solidità di argomenti il bel lavoro di Claudio Sartea (2024), ispirato dalle lungimiranti riflessioni di Sergio Cotta (1968). Per un approccio analogo si vedano le convincenti analisi sviluppate in Llano Alonso (2024).

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

me programmano azioni educative integrate, finalizzate alla promozione del benessere collettivo e alla riduzione delle diseguaglianze educative. Tali patti – differenti da meri contratti[15] – si configurano come accordi o manifesti condivisi, elaborati in seno alla "comunità educante" (Gasparini 2025), volti a definire valori, principi e regole comuni che orientano i comportamenti e le relazioni all'interno dei contesti scolastici e territoriali (Candela 2024).

La finalità principale di siffatti percorsi, corredati da specifici strumenti operativi, risiede nel promuovere ambienti educativi inclusivi, cooperativi e partecipati, in cui le differenze siano riconosciute e allo stesso tempo valorizzate, e in cui il dialogo tra le diverse componenti della comunità – di qui, appunto, la denominazione completa di "Patti educativi di comunità" (Meo 2022 – diventa condizione necessaria per il consolidamento di una cittadinanza attiva e responsabile (Moro 1998, 2013; Cotturri 2013).

In tal senso, essi possono includere disposizioni riguardanti la convivenza civile, la gestione dei conflitti, il coinvolgimento delle famiglie e della società civile nel processo educativo e la valorizzazione delle risorse locali, materiali e immateriali.

Il tema della partecipazione – di cui è ormai ricorrente sottolineare le molteplici forme di crisi (in stretta connessione con la crisi della democrazia) – riveste senz'altro una posizione cruciale, sia nella teoria sia nella prassi, configurandosi come un asse fondamentale della cittadinanza e della qualità della vita (Sclavi 2003). A tal proposito, nel contesto dei Patti educativi è

15 Sulla semantica del patto e su come questa nozione sia, nella tradizione occidentale, alle radici di ogni progetto di condivisione "trascendente gli interessi dei singoli coinvolti" (e dell'intera grammatica del costituzionalismo europeo come insieme di principi e pratiche di regolazione) restano un riferimento imprescindibile le riflessioni di Paolo Prodi (2005, pp. 1-22).

Con riferimento al mondo scolastico, va ricordato che è stato il Decreto del Presidente della Repubblica 21 novembre 2007, n. 235 a introdurre il "Patto educativo di corresponsabilità": più precisamente, all'articolo 3 del "Patto educativo di corresponsabilità e giornata della scuola" si legge: "1. Dopo l'articolo 5 del Decreto del Presidente della Repubblica 24 giugno 1998, n. 249, è inserito il seguente: "Art. 5-bis (Patto educativo di corresponsabilità). – 1. Contestualmente all'iscrizione alla singola istituzione scolastica, è richiesta la sottoscrizione da parte dei genitori e degli studenti di un Patto educativo di corresponsabilità, finalizzato a definire in maniera dettagliata e condivisa diritti e doveri nel rapporto tra istituzione scolastica autonoma, studenti e famiglie. 2. I singoli regolamenti di istituto disciplinano le procedure di sottoscrizione nonché di elaborazione e revisione condivisa, del patto di cui al comma 1". "Patto educativo di corresponsabilità" è dunque quell'atto, firmato da genitori e studenti contestualmente all'iscrizione a scuola, capace di stabilire un vincolo tra scuola e alunni attraverso una enucleazione ben definita e circoscritta di principi e comportamenti che la scuola, gli alunni e, naturalmente per essi le famiglie, condividono e si impegnano a onorare. Per quanto tale atto sia assai frequentemente inteso come un "vincolo contrattuale tra i contraenti (scuola e alunni)", esso può essere come strumento base di una forma di reciprocità (e di relazione) tra la scuola e i nuclei famigliari che eccede la grammatica esclusivamente giuridica dell'atto. Per un approfondimento delle finalità sociali di questo patto si veda Manti (2015).

emersa con forza la dimensione di *cittadinanza attiva*, intesa come capacità di soggetti sociali – abitanti, singoli o associati – di mobilitarsi per l'interesse pubblico, di esercitare pressione sulle istituzioni e di stimolare innovazione, ponendosi non come sostituti dell'azione pubblica, ma come promotori di una cultura autenticamente partecipativa.

Dal punto di vista giuridico, i Patti educativi di comunità si inseriscono nel *paradigma dell'amministrazione condivisa* (Arena, Bombardelli 2022; sui nessi tra democrazia partecipativa e amministrazione condivisa, Arena 2017), sancito dagli articoli 55 e 56 del Codice del Terzo Settore (D.lgs. 117/2017), nonché dal principio costituzionale di sussidiarietà orizzontale (art. 118, co. 4 Cost.), ribadito dalla Corte costituzionale con la sentenza n. 131 del 2020, che riconosce alla *co-progettazione* una funzione costitutiva del nuovo assetto collaborativo tra pubblico e privato sociale[16].

In tal senso, i Patti educativi si distinguono come strumenti in grado di implementare la capacità generativa della cittadinanza attiva, favorendo forme di cooperazione territoriale che non si limitano alla dimensione scolastica, ma si estendono a quella urbana e culturale.

I Patti educativi diventano dunque l'esemplificazione di pratiche di cooperazione, ispirate alla fiducia[17]:

> […] stringere un patto rappresenta un atto di responsabilità e fiducia: ognuno dei soggetti coinvolti decide di assumersi, consapevolmente, le proprie responsabilità e al contempo si affida all'altro, in un gioco delle parti che si poggia sull'equilibrio tra responsabilità individuale e fiducia collettiva. Si tratta di un genuino accordo di cooperazione, in cui si segue una logica per somma e non per sottrazione, poiché ogni soggetto coinvolto è parte delle decisioni che verranno assunte e ha il diritto di essere ascoltato e le sue opinioni di essere prese in esame (Severi 2025).

I Patti educativi diventano così strumenti non solo normativi e organizzativi, ma anche di indirizzo culturale, mediante i quali è possibile dare vita a percorsi di *empowerment*, valorizzando le competenze, nonché costruendo reti solidali grazie alle quali può essere valorizzata una cittadinanza consapevole e attiva. L'interazione concreta tra soggetti – istituzionali, associativi ma anche di tipo informale – è ciò che consente alla comunità, intesa appunto come comunità *educante*, di elaborare risposte ai bisogni educativi.

Lo sviluppo di percorsi partecipativi efficaci richiede un disegno attento, capace di attivare scambi e interazioni, fiducia e ascolto, affidamento e partecipazione: non si tratta soltanto di raggiungere obiettivi formali, ma di

16 Il testo della sentenza al seguente link: https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2020&numero=131

17 Il rilancio della nozione di "fiducia" e delle sue possibili pratiche, si deve a Tommaso Greco (2021).

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

coltivare un'educazione nella quale la scuola diventa fulcro di un percorso di cambiamento che prova a fornire risposte ai dilemmi, agli interrogativi, al disorientamento che attraversano l'intera società, e le diverse forme di interazione di quella che rappresenta una generazione non solo immersa in nuovi ambienti, ma "datificata" (Martoni 2025). In questo quadro, i Patti educativi di comunità potrebbero rappresentare un orizzonte di trasformazione possibile, purché sorretti da visioni lungimiranti, pratiche realmente inclusive e – aspetto sempre altamente problematico – risorse adeguate.

In questo contesto, che resta ancora sul versante prevalentemente programmatico, nasce a settembre 2021 l'Osservatorio Nazionale sui Patti educativi[18] a seguito di un accordo tra INDIRE[19] – Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa e Labsus[20] – Laboratorio per la sussidiarietà: esso costituisce un luogo di ricerca e monitoraggio volto a raccogliere, analizzare e valorizzare le esperienze di Patti educativi attivate sul territorio nazionale, con particolare attenzione ai contesti in cui operano le piccole scuole.

Più precisamente, l'azione dell'Osservatorio si articola nella costruzione di una mappatura dinamica e in costante aggiornamento degli attori, delle alleanze e delle pratiche educative che si sviluppano localmente a sostegno dell'offerta formativa delle istituzioni scolastiche.

I Patti educativi vengono intesi come strumenti innovativi e privilegiati per delineare un nuovo paradigma scolastico, fondato sul riconoscimento della comunità come nucleo centrale delle pratiche didattiche e dello spazio di apprendimento. Tale mutamento delinea un ambiente aperto, inclusivo, e proficuo per le relazioni interpersonali, nel quale vengono adoperate in modo integrato dimensioni formali e informali dell'apprendimento, e sperimentate anche nuove modalità e pratiche di interazione educativa.

L'Osservatorio si propone dunque di accompagnare e sostenere forme innovative di scuola aperta al territorio, favorendo processi di coprogettazione educativa ispirati ai principi di sussidiarietà orizzontale e corresponsabilità tra scuola e comunità.

In definitiva, mediante tali obiettivi, l'Osservatorio si propone di contribuire al consolidamento di una cultura educativa *collaborativa*, capace di promuovere inclusione, innovazione e coesione sociale. Siffatti obiettivi si

18 https://www.indire.it/progetto/osservatorio-nazionale-sui-patti-educativi/.

19 INDIRE – Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa è un ente pubblico di ricerca che, sin dalla sua istituzione nel 1925, accompagna i processi di trasformazione del sistema scolastico italiano.

20 Labsus – Laboratorio per la Sussidiarietà (https://www.labsus.org/) – è un'associazione culturale fondata nel 2005 con l'obiettivo di promuovere la piena attuazione del principio di sussidiarietà, come sancito dall'articolo 118, quarto comma, della Costituzione italiana.

ritiene possano essere perseguiti anche con specifico riguardo agli ambienti digitali e ai loro "abitanti".

In questa direzione, tra febbraio e aprile 2025 il Ministero dell'Istruzione e del Merito ha promosso il Percorso Formativo "L'innovazione a scuola attraverso i Patti Educativi di Comunità", nell'ambito della Piattaforma del PNRR per la formazione del personale scolastico "Scuola Futura"[21]. Il corso è stato interamente dedicato all'approfondimento dell'uso dei Patti educativi di comunità come strumenti capaci di coniugare innovazione didattica e rafforzamento della comunità educante.

La proposta si inserisce nel più ampio quadro della transizione digitale della scuola italiana, con l'intento di offrire ai partecipanti del corso sia riferimenti teorici, sia strumenti pratici e operativi per la progettazione, realizzazione e gestione dei patti.

Il percorso è stato indirizzato specificamente a dirigenti scolastici, personale di sistema e docenti, e ha avuto come destinatarie tutte le scuole di ogni ordine e grado del primo ciclo d'istruzione, ossia scuole dell'infanzia, scuole primarie e scuole secondarie di primo grado, sull'intero territorio nazionale.

L'obiettivo generale del percorso è quello di comprendere il valore strategico dei Patti come chiave per il rinnovamento delle pratiche scolastiche e per la costruzione di alleanze durature tra attori educativi, istituzionali e sociali. Nel corso della formazione sono stati dunque esplorati modelli organizzativi analogici e digitali, volti a facilitare l'integrazione tra scuola e territorio, promuovendo un approccio collaborativo e cooperativo alla definizione dell'offerta educativa.

3. Patti educativi *digitali*: esperienze e casi concreti in Italia

In questo orizzonte di rinnovata attenzione alla partecipazione educativa e alla corresponsabilità formativa tra scuola, famiglie e territorio, si colloca con coerenza l'esperienza dei Patti educativi digitali[22].

21 https://scuolafutura.pubblica.istruzione.it/l-innovazione-a-scuola-attraverso-i-patti-educativi-di-comunit%C3%A0.

22 Dopo aver appreso l'esistenza e lo sviluppo di quest'iniziativa grazie ad Andrea Rossetti, con il quale ho avuto poi la possibilità di dialogare sul tema, nell'ambito di una Tavola rotonda da me coordinata su "Scuola e Famiglie di fronte alla sfida del digitale organizzata", a Modena il 28 settembre 2023, presso Smart Life Festival con la partecipazione di Paola Salomoni (Assessora a scuola, università, ricerca, agenda digitale - Regione Emilia Romagna), Giorgio De Rita (Segretario Generale Censis), Roberto Basso (Direttore Relazioni Esterne e Sostenibilità - Wind Tre), Grazia Baracchi (Assessora a istruzione, formazione professionale, sport, pari opportunità - Comune di Modena) ho potuto approfondire i presupposti di questa importante progettualità con Marco Gui, tra i fondatori del Centro sul benessere digitale precedentemente menzionato e tra i suoi principali promotori, nell'ambito di un seminario dal titolo "I patti digitali. Educazione mediale e ruolo delle istituzioni"

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

Questi Patti nascono "dal basso" al fine di rispondere al crescente senso di spaesamento che investe famiglie e contesti educativi nell'era della *connessione permanente* (Gui 2019, pp. 119-161; Sgorlon 2024) e dell'*iperconnessione* (Mauceri, Di Censi 2020; sui c.d. "hikikomori", Lancini 2019). Il contesto educativo, infatti, fortemente influenzato dalla crescente digitalizzazione, rischia sovente di trovarsi impreparato di fronte alla grande sfida del digitale e dinanzi ai molteplici rischi che la tecnologia porta inevitabilmente con sé[23].

Come ha puntualmente osservato Claudio Sartea:

> [s]e qui ci concentriamo sulle professioni liberali, un primo comparto che è stato direttamente e massicciamente coinvolto nelle nuove tecnologie è quello dell'istruzione. È nota a tutti la nota tendenza […] ad introdurre le nuove tecnologie nell'ambito didattico […] anche e soprattutto […] nelle relazioni educative, come uno strumento da considerare inizialmente utile, e poi sempre più convintamente indispensabile (Sartea 2024, p. 228).

Eppure – nonostante il dibattito sia ancora in corso e aperto – molteplici sono gli studi che chiedono prudenza, ma soprattutto preparazione e consapevolezza rispetto all'utilizzo degli strumenti e dei dispositivi digitali da parte delle persone di minore età, degli adolescenti, ancor più nei contesti educativi.

In parallelo alla formazione e alla valorizzazione del corpo docente e dell'intero personale scolastico, diviene necessaria una vera e propria *alfabetizzazione digitale* che, come nota molto opportunamente Barbara G. Bello, deve essere intesa come educazione ai diritti fondamentali, digitali e non digitali (Bello 2023, pp. 103-105): infatti "i nativi digitali solo apparentemente sono in grado di sfruttare pienamente e correttamente le tecnologie informatiche" (Illica Magrini 2025, p. 249). Per esercitare a pieno i propri diritti fondamentali (e digitali[24]) e una vera e propria cittadinanza (compresa quella digitale, Martoni 2025), non è pertanto "sufficiente l'uso spontaneo e intuitivo dei dispositivi, bensì sono richieste conoscenze informatiche di base, abilità operative digitali (*skills*) e una sensibilizzazione sull'etica e sui valori necessari per un uso accorto su internet" (Illica Magrini 2025, pp. 248-249).

---

organizzato il 17 maggio 2024 nell'ambito del Dottorato in "Humanities Technology and Society" in collaborazione con il Corso di Informatica del Dipartimento di Giurisprudenza dell'Università di Modena e Reggio Emilia.

23 Per una mappa dei rischi – dall'iperconnettività all'autoreclusione, dal sessismo al cyberbullismo, dallo *sharenting* alle fake news fino a quelli estremi che si celano nel dark web – si può ora vedere Casadei, Barone, Rossi (2025).

24 Per un'approfondita riflessione sui diritti digitali delle persone di minore età, con particolare riguardo al contesto spagnolo, che si è dotato di una apposita *Carta de Derechos Digitales y los derechos humanos de los niños, niñas y adolescentes*, si rinvia, da ultimo, a Barranco Avilés (2025).

I Patti educativi digitali rappresentano una declinazione specifica dei Patti educativi di comunità, per rispondere proprio a siffatte esigenze: essi si fondano sugli stessi presupposti di alleanza territoriale e partecipazione condivisa, ma si focalizzano sull'accompagnamento consapevole all'uso delle tecnologie da parte di bambini, bambine e adolescenti, con particolare attenzione all'età di accesso allo smartphone e alla costruzione di regole comuni tra famiglie e istituzioni.

La proposta dei patti digitali si caratterizza per l'adozione di un "*approccio comunitario" all'educazione mediale* (Gui *et al*. 2022), che non si limita a interventi informativi, ma punta alla creazione di ambienti educativi coerenti, in cui genitori, scuole e attori del territorio – istituzionali e associativi – agiscono in modo coordinato e si misurano in maniera accurata con gli ambienti digitali le loro peculiarità.

In questo senso, i Patti educativi digitali non solo arricchiscono il panorama delle esperienze partecipative in campo educativo, ma mostrano la fecondità di un modello generativo di cittadinanza attiva, capace di rispondere alle sfide poste dall'accelerazione tecnologica (Wajcman 2020) attraverso pratiche di cura, responsabilità condivisa e costruzione partecipata ("dal basso") di norme educative adeguate alle sfide del presente e alle diverse forme di "vulnerabilità digitale" (Dadà 2024), con specifico riferimento alle nuove generazioni.

I Patti educativi digitali[25] e la rete che ne è scaturita rappresentano un'indicazione strategica che vale la pena conoscere e valorizzare (Rete nazionale dei patti digitali di comunità)[26].

25 Per tutte le informazioni si rinvia al portale https://pattidigitali.it/.

26 L'esperienza pilota è nata grazie alla collaborazione delle prime due iniziative sorte sul territorio italiano: quella friulana e quella lombarda. Più precisamente, il primo progetto si sviluppa grazie all'iniziativa della Regione autonoma Friuli-Venezia Giulia e dell'associazione MEC – Media Educazione Comunità, in collaborazione con gli Istituti comprensivi di Gemona del Friuli, di Trasaghis e con le scuole paritarie del territorio, la Rete B*sogno d'esserci, gli Istituti comprensivi di Udine e le scuole paritarie del capoluogo, la Rete cittadina degli Istituti del primo ciclo di Udine, gli Istituti comprensivi e i Comuni di Pozzuolo del Friuli e di Mortegliano, nonché con i pediatri di famiglia aderenti al progetto "Custodi Digitali" menzionato in precedenza.

L'esperienza avviata in Lombardia nasce invece dalla collaborazione tra il Centro di Ricerca "Benessere Digitale" dell'Università degli Studi di Milano-Bicocca (https://www.benesseredigitale.eu/) e tre associazioni attive nell'ambito dell'educazione consapevole all'uso dei media: Meic, Aiart Milano e Sloworking.

Dal confronto tra queste due esperienze fondative ha preso forma l'idea di un ampliamento dell'iniziativa: il Centro di Ricerca "Benessere Digitale", insieme a MEC, all'Associazione AIART-Milano e all'Associazione culturale Sloworking, ha promosso l'istituzione di un Coordinamento nazionale con l'obiettivo di estendere il modello dei patti digitali ad ulteriori contesti. Per un approfondimento su questa esperienza e sulle sue motivazioni fondanti, si rimanda a Gui, Fiore, Grollo, Garassini, Lanza 2023.

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

L'obiettivo prioritario del progetto consiste nel promuovere la costituzione e il consolidamento di Patti di comunità volti a regolamentare, in modo partecipato, l'uso delle tecnologie digitali tra bambini, bambine e adolescenti su scala nazionale, nonché a promuovere forme di utilizzi e fruizione degli strumenti digitali attente e volte al rafforzamento dei legami sociali.

Alla base dell'iniziativa vi è la convinzione che la sfida di un utilizzo sano ed equilibrato del digitale possa essere affrontata efficacemente solo attraverso un'azione collettiva e coordinata, che coinvolga in maniera attiva l'intera comunità educante e alcune esperienze già in atto hanno dimostrato l'efficacia di questo approccio partecipativo. L'intento, dunque, è quello di favorire spazi di dialogo e confronto tra genitori, insegnanti e altre figure educative con cui le persone di minore età entrano quotidianamente in relazione, al fine di definire un insieme di regole comuni, che possa costituire la base di un'educazione digitale consapevole.

In particolare, i punti principali di un patto che la Rete nazionale promuove sono tre: in primo luogo "Decidere insieme il momento" nel quale le persone di minore età – e i giovani in generale – possono sperimentare diversi tipi di schermi, nonché differenti contenuti; in secondo luogo "partecipare con le famiglie a momenti di educazione digitale", mediante l'organizzazione di incontri divulgativi, nonché di scambio di esperienze, al fine di promuovere un uso degli strumenti digitali creativo, divertente e partecipato dalle famiglie; infine "regolare l'utilizzo dello smartphone e dei dispositivi digitali", stabilendo accordi tra genitori e figli che entrambe le parti si impegnano a rispettare.

Sulla base di tali premesse, è stato stilato un "Manifesto dell'educazione digitale di comunità"[27], che si articola in cinque punti, ossia:

1. Sì alla tecnologia nei tempi giusti
2. Preparare l'autonomia digitale
3. Regole chiare e dialogo
4. Adulti informati e disponibili a cambiare abitudini
5. Serve una comunità!

Ad oggi, la Rete conta 125 patti digitali avviati, 21 patti in avvio e 15 regioni coinvolte.

Tra questi rientra l'esperienza del Patto Educativo Digitale della città di Milano, promossa nell'ambito del progetto MUSA (Multilayered Urban Sustainability Action), finanziato con fondi del PNRR, e che ha visto la partecipazione di numerosi enti, tra cui il Comune di Milano e ATS Milano, CORECOM Lombardia e altri attori del territorio, oltre, naturalmente, all'Università di Milano Bicocca.

27 https://pattidigitali.it/#manifesto.

L'esperienza è significativa e meritevole di menzione: oltre ad aver portato alla pubblicazione di un Report redatto sulla base di uno studio empirico che ha coinvolto più di 11.000 partecipanti tra genitori e bambini – attraverso la compilazione di un questionario – essa ha consentito di esplorare temi quali il possesso e l'uso dei dispositivi digitali, l'autonomia online delle persone di minore età, l'applicazione del parental control e le percezioni su rischi e opportunità offerti dalla tecnologia. Anche sulla base delle evidenze raccolte è stata redatta la "Raccomandazione di Milano", presentata ufficialmente il 10 ottobre 2024 in occasione della Milano Digital Week[28].

Questo documento è costituito da otto linee guida volte a supportare persone adulte e istituzioni nella promozione di un utilizzo sano e consapevole delle tecnologie da parte delle nuove generazioni[29].

Il percorso va così consolidandosi, come dimostra il fatto che a poco più di un anno di distanza dal Primo meeting nazionale dei Patti Digitali, incentrato sulle possibili azioni di supporto per aiutare i genitori e le famiglie ad affrontare le nuove sfide educative poste dalla società digitale, il 31 gennaio 2025 si è tenuto il secondo incontro nazionale, dal titolo "Il villaggio cresce: i Patti di comunità per l'educazione digitale", nel corso del quale la rete dei Patti Digitali ha tracciato un primo bilancio dei risultati raggiunti (cfr. Gasparini 2025).

4. Prospettive e alleanze per un'educazione digitale consapevole

Mentre le iniziative continuano a svilupparsi e diffondersi[30] e trovano spazi di confronto e discussione anche a livello internazionale[31], pare possibile

28 https://www.comune.milano.it/documents/20126/497184820/Raccomandazioni_di_Milano.pdf/b70f5555-6f2c-b4d2-e1a9-4ee720ae0ea6?t=1734350612490.

29 I punti principali sono i seguenti:

1. "Consapevolezza degli adulti". 2. "Autonomia digitale crescente e fase specifica". 3. "Osservanza delle indicazioni delle fonti istituzionali già esistenti". 4. "Smartphone e altri dispositivi personali connessi". 5. "Il mondo fisico è irrinunciabile". 6. "Sviluppare le competenze digitali". 7. "Compiti a casa su Internet". 8. "Collaborazione tra mondo educativo, sanitario e sociale.

30 Sul territorio modenese, sia consentito menzionare il gruppo di lavoro "Patti educativi digitali e uso consapevole della rete" (https://www.crid.unimore.it/site/home/attivita/laboratori-e-gruppi-di-lavoro/articolo1065068599.html), nato in seno all'Officina Informatica DET – Diritto Etica Tecnologie, istituita presso il CRID – Centro di Ricerca interdipartimentale su Discriminazioni e vulnerabilità, Unimore.

Il gruppo di lavoro, coordinato dalla Dott.ssa Claudia Severi e dalla Prof.ssa Barbara G. Bello, collabora con la Rete Patti educativi, promuovendo il modello dei patti educativi digitali mediante incontri nelle scuole e in varie realtà associative e istituzionali del territorio.

31 Nel gennaio scorso si è tenuta la Future House del Forum di Davos, un raduno internazionale di chi si occupa degli effetti collaterali dei media digitali sui bambini, all'interno

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

delineare alcuni aspetti particolarmente interessanti, sui quali potrebbe poggiare una strategia d'insieme.

Stando ad un primo aspetto, che tiene in conto la questione sul benessere degli adolescenti come "abitanti digitali", i dati raccolti dagli ormai molteplici studi mettono in evidenza i diversi effetti collaterali di un'esposizione precoce, prolungata e non mediata alla tecnologia, in particolare allo smartphone: tra questi, interferenze significative sullo sviluppo neuro-cognitivo, problemi dell'attenzione, ricadute sull'apprendimento e sulla memoria, compromissione delle capacità relazionali e una crescente difficoltà nella regolazione emotiva (Bozzola, Spina, Ruggiero *et al.* 2018, pp. 1-5).

Studi recenti mostrano, inoltre, una correlazione tra uso intensivo dei dispositivi digitali e incremento dei livelli di ansia, isolamento sociale, disturbi del sonno e sensazione di disconnessione dalla realtà, soprattutto tra i giovani tra i 10 e i 19 anni.

La difficoltà a bilanciare vita online e offline alimenta un senso di frustrazione e solitudine, che può avere ripercussioni significative sul benessere psicologico delle nuove generazioni[32].

Si rinvengono qui alcune motivazioni che, nel luglio 2024, hanno portato ad una prima circolare ministeriale[33] che ha vietato l'uso dello smartphone, anche per fini didattici, nelle scuole primarie e secondarie di primo grado, e nel giugno 2025 ad una seconda circolare che ha portato all'estensione del divieto anche alle secondarie di secondo grado. Il dibattito è aperto[34], la

---

del quale la Rete dei Patti digitali è stata rappresentata da Marco Gui. Cfr. il reportage Gui, 26 gennaio 2025.

32 https://diariodelweb.it/trend/generazione-z-disconnessione-vita-online-offline-esperimento-sociale-lenovo/.

33 Ministero dell'Istruzione e del Merito, Circolare avente a oggetto "Disposizioni in merito all'uso degli smartphone e del registro elettronico nel primo ciclo di istruzione - A.S.2024-2025., 11 luglio 2024: https://www.mim.gov.it/documents/20182/7975243/m_pi.AOODPIT.REGISTRO+UFFICIALE%28U%29.0005274.11-07-2024.pdf/bc4c9df9-c36f-aa79-d582-e0903ac162e3?version=1.0&t=1720722711827.

34 Attualmente in Parlamento sono in discussione quattro disegni di legge, presentati rispettivamente dalle Onorevoli Marianna Madia, Lavinia Mennuni, Giulia Pastorella, e congiuntamente dagli Onorevoli Gilda Sportiello e Devis Dori, che affrontano, da prospettive diverse ma convergenti, il tema dell'educazione digitale delle persone di minore età.

Questi testi, pur provenendo da forze politiche differenti, sono accomunati dalla consapevolezza dell'urgenza di intervenire di fronte all'impatto crescente delle tecnologie digitali sull'infanzia e sull'adolescenza, con particolare attenzione all'uso precoce degli smartphone e ai rischi connessi a una fruizione non accompagnata dei dispositivi digitali.

I quattro disegni propongono misure orientate sia alla regolazione dell'accesso personale ai dispositivi, sia al rafforzamento dell'educazione digitale all'interno dei percorsi scolastici. Si sottolinea la necessità di coinvolgere in modo strutturato famiglie, scuole e istituzioni territoriali, promuovendo strumenti come i patti educativi e percorsi di consapevolezza e responsabilizzazione. La finalità comune è quella di costruire un quadro normativo che non si limiti a vietare o a sanzionare, ma che accompagni bambini e adolescenti in un percorso

necessità di tutelare i minori da un accesso precoce e autonomo alla rete è ormai attestata, e aumentano da parte di molte famiglie e altre figure educative le richieste di raccomandazioni collettive, coadiuvate dal fatto che difficilmente le istituzioni possono restare neutrali.

Nell'assenza di indirizzi istituzionali pienamente condivisi, si stanno diffondendo in Italia, come in diverse parti del mondo, gruppi "dal basso" che, come accennato in precedenza, si autoregolano attraverso norme sociali elaborate e messe a punto al loro interno. Per esempio, decidono insieme l'età di arrivo degli smartphone, l'età di apertura di un profilo social, ragionano sugli usi significativi degli schermi adatti alle diverse età.

Si parla sempre più spesso della promozione di Smartphone-Free Schools, "scuole in cui, pur utilizzando una didattica digitale guidata dall'insegnante e con strumenti della scuola, è vietato l'utilizzo di dispositivi personali connessi alla rete" (Gui 2025). Inoltre, si discute molto di leggi per regolamentare le piattaforme, nonché della loro possibilità di utilizzare i dati personali e dell'obbligo di verificare l'età degli utenti. Questi dibattiti, oltre a voler migliorare l'ambiente relazionale scolastico, sollecitano le istituzioni ad assumere posizione sul tema e varare provvedimenti specifici.

Un secondo aspetto emerge dai confronti che si svolgono nel mondo della scuola e chiama in causa anche profili relativi più strettamente al diritto e, se si vuole, alla cultura giuridica: un'attenzione crescente è riservata alla prevenzione e al contrasto dei fenomeni giuridicamente rilevanti che coinvolgono l'universo digitale giovanile. Se, insieme alle opportunità, alle possibilità, alle sfide avvincenti, "la tecnologia aumenta il crimine" (Amato Mangiameli, Campagnoli 2020, pp. 123-166) e l'informatica assume molteplici forme criminali (Pietropaoli 2025), aumenta, di conseguenza e più ampiamente, il bisogno di sicurezza e di cybersicurezza (Casadei 2025b), il che significa di cura degli ambienti digitali e delle pratiche che in essi si sviluppano.

Alcuni fenomeni, in tempi recenti, hanno vividamente offerto conferma di questi processi.

Basti pensare, proprio con specifico riferimento al mondo della scuola, al cyberbullismo, disciplinato in Italia dalla Legge 71/2017: quest'ultima, per la prima volta, ha introdotto una definizione normativa del fenomeno e misure specifiche di tutela per i giovani coinvolti, tra cui il diritto alla rimozione dei contenuti lesivi e la possibilità, anche per i minori stessi, di segnalare direttamente al gestore del sito o del social network i contenuti offensivi. La recente Legge 70/2024[35] ha ampliato le disposizioni in mate-

di crescita capace di integrare la dimensione digitale in modo critico, equilibrato e rispettoso dei loro diritti.

35 Vale la pena anche richiamare la L. 29 giugno 2024, n. 90 che, seppur focalizzata sulla cybersicurezza nazionale, prova a rafforzare la tutela preventiva nel digitale, introducendo obblighi per le pubbliche amministrazioni e per gli enti strategici di gestire tempestiva-

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

ria, rafforzando gli obblighi formativi per le scuole e le responsabilità degli adulti (Mondello 2025).

Un ulteriore ambito particolarmente complesso è quello della pornografia non consensuale (denominata impropriamente *"revenge porn"*), oggetto della Legge 69/2019, che ha introdotto l'articolo 612-ter del Codice penale, configurando come reato la diffusione illecita di immagini o video sessualmente espliciti senza il consenso della persona ritratta (Barone 2025): fenomeno, questo, che può coinvolgere anche persone molto giovani.

Un altro ambito assai rilevante è quello che riguarda l'incitamento all'odio online e altre forme di violenza digitale (Bello, Scudieri, 2022; Severi 2023). Tra queste, il cd. *hate speech* pone interrogativi rilevanti in termini di legame con condizioni di vulnerabilità pregresse e di possibili risposte normative, posto che questi contenuti si pongono al limite – labile – tra libertà d'espressione e offesa alla dignità personale (Mondello 2025).

A partire da tali fenomeni – che possono risultare penalmente rilevanti – la riflessione non può limitarsi al piano repressivo o sanzionatorio, considerato che non tutte le condotte richiamate sono sempre, o necessariamente, sussumibili in precise fattispecie di reato.

Al contrario, diventa fondamentale evidenziare l'appropriatezza di un approccio fondato piuttosto sulla prevenzione, sulla responsabilizzazione e sull'educazione alla cittadinanza digitale (e il 2025, per inciso, è l'anno dedicato a questo obiettivo dal Consiglio d'Europa; cfr. Bello 2025[36]), in altri termini all'uso consapevole delle tecnologie, che accompagni le diverse fasi del percorso evolutivo e di crescita dei giovani.

In tale prospettiva, i patti educativi digitali paiono poter rappresentare strumenti concreti a disposizione della comunità educante – composta da famiglie, scuole, enti locali, associazioni e servizi territoriali – finalizzati a promuovere una cultura del rispetto, della cura e della legalità anche nello spazio digitale, mediante la costruzione di un quadro comune di regole volte a prevenire l'insorgenza di comportamenti irrispettosi, aggressivi o, appunto, addirittura penalmente rilevanti.

Le esperienze descritte e quelle che via via vanno sviluppandosi, seppur differenti per origine territoriale e impostazione progettuale, convergono nella medesima direzione, ossia la promozione di una cultura dell'educazione digitale che sia condivisa, partecipata e radicata nella responsabilità individuale e collettiva e, al tempo stesso, paiono potersi proficuamente

---

mente i rischi informatici, con particolare attenzione per la sicurezza nei contratti pubblici e nelle forme di *governance* del rischio. La norma ha, dunque, un impatto diretto sui mondi educativi, determinando le azioni di tutte le PA e, dunque, anche dei mondi scolastici pubblici. Per considerazioni puntuali sulla norma si rimanda al contributo di Mittica in questo volume, che critica – in modo condivisibile – l'approccio di fondo di questa legge.

36 Si veda anche il contributo di Giovanni Pascuzzi in questo dossier.

espandere anche in ambiti sino ad oggi rimasti per così dire a latere come quello sportivo[37].

I Patti educativi digitali si configurano così non soltanto come strumenti strategici per far fronte alle sfide poste dalla transizione digitale in una fase della vita così complessa come quella evolutiva ma, più ampiamente, paiono poter offrire una prospettiva, anche di senso, alla sfida della civiltà tecnologica, con l'obiettivo di costituire una solida alleanza tra scuola, famiglie, istituzioni e tutti gli ambiti delle comunità.

Non si tratta semplicemente di tutelare le persone di minore età dai rischi della rete, ma altresì di costruire i presupposti per implementare una educazione che consenta di cogliere le possibilità di una società digitale che, oltre a scambi di informazioni e veloci connessioni, necessita di prossimità, fiducia, cooperazione e di tempi giusti per maturare modalità efficaci per abitare e vivere nuovi ambienti, ma anche quelli più antichi, come il contesto scolastico ed educativo[38].

37 In questa direzione si sta muovendo l'esperienza condotta dal già menzionato gruppo di lavoro "Patti educativi digitali e uso consapevole della rete" del CRID, che, a partire da un accordo di collaborazione con il CSI – Centro Sportivo Italiano di Modena, ha in programma una serie di iniziative che andranno a coinvolgere genitori, educatori ed educatrici dei mondi dello sport, ragazzi e ragazze impegnati nella pratica sportiva, nonché rappresentanti istituzionali.

38 Il presente contributo è stato elaborato nell'ambito del Progetto Safely – Social media Awareness for Education and Legal Youth. Elaborato presso il CRID – Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità dell'Università di Modena e Reggio Emilia e risultato vincitore di un bando a cascata promosso dallo Spoke 8 "Risk Management and Governance" della Fondazione SERICS – Security and Rights in CyberSpace, esso mira alla promozione di un uso consapevole delle tecnologie digitali concentrandosi in particolare sulle giovani generazioni.

Nella fase di messa a punto e prima stesura è stato particolarmente proficuo un soggiorno come Visiting Professor presso la Facultad de Derecho dell'Università di Siviglia, reso possibile dall'invito del suo Decano, il Prof. Fernando H. Llano Alonso (che molto ringrazio) e, più in particolare, una tavola rotonda che ha preso le mosse dal progetto e si è svolta il 19 febbraio 2025.

La trattazione ha potuto inoltre giovarsi delle riflessioni condotte nell'ambito di altri progetti e, in particolare, di DENORIA – Desafios teoricos, eticos y normativos de la inteligencia artificial. Oportunidades y límites de su regulación coordinato dall'Univ. di Oviedo (PI: Prof. Roger Campione – PID2023-146621OB-C21).

Un ringraziamento speciale va al Dott. Marco Mondello, per il censimento di alcuni progetti attivi sul territorio nazionale, e alla Dott.ssa Claudia Severi, la quale non solo mi ha messo assai generosamente a conoscenza di materiali, report e studi sulle questioni affrontate in questo contributo ma ha discusso con me alcuni passaggi chiave, offrendomi con grande acume spunti di analisi e indicazioni fondamentali.

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

Bibliografia

Alvich, V., Cella, F., Suardi, L. (2025), *Intelligenza artificiale e scuola: guida all'uso per docenti, dirigenti (e genitori curiosi)*, Milano, Corriere della Sera.

Arena, G. (2016), Democrazia partecipativa e amministrazione condivisa, in Valastro, A., a cura di, *Le regole locali della democrazia partecipativa: tendenze e prospettive dei regolamenti comunali*, Napoli, Jovene, pp. 229-239.

Arena, G., Bombardelli, M., a cura di (2022), *L'amministrazione condivisa*, Napoli, Editoriale scientifica.

Bagnato, K. (2023), *L'Hikikomori: un fenomeno di auto reclusione giovanile*, Roma, Carocci.

Barbuzzi, N.P. (2024), *Cyberbullismo, odio in rete e diffamazione nell'era digitale. Analisi giuridica e strategie di tutela*, Roma, Duepuntozero.

Barone, V. (2025), "Revenge Porn": la violenza digitale di genere. In Casadei, Th., Barone, V., Rossi, B., a cura di, *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Torino, Giappichelli, pp. 73-86.

Barranco Avilés, M.C. (2025), La Carta española de Derechos Digitales y los derechos humanos de los niños, niñas y adolescentes, *Revista de Derecho Privado*, 48, pp. 47-68.

Bello, B.G. (2023), *(In)giustizie digitali. Un itinerario su tecnologie e diritti*, Pisa, Pacini Giuridica.

Bello, B.G. (2025), Giovani e cittadinanza digitale: strategie internazionali ed europee. In Casadei, Th., Barone, V., Rossi B., a cura di, *Giovani in rete. Guida all'uso consapevole delle tecnologie*, Torino, Giappichelli, pp. 45-60.

Bello, B.G., Scudieri, L., a cura di (2022), *L'odio online: forme, prevenzione e contrasto*, Torino, Giappichelli.

Bruschi, B., Perissinotto, A. (2020), *La didattica a distanza. Cos'è, come potrebbe essere*, Roma-Bari, Laterza.

Campagnoli, M.N. (2024), Revenge Porn, in Amato Mangiameli, A.C., Saraceni, G., a cura di, *Cento e una voce di informatica giuridica*, Torino, Giappichelli, pp. 400-404.

Candela, G., (2024), *I patti educativi per una scuola di comunità. L'esperienza di Fuoriclasse in Movimento*, Save the children.

Carbone, M., Lingua, G. (2024), *Antropologia degli schermi: mostrare e nascondere, esporre e proteggere*, Roma, Luiss University Press.

Casadei, Th. (2021), L'impatto delle tecnologie informatiche e della rete sull'esperienza sociale e giuridica, in Marzocco, V., Zullo, S., Casadei, Th., a cura di, *La didattica del diritto. Metodi, strumenti, prospettive*, seconda edizione, Pisa, Pacini, pp. 156-173.

Casadei, Th. (2025a), TikTok: A Legal Perspective on the Digital Environment, Highly Accessed by Minors, *Revista de derecho privado*, 48, pp. 87-116.

Casadei, Th. (2025b), La direttiva NIS2 tra diritto e tecnologia: normatività, nomotropismo e sfide della cybersicurezza, in Pietropaoli, S., a cura di, *Cybersecurity*, Torino, Epieikeia, pp. 1-15.

Casadei, Th., Barone, V., Rossi, B., a cura di, (2025), *Giovani in rete. Guida all'uso consapevole delle tecnologie*, Torino, Giappichelli.

Cenni, E., Martoni, M., Salerno, G. (2025), Cittadinanza elettronica e intelligenza digitale. Spunti di riflessione a partire dal progetto "Insieme nella rete", in Casadei, Th., Barone V., Rossi, B., a cura di, *Giovani in rete. Guida all'uso consapevole delle tecnologie*, Torino, Giappichelli, pp. 183-196.

Cotta, S. (1968), *La civiltà tecnologica*, Bologna, il Mulino.

Cotturri, L. (2013), *La forza riformatrice della cittadinanza attiva*, Roma, Carocci.

Crepaldi, M. (2019), *Hikikomori: i giovani che non escono di casa*, Milano, Alpes.

Dadà, S. (2024), *Vulnerabilità digitale: etica, intelligenza artificiale e medicina*, Milano-Udine, Mimesis.

Degen, J.L. (2024), *Swipe, like, love. Intimität und Beziehung im digitalen Zeitalter*, Giesen, Psychosozial-Verlag.

Fasoli, M. (2019), *Il benessere digitale*, Bologna, il Mulino.

Federazione italiana medici pediatri (2023), *Bambini e adolescenti in un mondo digitale*, Pisa, Pacini editoria medicina.

Furuhashi, T. *et. alii* (2023), *An examination of the potential benefits of expert guided physical activity for supporting recovery from extreme social withdrawal: Two case reports focused on the treatment of Hikikomori*, *Frontiers in Psychiatry*, 14, pp. 1-14.

Gasparini, G. (2025a), Patti Digitali, famiglie unite per l'educazione: l'esperienza in Italia, *Agenda digitale*, 27 febbraio.

Gasparini, G. (2025b), Per una comunità educante digitale: la formazione di insegnanti e genitori, la partecipazione consapevole dei giovani, in Casadei, Th., Barone V., Rossi B., a cura di, *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Torino, Giappichelli, pp. 155-166.

Giaccardi, C., Magatti, M. (2022), *Supersocietà*, Bologna, il Mulino.

Greco, T. (2021), *La legge della fiducia: alle radici del diritto*, Roma-Bari, Laterza.

Grollo, M., Gui, M., Pellai, A., Oretti, C., Gruppo di lavoro Pediatri del Friuli-Venezia Giulia (2022), Educazione digitale familiare dalla nascita, *Medico e Bambino*, 41, 9, pp. 569-580.

Gui, M. (2019), *Il digitale a scuola. Rivoluzione o abbaglio?*, Bologna, il Mulino.

Gui, M., a cura di (2019), *Benessere digitale a scuola e a casa: un percorso di educazione ai media nella connessione permanente*, Firenze, Mondadori University.

Gui, M., Fasoli, M., Carradore, R. (2017), Digital well-being. Developing a new theoretical tool for media literacy research, *Italian Journal of Sociology of Education*, 9, 1, pp. 155-173.

Gui, M., Fiore, B., Grollo, M., Garassini, S., Lanza, S. (2023), I "patti digitali": un approccio comunitario all'educazione mediale, *Comunicazionepuntodoc*, *28, 2023, pp. 81-104.*

Gui, M., Gerosa, T., Vitullo, A., Losi L. (2020)*, L'età dello smartphone. Un'analisi dei predittori sociali dell'età di accesso al primo smartphone personale e delle sue possibili conseguenze nel tempo*, Report del Centro di ricerca Benessere Digitale, Università di Milano Bicocca, https://boa.unimib.it/retrieve/e39773b8-2216-35a3-e053-3a05fe0aac26/Report-1_Let%c3%a0-dello-smartphone.pdf.

Gui, M., Picca, M., Sala, M. (2024), *Raccomandazioni di Milano sul benessere e la sicurezza online di bambini/e e pre-adolescenti*: https://www.comune.milano.it/documents/20126/497184820/Raccomandazioni_di_Milano.pdf/b70f5555-6f2c-b4d2-e1a9-4ee720ae0ea6?t=1734350612490.

Gui, M. (26 gennaio 2025), Il raduno a Davos sugli effetti collaterali del digitale: «Cresce l'attivismo critico. Ma serve una guida democratica per la tutela dei minori», *Corriere della Sera*, https://www.corriere.it/tecnologia/25_gennaio_26/il-raduno-a-davos-sugli-effetti-collaterali-del-digitale-cresce-l-attivismo-critico-ma-serve-una-guida-democratica-per-la-tutela-e8d8e7b3-010b-4d30-826e-9dc4c1dd3xlk.shtml.

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

Han, B.C. (2022), *Le non cose. Come abbiamo smesso di vivere il reale*, Torino, Einaudi.

Illica Magrini, A. (2025), Il cammino della cittadinanza digitale: criticità, risorse, prospettive di sviluppo, in Casa, F., Gaetano, S., Pascali, G., a cura di, *Intelligenza artificiale: diritto, etica e democrazia*, Bologna, il Mulino, pp. 237-254.

Lavenia, G. (2018), *Le dipendenze tecnologiche: valutazione, diagnosi e cura*, Firenze, Giunti.

Lancini, M. (2019), *Il ritiro sociale negli adolescenti: la solitudine di una generazione iperconnessa*, Milano, Raffaello Cortina.

Llano Alonso, F.H. (2024), *Homo ex machina: ética de la inteligencia artificial y derecho digital ante el horizonte de la singularidad tecnológica*, Valencia, Tirant lo Blanch.

Lodevole, L. (2024), Minore, in Amato Mangiameli, A.C., Saraceni, G., eds., *Cento e una voce di biogiuridica*, Torino, Giappichelli, pp. 287-291.

Longo A., Scorza, G. (2020), *Intelligenza artificiale: l'impatto sulle nostre vite, diritti e libertà*, Milano, Mondadori Università.
Lupton, D. (2015), *Sociologia digitale*, Milano-Torino, Pearson-Italia.
Manti, F., ed. (2015), *Il patto di corresponsabilità educativa: per una scuola socialmente responsabile*, Genova, University Press - De Ferrari Comunicazione.
Marangi, M. (2023), *Addomesticare gli schermi: il digitale a misura dell'infanzia 0-6*, prefazione di Rivoltella, P.C., Brescia, Scholé.
Martoni, M. (2025), Digital Transformation and e-Citizenship. Children's Access to Online Services, *Revista de Derecho Privado*, 48, pp. 69-86.
Mauceri, S., Di Censi, L., a cura di, (2020), *Adolescenti iperconnessi: un'indagine sui rischi di dipendenza da tecnologie e media digitali*, Roma, Armando.
Meo, V., a cura di, (2022), *Educare ai diritti*, *Facciamo un patto! I patti educativi di comunità e la partecipazione dei ragazzi e delle ragazze*, Unicef Italia, Milano, Franco Angeli.
Mignolli, M.S., Locati, A. (2023), *Hikikomori*: *il Re escluso*, Milano, Feltrinelli.
Mondello, M. (2025), Cyberbullismo e "discorsi d'odio": le forme della violenza online, in Casadei, Th., Barone, V., Rossi, B. a cura di, *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Torino, Giappichelli, pp. 87-100.
Morcellini, M., a cura di (2023), *Il digitale fa bene ai bambini?*, Sesto San Giovanni (MI), Meltemi.
Moro, G. (1998), *Manuale di cittadinanza attiva*, con la collaborazione di Costantini, M.P., Roma, Carocci.
Moro, G. (2013), *Cittadinanza attiva e qualità della democrazia*, Roma, Carocci.
Moro, P. (2025), *Diritto ibrido. Metodo del giurista e tecnologie dirompenti*, Milano, Mondadori.
Pezzano, G. (2024), *D1git4l-m3nte: antropologia filosofica e umanità digitale*, Milano, Franco Angeli.
Pietropaoli, S. (2025), *Informatica criminale. Diritto e sicurezza nell'era digitale. Aggiornata alla legge 90/2024 e alla direttiva NIS2*, Torino, Giappichelli.
Pigozzi, L. (2019), *Adolescenza zero: hikikomori, cutters, ADHD e la crescita negata*, Milano, Nottetempo.
Prodi, P. (2005), Il patto politico come fondamento del costituzionalismo europeo, *Scienza & Politica. Per una Storia delle Dottrine*, 17, pp. 1-22.
Rossi, B. (2025). Il rischio dell'autoreclusione. Iperconnettività: hikikomori, in Casadei, Th., Barone, V., Rossi, B., a cura di, *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Torino, Giappichelli, pp. 61-72.

Sagliocco, G., ed. (2011), *Hikikomori e adolescenza: fenomenologia dell'autoreclusione. Seminario di studi e approfondimenti per un'ipotesi di cura*, Milano-Udine, Mimesis.

Saito, T., Angles, J. (2013), *Hikikomori: adolescence without end*, Minneapolis, University of Minnesota Press.

Sartea, C. (2024), *Ecotecnologia. Sfide etico-giuridiche della civiltà tecnologica*, Torino, Giappichelli.

Sclavi, M. (2003), *Arte di ascoltare e mondi possibili. Come si esce dalle cornici di cui siamo parte*, Milano, Bruno Mondadori.

Severi, C. (2023), L'odio online: un fenomeno dai molteplici volti. Alcuni possibili antidoti, *Clionet. Per un senso del tempo e dei luoghi*, 7.

Severi, C. (2025). I patti educativi digitali. Fiducia, cooperazione e diritti per un'educazione digitale consapevole, in Casadei, Th., Barone, V., Rossi, B., a cura di, *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Torino, Giappichelli, pp. 167-182.

Sgorlon, A. (2024), *Relazioni connesse: come essere felici nell'era digitale*, youcanprint.

Verza, A. (2016), *L'hikikomori e il giardino all'inglese: inquietante irrazionalità e solitudine comune*, *Ragion pratica*, 46, pp. 243-258.

Vicari, S. (2022), *Adolescenti che non escono di casa: non solo Hikikomori*, Bologna, il Mulino.

Viggiani, G. (2022), *Il cyberbullismo: considerazioni socio-giuridiche a cinque anni dall'entrata in vigore della legge 71/2017*, in Bello, B.G., Scudieri, L. a cura di, *L'odio online: forme, prevenzione e contrasto*, Torino, Giappichelli, pp. 123-136.

Wajcman, J. (2020), *La tirannia del tempo: l'accelerazione della vita nel capitalismo digitale*, Roma, Luiss University Press.

Child Rights Impact Assessment e design responsabile nella trasformazione digitale. Note per una prima riflessione

Child Rights Impact Assessment and Responsible Design in the Digital Transformation. Notes for a Preliminary Reflection

Michele Martoni[1]

Sommario

La trasformazione digitale sta modificando in profondità le esperienze dell'infanzia, aprendo nuove possibilità ma anche generando rischi rilevanti per i diritti dei minori. In questo contesto, il principio del superiore interesse del minore, riconosciuto dalla Convenzione ONU sui Diritti dell'Infanzia, richiede strumenti capaci di guidare concretamente le scelte progettuali. La valutazione d'impatto sui diritti dei minori o *Child Rights Impact Assessment* (CRIA) risponde a questa esigenza come metodologia di valutazione preventiva, utile a integrare la prospettiva dei diritti nei processi che portano alla realizzazione di tecnologie digitali. Il contributo esamina i limiti del paradigma del consenso informato e propone un cambio di approccio, fondato sulla responsabilità progettuale e sull'etica *by design*. Dopo aver ricostruito il quadro normativo e le principali esperienze internazionali in materia di *impact assessment*, si riflette sul ruolo che le imprese possono e devono assumere nel tutelare l'infanzia *online*. La CRIA viene così delineata come uno strumento capace di coniugare dimensione tecnica, giuridica e culturale. Il paper si chiude richiamando l'importanza di rendere sistematiche le valutazioni d'impatto sui diritti dei bambini, affinché la tutela dell'infanzia diventi parte integrante delle politiche pubbliche e delle strategie del settore privato.

Parole chiave: trasformazione digitale; valutazione d'impatto sui diritti dell'infanzia; CRIA; progettazione responsabile; interesse prioritario del minore

---

1 Università degli Studi di Urbino, Dipartimento di Giurisprudenza. michele.martoni@uniurb.it.

Il presente articolo è frutto delle attività di ricerca del Progetto PRIN 2022 DAFNE (Democratic governance of Automated system for Fake News), finanziato dall'Unione europea - Next Generation EU, Missione 4, Componente 1, CUP H53D23010930001, Codice MUR P2022R7RS.

Data invio: 1 luglio 2025. Data accettazione: 5 settembre 2025.
DOI: https://doi.org/10.54103/1972-5760/30056

Abstract

Digital transformation is profoundly reshaping childhood experiences, offering new opportunities but also posing significant risks to children's rights. Against this backfrop, the principle of the best interests of the child, as established by the UN Convention on the Rights of the Child, must be translated into tools capable of concretely guiding design choices. The Child Rights Impact Assessment (CRIA) meets this need by providing a preventive evaluation method that embeds a child-rights perspective into the development of digital technologies. This paper critiques the limitations of the informed-consent model and advocates for a shift toward a responsibility-driven, ethics-by-design approach. After outlining the relevant legal framework and reviewing key international experiences with impact assessments, the paper examines the role businesses can play in protecting children's rights in digital environments. CRIA is presented as a method that bridges technical, legal, and cultural dimensions. The conclusion emphasizes the urgency of institutionalizing child rights impact assessments, ensuring that the protection of children becomes an integral part of both public policy and corporate strategy.

Keywords: digital transformation; child rights impact assessment; CRIA; responsible design; best interests of the child

1. Introduzione

La trasformazione digitale opera oggi come forza sistemica capace di ridefinire i contorni dell'infanzia, influenzando luoghi, tempi e modi attraverso cui il minore fa esperienza della realtà, apprende, costruisce relazioni e acquisisce consapevolezza di sé (Haidt 2024; Barassi 2021; Twenge 2018).

L'uso precoce e intensivo delle tecnologie nel processo di crescita non si limita a creare un semplice cambiamento di scenario, ma reingegnerizza l'*habitat* (Floridi 2020; Galimberti 2018). I minori non abitano un contesto meramente assistito dalla tecnica, bensì un ambiente a matrice digitale caratterizzato da una forma di normatività implicita, spesso opaca (Maestri 2017; Lessig 1999).

Le tecnologie digitali, se utilizzate e progettate in modo responsabile, possono promuovere l'accesso alla conoscenza, la creatività, la socialità e persino la partecipazione civica. Tuttavia, se prive di una consapevolezza etica e giuridica adeguata, espongono i minori a significativi rischi strutturali, come la profilazione massiva, la manipolazione del comportamento, la chiusura in bolle algoritmiche che limitano l'accesso alla conoscenza.

Nonostante il diritto internazionale, in particolare la *Convention on the Rights of the Child* (o CRC) delle Nazioni Unite, richieda che l'interesse

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

superiore del minore sia prioritario, nella pratica dei servizi digitali spesso tale principio viene subordinato a logiche di mercato focalizzate su *engagement* e monetizzazione, piuttosto che su sicurezza e sviluppo equilibrato del minore (Livingstone *et al.* 2024; Comitato sui diritti dell'infanzia 2021; Livingstone 2020)[2].

In tale contesto, emerge con urgenza l'esigenza di strumenti concreti, da poter portare a sistema, per valutare preventivamente gli impatti delle tecnologie sui diritti dell'infanzia.

Il *Child Rights Impact Assessment* (o CRIA) risponde precisamente a questa necessità, rappresentando uno strumento metodologico capace di integrare i diritti dei minori nei processi di progettazione, sviluppo e distribuzione di prodotti e servizi della società dell'informazione (UNICEF 2024 e 2021; Hoffman 2020; Payne 2019).

Per comprendere la rilevanza di uno strumento come la CRIA, è utile considerare l'esperienza del *Data Protection Impact Assessment* (DPIA), introdotto con il Regolamento Generale sulla Protezione dei Dati (GDPR). Questo strumento si è rivelato fondamentale per rendere operativa la *privacy by design* e *by default*, imponendo ai titolari del trattamento un'analisi sistematica dei rischi connessi al trattamento dei dati[3].

Allo stesso modo, più recentemente, il *Fundamental Rights Impact Assessment* (FRIA), previsto dall'*Artificial Intelligence Act* europeo (*AI Act* o AIA), mira a valutare l'impatto delle tecnologie AI sui diritti fondamentali[4].

La CRIA si colloca in continuità con questi strumenti, ma si distingue per il suo *focus* specifico sulla condizione dell'infanzia, la quale richiede parametri, criteri e metodologie differenti, adattati alla vulnerabilità e alla complessità del soggetto minore (Comitato sui Diritti dell'Infanzia 2013 e 2021).

La CRIA si propone non solo come uno strumento tecnico, ma come un vero e proprio cambio di paradigma. Esso invita a spostare il baricentro della responsabilità, non più sul singolo utente – chiamato a leggere informative complesse o a esercitare un consenso spesso simbolico – bensì sul progettista, sul decisore, sull'impresa. A ciascuno di questi attori si chiede di assumere un ruolo attivo nella promozione di un ambiente digitale che

2 *Convention on the Rights of the Child* (o CRC), approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989, in https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child. Sull'interesse dei bambini come priorità e sull'impatto rispetto alla società si vedano Lalatta Costerbosa (2019), Mittica (2001) e Ronfani (1998).

3 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016. Testo completo disponibile al link ufficiale EUR-Lex: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679.

4 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024. Il testo completo è disponibile su EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=it.

sia non solo funzionale e redditizio, ma anche giusto, inclusivo e rispettoso della dignità delle persone, a partire da quelle più vulnerabili.

In tal senso, la CRIA non si limita a tematizzare i diritti dei bambini in chiave protettiva, ma li assume come lente attraverso cui ridefinire le priorità dell'innovazione digitale stessa. Progettare tenendo conto della condizione minorile implica, in ultima analisi, riconoscere che l'etica dell'innovazione si misura dalla sua capacità di tutelare e valorizzare la soggettività più vulnerabile, restituendo al minore non solo protezione, ma anche voce, *agency* e visibilità.

È dunque importante interrogarsi su come integrare i diritti dell'infanzia nei processi di progettazione tecnologica. Per questo ci sembra utile proporre una riflessione sulla CRIA, intesa come strumento metodologico e culturale capace di orientare il *design* digitale verso la responsabilità e la giustizia sociale. Dopo aver delineato il contesto normativo e tecnologico attuale, ci soffermeremo sui limiti del paradigma del consenso e sulle potenzialità dell'approccio *by design*. Ricostruiremo quindi le basi teoriche, la struttura e gli ambiti di applicazione del *Child Rights Impact Assessment*, per poter infine cogliere prospettive e condizioni utili a renderlo una pratica ordinaria nell'innovazione digitale.

2. Datificazione e profilazione del minore

Nel quadro del capitalismo della sorveglianza – delineato da Shoshana Zuboff (2019) come un sistema fondato sull'estrazione del *surplus* comportamentale – anche l'infanzia viene progressivamente assoggettata a una logica estrattiva che traduce l'esperienza umana in materia computabile.

Sin dai primi istanti di vita, e attraverso tutte le interazioni quotidiane registrate da dispositivi digitali, anche scolastici, ogni azione del bambino viene trasformata in dati. Queste informazioni vengono, quindi, raccolte, classificate e sfruttate economicamente all'interno di un sistema economico fondato sull'attenzione e alimentato dall'incessante raccolta di dati (Barassi 2021; Mascheroni 2020).

Tale processo, reso con il brutto neologismo di *datafication* o datificazione, comporta una trasformazione strutturale delle modalità con cui si interpreta e si codifica la realtà (Martoni 2020; Berlingò 2017; Mai 2016; Van Dijck 2014).

Si tratta di una sorta di rivoluzione simbolica che modifica profondamente i parametri stessi della percezione umana, del significato attribuito alle esperienze, nonché della generazione di valore sociale ed economico (Garapon, Lassègue 2021, p. 44).

In questo contesto, si profila chiaramente il rischio che l'infanzia sia trattata principalmente come una fonte inesauribile di dati da monetizzare.

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

Barassi (2021) documenta efficacemente come la sorveglianza digitale sui minori inizi ancor prima della nascita, attraverso piattaforme di *pregnancy tracking* che raccolgono dati biometrici della madre e del nascituro, integrandoli con informazioni di consumo. Questo fenomeno prosegue sui *social network* – con il cosiddetto *sharenting* – ove viene resa pubblica la vita dei figli, nella prassi senza il loro consenso esplicito. Infine, con l'ingresso all'asilo e poi a scuola, la raccolta e analisi dei dati diviene istituzionale mediante strumenti come i sistemi di *learning analytics*, i *badge* comportamentali, le piattaforme di didattica digitale, e dispositivi IoT come *smartdesk* e telecamere che misurano l'attenzione degli studenti (Paolucci *et al.* 2024; Barassi 2021; Beerwinkle 2021; Selwyn 2019).

Il percorso educativo del bambino viene sempre più frequentemente anticipato e condizionato da modelli predittivi basati su algoritmi che analizzano dati. Da qui il rischio concreto che tali sistemi, prevedendo precocemente eventuali difficoltà scolastiche, generino una profezia auto-avverante, limitando di fatto le opportunità educative e influenzando negativamente lo sviluppo personale dello studente.

Si assiste a un'inversione di ruoli dove non è la tecnologia a essere progettata attorno ai bisogni e alle caratteristiche del minore, bensì è il minore stesso a doversi adattare alle logiche e ai linguaggi delle piattaforme digitali. In questo modo il bambino viene ridotto progressivamente a semplice entità informazionale, modellata secondo le esigenze del sistema tecnico che lo analizza e lo classifica.

La progressiva riduzione della frizione ontologica, cioè della separazione tra la persona e i sistemi digitali che la processano, conduce a una convergenza tra dati, algoritmi e individuo in un unico ecosistema definito infosfera. In questo ambiente digitale, la distinzione fra realtà e rappresentazione digitale diventa sempre meno percepibile.

Il profilo digitale del minore non è solo una rappresentazione della sua identità, ma influenza concretamente le sue possibilità di accesso a servizi essenziali, come istruzione, sanità e credito. Errori, distorsioni o *bias* – per esempio attraverso un'etichetta attribuita da un registro scolastico automatizzato o un punteggio di affidabilità generato all'interno di un *social game* – possono avere conseguenze durature. Tali informazioni, una volta immesse nei sistemi digitali, si replicheranno in una molteplicità di *database*, rendendo estremamente complessa qualsiasi forma di rettifica o cancellazione.

Il GDPR e, nello specifico, l'art. 17 sul diritto alla cancellazione (noto anche come diritto all'oblio), introduce garanzie importanti, ancorché la concreta attuazione, in particolare per i minori, risulti complessa. Cancellare un *link* dai risultati di un motore di ricerca (cosiddetta deindicizzazione) non elimina la copia del dato sui *server* di soggetti terzi, né rimuove le previsioni già derivate o inferite da quei dati. Il vero potere dei dati non è solo di chi li possiede, ma anche dei terzi decisori che li utilizzano.

Profilazione e datificazione sono dinamiche convergenti che generano effetti significativi per l'infanzia (Livingstone, Third 2017; Barassi 2021). Si delineano, in particolare, tre ordini di impatto.

In primo luogo, l'adozione di tecniche di *micro-targeting* promozionale – basate sulla raccolta e analisi di dati personali – permette di orientare l'offerta di beni e servizi attraverso la suddivisione degli utenti in *cluster* omogenei, costruiti a partire da variabili quali l'età, gli interessi o i comportamenti osservati nell'uso delle applicazioni (Hirsch, Binder, Matthes 2025; Barassi 2021). In questo scenario, il bambino non è solo destinatario passivo delle proposte digitali, ma svolge un ruolo attivo nella generazione di dati, è, cioè, al tempo stesso consumatore e produttore (*prosumer*), contribuendo alla definizione della propria identità digitale. A ciò si aggiunge l'impatto derivante dall'esposizione precoce agli algoritmi di raccomandazione che, nel delineare percorsi personalizzati e ripetitivi, tendono a restringere l'esperienza dell'utente censurando altre prospettive e limitando lo sviluppo critico (Pariser 2012).

In secondo luogo, l'introduzione di sistemi di reputazione scolastica nelle piattaforme digitali tende a promuovere modelli di efficienza misurabile, trascurando aspetti fondamentali dell'esperienza educativa, come la creatività, il pensiero critico o le capacità relazionali, difficilmente quantificabili ma essenziali per una formazione integrale.

Infine, i rischi connessi alla sicurezza digitale – come, per esempio, il furto di identità, l'uso improprio di immagini o la diffusione di contenuti falsi (*deepfake*) – risultano particolarmente insidiosi per i minori che non dispongono ancora delle risorse necessarie per tutelarsi in modo autonomo.

Diviene urgente, come opportunamente osserva Barassi, «restituire ai figli dell'algoritmo il diritto al divenire imprevedibile», sottraendo l'infanzia alla logica della predestinazione statistica che deriva dalla continua profilazione algoritmica. In tale prospettiva, la formazione dovrebbe tornare alla sua dimensione originaria di esplorazione aperta, luogo di crescita non predeterminata, piuttosto che ridursi a un addestramento funzionale all'ottimizzazione di modelli predittivi.

La fotografia appena delineata invita a riportare il principio del *best interest of the child* ad una dimensione concreta capace di incidere realmente sulle architetture digitali. Non si tratta solo di una tutela individuale, ma anche di una responsabilità collettiva. Garantire il superiore interesse del minore significa proteggere la sua dignità, il suo diritto a crescere libero da automatismi predittivi e da modelli riduttivi, ma anche custodire l'infanzia come esperienza umana condivisa, come tempo di apertura, relazione e possibilità. In gioco non c'è solo la protezione dei più piccoli, ma la qualità del futuro che siamo in grado di immaginare e costruire.

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

3. Interesse del minore e ambienti digitali

Le legislazioni occidentali in ambito familiare e minorile, e così la CRC, riconoscono l'interesse del minore come principio cardine, da considerarsi preminente in ogni decisione che lo riguardi[5].

Non si tratta solo di tutelare i diritti del minore, ma di promuoverne una crescita armoniosa (Comitato sui Diritti dell'Infanzia 2013).

Questo approccio implica una visione complessiva dello sviluppo, che non si limita agli aspetti fisici o cognitivi, ma si estende alle dimensioni affettive, morali, spirituali, relazionali e psicologiche, riconoscendo l'interconnessione profonda tra i diversi piani dell'esperienza (Comitato sui Diritti dell'Infanzia 2021, p. 10).

Ciò richiede il coinvolgimento attivo e responsabile di tutti i soggetti chiamati a interagire con l'infanzia – dalle istituzioni pubbliche agli operatori sociali, dal mondo della scuola fino alle famiglie – affinché siano garantite non solo la protezione e la sicurezza del minore, ma anche il riconoscimento della sua dignità come persona titolare di diritti.

Il superiore interesse del minore è un principio che consente di intervenire in tre funzioni strettamente interconnesse. La prima è di garanzia a che gli interessi prioritari del bambino siano effettivamente considerati e messi al centro in ogni processo decisionale che lo coinvolge, sia in ambito pubblico sia privato. La seconda è rivolta a impiegare il principio come criterio interpretativo di riferimento, orientando la lettura e l'applicazione delle norme. La terza opera come regola di natura procedurale, imponendo l'obbligo di considerare formalmente e motivare esplicitamente come e in che misura tale interesse sia stato preso in considerazione (Comitato sui Diritti dell'Infanzia 2013, pp. 6 e ss.).

Questa triplice configurazione rende il principio non solo un orientamento etico e giuridico, ma anche uno strumento concreto per garantire che le scelte che incidono sulla vita dei bambini siano realmente orientate alla promozione del loro benessere integrale.

Per cogliere appieno la portata del principio del superiore interesse del minore, è opportuno richiamare due ulteriori elementi centrali emersi nell'interpretazione del Comitato sui diritti dell'infanzia.

Innanzitutto, l'articolo 3 della CRC impone agli Stati l'obbligo di assicurare che gli interessi dei minori siano oggetto di una valutazione accurata e ricevano effettiva priorità in tutte le decisioni e azioni intraprese anche da soggetti privati, compresi i fornitori di servizi (per esempio coloro che

5 L'art. 3 della CRC dispone che «in tutte le decisioni relative ai fanciulli, di competenza delle istituzioni pubbliche o private di assistenza sociale, dei tribunali, delle autorità amministrative o degli organi legislativi, l'interesse superiore del fanciullo deve essere una considerazione preminente». Sull'interesse del minore nella cultura giuridica, si veda, fra gli altri, Ronfani (1997, 1998). Per un ulteriore approfondimento si veda Breen (2002).

erogano servizi della società dell'informazione). Si tratta di un'estensione significativa, che riconosce come la responsabilità di tutelare l'infanzia non ricada soltanto sugli attori istituzionali, ma coinvolga l'intero tessuto sociale ed economico (Comitato sui Diritti dell'Infanzia 2013, p. 10).

In secondo luogo, l'espressione «che riguardano» il minore – contenuta sempre nell'art. 3 – deve essere intesa in senso ampio. Non ci si riferisce soltanto agli atti che direttamente coinvolgono i bambini, ma anche a tutte quelle decisioni che, pur non avendo un impatto immediato o manifesto, potrebbero potenzialmente incidere in modo significativo sulla loro vita e sul loro benessere (Comitato sui Diritti dell'Infanzia 2013, pp. 13 e ss.). Per riprendere l'esempio già menzionato, rientrano nell'ambito di applicazione anche quei servizi della società dell'informazione che, pur non essendo espressamente destinati ai minori, risultano di fatto ampiamente utilizzati da essi, come confermato con frequenza dalla cronaca e da numerose evidenze empiriche.

Allo stesso modo, la formula «in primaria considerazione» va intesa come attribuzione di un peso specifico e prioritario agli interessi del minore nel bilanciamento con altri fattori. Non può essere trattata alla stregua di una valutazione generica o alla pari con altri interessi in gioco (Comitato sui Diritti dell'Infanzia 2013, pp. 14 e ss.).

Questa posizione rafforzata trova giustificazione nello *status* dei bambini, caratterizzato da una naturale dipendenza, da un grado variabile di maturità, da una limitata capacità giuridica e da un ridotto potere di partecipazione nei processi decisionali che li riguardano. Proprio per questa ragione, in assenza di adeguate misure di tutela, i loro interessi rischiano di essere marginalizzati o ignorati.

Adottare il principio del superiore interesse come criterio guida nell'assunzione di decisioni significa, quindi, tenere conto in modo concreto e attuale della sicurezza, del benessere e dell'integrità della persona minorenne. , anche in prospettiva precauzionale, valutando i possibili rischi futuri e le conseguenze a medio e lungo termine.

Assume rilievo fondamentale l'esigenza di una valutazione puntuale e argomentata delle conseguenze che ogni decisione può avere sulla vita e sul benessere del minore.

Il processo decisionale deve essere accompagnato da precise garanzie procedurali, che assicurino trasparenza, tracciabilità e inclusività (Comitato sui Diritti dell'Infanzia 2013, pp. 40 e ss.).

La motivazione della decisione deve esplicitare come e in che misura il superiore interesse del minore sia stato preso in considerazione, specificando i criteri adottati, le fonti valutative utilizzate, nonché l'eventuale bilanciamento operato rispetto ad altri interessi o esigenze in gioco (Comitato sui Diritti dell'Infanzia 2013, pp. 7 e ss.). La sola menzione del principio non

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

è sufficiente, occorre dimostrare che esso ha effettivamente guidato l'intero *iter* decisionale, in coerenza con il ruolo prioritario che gli è riconosciuto.

A tale riguardo, il Comitato sui diritti dell'infanzia ha individuato – pur senza pretese di esaustività o di gerarchia – una serie di elementi che ogni organo decisionale dovrebbe considerare nel determinare ciò che concretamente costituisce il superiore interesse di un minore. Tra questi, assumono particolare rilevanza per il presente lavoro: (i) l'ascolto e la valorizzazione dell'opinione del minore, in linea con l'articolo 12 della CRC, che riconosce la capacità progressiva del bambino di esprimere la propria visione su quanto lo riguarda; (ii) la garanzia di condizioni di protezione e cura adeguate al benessere complessivo del minore (art. 3 CRC), che includono bisogni materiali ed educativi, ma anche dimensioni affettive e relazionali, come il diritto a sentirsi accolto, al sicuro, non esposto a forme di violenza, sfruttamento o trascuratezza, comprese quelle di natura psicologica o sistemica; (iii) la salvaguardia della salute psicofisica del minore, tutelata dall'articolo 24 della CRC, che impone agli Stati di garantire accesso alle cure e alle condizioni che favoriscono uno sviluppo sano (Comitato sui Diritti dell'Infanzia 2013, pp. 28 e ss.).

Il principio del superiore interesse del minore, per la sua natura dinamica, richiede poi di essere riletto alla luce delle trasformazioni imposte dalla rivoluzione digitale (Comitato sui Diritti dell'Infanzia 2021).

Le tecnologie digitali che i minori utilizzano, pur non essendo state originariamente progettate per loro, occupano un ruolo centrale nella vita quotidiana, influenzandone esperienze, relazioni e processi di sviluppo.

In questo ambiente fattosi digitale, occorre interrogarsi su diritti e libertà perché, come è stato approfondito nel precedente paragrafo 4, le tecnologie digitali hanno acquisito il potere di condizionare le vite, le scelte, financo l'esercizio dei diritti (civili, politici, culturali, economici, sociali, etc.), in modo ampio, interdipendente, paradossalmente anche in assenza di internet.

In questo scenario si colloca il Commento Generale n. 25 del 2021 del Comitato sui Diritti dell'Infanzia, che adatta i principi della CRC all'ambiente digitale individuandone quattro come centrali (Comitato sui Diritti dell'Infanzia 2021, pp. 7 e ss.).

Il primo è il principio di non discriminazione, che impone agli Stati di garantire un accesso equo e inclusivo, contrastando il divario digitale e le distorsioni derivanti da profilazioni automatizzate o dati incompleti.

Il secondo è il principio del superiore interesse del minore, che, come già visto, deve orientare ogni decisione pubblica o privata con effetti diretti o indiretti sulla vita del bambino.

Il terzo principio riguarda il diritto alla vita, alla sopravvivenza e allo sviluppo. Esso impone la protezione da contenuti dannosi, dinamiche opache e sfruttamento commerciale.

Infine, il terzo principio si volge alla tutela del diritto del minore a esprimere liberamente la propria opinione includendo anche le forme di partecipazione digitale, a condizione che non si traducano in strumenti di sorveglianza o raccolta indebita di dati.

Il Comitato raccomanda agli Stati di aggiornare le normative per garantire che i diritti dell'infanzia siano pienamente rispettati anche nell'ambiente digitale.

A tal fine, indica altresì la necessità di adottare strumenti di valutazione preventiva – come la CRIA – già nella fase di ideazione di normative e politiche pubbliche, secondo un approccio *by design*. È particolarmente interessante anche l'attenzione prestata agli operatori privati che, attraverso i propri servizi, incidono in modo sostanziale sull'esperienza *online* dei bambini (Comitato sui Diritti dell'Infanzia 2021, pp. 19 e ss.)[6].

Se, da una parte, gli Stati, in quanto parti della Convenzione, hanno il dovere di garantire che le imprese rispettino tali diritti, anche attraverso misure che impediscano l'uso improprio dei servizi digitali o la loro implicazione, diretta o indiretta, in pratiche lesive, come la violazione della riservatezza, la raccolta abusiva di dati personali o la manipolazione delle scelte comportamentali dei minori. Nondimeno, dall'altra parte, le imprese sono chiamate a svolgere attività di *due diligence* orientate ai diritti dell'infanzia e a rendere pubblici i risultati delle valutazioni d'impatto, promuovendo trasparenza e *accountability*. Ciò implica una revisione dei modelli operativi, dei criteri progettuali e delle strategie di mercato, affinché siano ispirati ai più elevati *standard* di protezione della *privacy*, della sicurezza e dell'autonomia del minore (Comitato sui Diritti dell'Infanzia 2021, p. 21).

La stessa infrastruttura su cui poggia l'ambiente digitale pone dei problemi. Essa, infatti, non si configura semplicemente come un dominio tecnico o strumentale, bensì come uno spazio intrinsecamente normativo, regolato da chi detiene il controllo sulle infrastrutture tecnologiche. È all'interno di questa cornice che si colloca la nota affermazione di Lawrence Lessig, secondo cui *code is law*. Il codice, inteso non solo come linguaggio di programmazione ma come architettura normativa, non è lo sfondo neutro dell'esperienza *online*, ma determina ciò che è possibile, vietato o tacitamente incoraggiato (Maestri 2017; Lessig 1999).

6 Interessante la considerazione che anche le imprese, e in primo luogo l'industria tecnologica, dovrebbero essere adeguatamente formate sui potenziali impatti che i propri prodotti e servizi possono avere sui diritti dei minori in diversi ambiti: educativo, relazionale, sanitario, identitario. Oltre alla conoscenza specifica del contesto digitale, viene ritenuta essenziale una formazione orientata all'applicazione concreta degli *standard* internazionali sui diritti umani e dell'infanzia, così da assicurare che la progettazione e la gestione delle tecnologie non solo evitino di arrecare danno, ma contribuiscano positivamente alla promozione del benessere dei più giovani (Comitato sui Diritti dell'Infanzia 2021, p. 19).

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

Su questo aspetto, sebbene centrale, mi limiterò a un rapido accenno, in quanto già ampiamente affrontato nel contributo di Maestri incluso nel presente Dossier.

Se si accetta l'idea che scrivere codice significa esercitare un potere normativo, allora risulta evidente che i progettisti e gli sviluppatori digitali svolgono un ruolo cruciale. Attraverso l'architettura delle piattaforme – che definisce le impostazioni di *default*, i percorsi consentiti, i limiti dell'accesso – prende forma l'ambiente in cui si svolge l'esperienza.

In questa prospettiva, il predominio di logiche economiche nello spazio digitale implica che il codice venga progettato e ottimizzato in funzione di obiettivi commerciali. A guidare le scelte non è il benessere ma la massimizzazione dell'*engagement*. E così anche i criteri di valutazione algoritmica, *rating* di affidabilità e filtri reputazionali, tendono ad imporre modelli di condotta e a orientare le dinamiche sociali.

Inserire l'interesse prioritario del minore in questo contesto significa, allora, rovesciare l'asimmetria: giuridificare il codice e tecnicizzare il diritto. Vuol dire pretendere che i sistemi di raccomandazione integrino parametri di sicurezza psicosociale, che gli *audit* algoritmici valutino non solo *bias* statistici ma effetti educativi, che la *data minimisation* diventi configurazione predefinita (di *default*) su ogni *device* destinato ai bambini. Ma implica anche riconoscere la dimensione collettiva del rischio; se gli impatti sono sociali, le soluzioni devono esserlo altrettanto, passando da negoziati privati (l'informativa, il consenso) a garanzie strutturali *ex ante*, e quindi architetture di piattaforma che mettano il bambino prima del profitto.

In questa direzione si colloca il rapporto *The best interests of the child in the digital environment*, curato dalla 5Rights Foundation e dalla London School of Economics and Political Science. Secondo gli autori, il superiore interesse del minore non si sostituisce ai diritti previsti dalla CRC, ma si realizza attraverso la loro attuazione integrale. Non può essere ridotto a un criterio flessibile né utilizzato per giustificare compromessi dettati da logiche di mercato (Livingstone *et al.* 2024).

Un esempio significativo è l'*Age Appropriate Design Code* (AADC) introdotto nel Regno Unito, che stabilisce la prevalenza del *best interest* del minore sugli interessi commerciali. In caso di conflitto tra profitto e protezione, la priorità spetta senza ambiguità al secondo. Alcune aziende hanno adottato misure coerenti con questa direzione come i *Trust, Transparency & Control (TTC) Labs* di Meta che hanno sviluppato impostazioni predefinite sulla *privacy* o la funzione "fai una pausa". Tuttavia non pare che Meta abbia, invece, affrontato questioni importanti come la monetizzazione dei dati dei minori o la sostenibilità dei modelli economici basati sul coinvolgimento compulsivo (Livingstone *et al.* 2024, p. 8 e p. 12).

Ne sono una conferma le recenti azioni legali promosse da 42 procuratori generali contro Meta per le pratiche ritenute lesive nei confronti degli ado-

lescenti[7]. Documenti interni pubblicati dal *Wall Street Journal* hanno mostrato l'intenzione dell'azienda di sviluppare prodotti espressamente pensati per i preadolescenti, descritti come «un pubblico prezioso ma ancora non pienamente sfruttato»[8].

In presenza di dinamiche potenzialmente lesive – come la manipolazione commerciale o l'esposizione a contenuti dannosi – la valutazione del superiore interesse del minore deve orientarsi verso una protezione rafforzata. In tali casi, la tutela della *privacy* e della salute richiede misure integrate nel *design* e non può essere demandata al solo consenso o al controllo familiare.

4. Oltre il modello consensuale: *Rights by Design*

L'architettura europea della normativa sulla protezione dei dati personali si fonda sull'idea che l'utente, adeguatamente informato, sia in grado di valutare benefici e rischi dello scambio informativo e di esprimere un consenso libero, specifico, informato e consapevole. In questo modello, il trattamento si legittima attraverso l'autonomia del soggetto, intesa come capacità di autodeterminarsi (Solove 2013).

Tuttavia, l'ingresso nell'ambiente digitale avviene spesso in condizioni strutturalmente sfavorevoli, segnato dall'azione combinata di tre fattori: limiti cognitivi, carenze di competenze e scelte di *design* orientate a finalità estranee all'interesse dell'utente.

Sui primi limiti, l'economia comportamentale ha messo in luce come numerosi *bias* compromettano la razionalità delle scelte, soprattutto quando implicano effetti futuri difficilmente prevedibili (Vella 2023; Acquisti, Grossklags 2008, 2005; Kahneman, Tversky 1982, 1973).

Sulla carenza di competenze, è evidente che comprendere i meccanismi di profilazione, le logiche del *targeting* o il funzionamento degli algoritmi richiede competenze tecniche che la maggior parte degli utenti non possiede[9].

Infine, l'interfaccia delle piattaforme, il loro *design*, non è neutra nella misura in cui viene progettata per massimizzare l'interazione e la raccolta di dati, anche mediante tecniche di manipolazione del comportamento (Heyndels 2023; Zaccaria 2022, p. 81; Galimberti 2018, p. 229; Sunstein, Thaler 2009; Sunstein 2022, 2019; Cominelli 2018).

---

7 Per un approfondimento si veda https://www.washingtonpost.com/technology/2023/10/24/meta-lawsuit-facebook-instagram-children-mental-health/ (consultato il 2 giugno 2025).

8 Sulla vicenda si veda https://www.wsj.com/tech/facebook-instagram-kids-tweens-attract-11632849667?mod=article_inline (ultimo accesso: 2 giugno 2025).

9 Per un approfondimento sulle competenze informatiche si veda l'Indice di digitalizzazione dell'economia e della società (DESI), in https://digital-strategy.ec.europa.eu/it/policies/desi (consultato il 30 maggio 2025).

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

A questi fattori si aggiungono gli ostacoli connessi alla comprensione delle informative. I testi prodotti per adempiere all'obbligo di trasparenza risultano spesso lunghi, complessi e inaccessibili. Il consenso, pur formalmente espresso, si basa su un'informazione che non è, nella sostanza, fruibile. Inoltre, si tratta di un consenso individuale, mentre molti effetti del trattamento (*bias* algoritmici, manipolazione informativa, profilazioni di gruppo) investono la collettività.

A questo si aggiunga che, una volta elaborati i dati, le inferenze prodotte restano attive anche se il consenso viene revocato. In molti casi, poi, il consenso si dà non perché si condivide la finalità, ma perché l'alternativa è l'esclusione da servizi essenziali – dall'istruzione all'assistenza pubblica – sempre più mediati dal digitale.

Il risultato è una forte asimmetria, in cui il dato diventa merce di scambio, e il potere regolativo si trasferisce dagli ordinamenti ai *terms of service*, dalla norma giuridica al codice informatico. In questa logica, il consenso rischia di ridursi, per riprendere le parole di Rodotà (1997, p. 150), alla «risultante di un insieme di condizionamenti».

Affermare la necessità di superare il modello consensuale non significa escludere il consenso, ma ridefinirne la funzione.

La manifestazione di volontà non può più essere l'unico fondamento della legittimità, ma deve essere inserita in una filiera di responsabilità preventiva, che intervenga a monte, nel momento della progettazione. Il centro della tutela non può essere il *click* su "accetto", ma il *design* stesso delle piattaforme, il modo in cui si organizzano i flussi di dati, si configurano le scelte, si determinano le condizioni dell'esperienza digitale.

Rimettere al centro l'autonomia significa allora intervenire sulle infrastrutture, richiedere *standard* tecnici obbligatori, *audit* indipendenti, strumenti di controllo accessibili. La tutela non può limitarsi alla prescrizione astratta di princìpi come la *privacy by design*, ma deve includere la possibilità concreta di verificarne l'attuazione, valutarne i rischi e correggerne gli effetti.

È qui che entra in gioco l'*Impact Assessment*, procedura di valutazione preventiva che traduce princìpi astratti (come *data minimisation*, non discriminazione, trasparenza) in parametri verificati e verificabili, soglie di rischio, piani di mitigazione e obblighi di documentazione.

Nei prossimi paragrafi ne saranno approfonditi alcuni aspetti, per mostrarne la funzione di cerniera operativa tra la progettazione responsabile delle piattaforme e la garanzia effettiva dei diritti nell'ambiente digitale.

5. L'*Impact Assessment*

La valutazione d'impatto o *Impact Assessment*, rappresenta uno strumento analitico e decisionale volto a esaminare, in fase preventiva e lungo il ciclo di

vita di un intervento tecnico, normativo o organizzativo, i possibili effetti su persone, diritti, beni e valori fondamentali (Lud 2020; Bisztray e Gruschka 2019).

Non si tratta di un mero adempimento formale, bensì di un processo orientato alla responsabilità, finalizzato a guidare le scelte in una fase in cui è ancora possibile riorientare o, se del caso, rinunciare all'intervento stesso.

L'*International Association for Impact Assessment* (IAIA) ne offre una definizione efficace qualificandolo come un procedimento volto a valutare le implicazioni delle azioni proposte per le persone e l'ambiente, mentre è ancora possibile modificarle o, se necessario, abbandonarle (Baroni 2024, p. 108).

Nel contesto della regolazione tecnologica, e in particolare con riferimento ai sistemi basati su algoritmi e intelligenza artificiale, si avverte con urgenza l'esigenza di adottare valutazioni d'impatto capaci di integrare dimensioni giuridiche, etiche e sociali fin dalla fase di progettazione.

L'*Impact Assessment* assume così una funzione chiave nella *governance* delle tecnologie emergenti, promuovendo un approccio responsabile orientato alla prevenzione dei rischi e alla tutela sostanziale dei diritti, andando oltre la logica delle *checklist* tecniche e richiedendo piuttosto una vera e propria presa in carico dell'impatto socio-giuridico delle tecnologie fin dalla loro fase di concezione (OECD 2024).

Si tratta di un processo ciclico, iterativo e trasparente, solitamente organizzato in fasi che schematicamente, e puramente e titolo esemplificativo, si potrebbero individuare in: (i) definizione del contesto e degli obiettivi; (ii) mappatura dei soggetti impattati; (iii) individuazione dei potenziali impatti; (iv) valutazione dei rischi in termini di gravità e probabilità; (v) predisposizione delle misure di mitigazione o compensazione; (vi) consultazione e partecipazione degli *stakeholders*; (vii) documentazione e motivazione delle decisioni assunte; (viii) monitoraggio continuo ed eventuale revisione.

Sebbene la sequenza possa variare in base allo strumento adottato (DPIA, FRIA, HRIA, CRIA, ecc.), resta invariata la logica di fondo, improntata alla responsabilizzazione e alla tracciabilità delle scelte.

Nel quadro della regolazione europea in materia di diritti fondamentali e nuove tecnologie, il Regolamento Generale sulla Protezione dei Dati (GDPR) ha introdotto, all'articolo 35, la valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*, o DPIA) quale strumento di prevenzione e responsabilizzazione. La DPIA è prescritta nei casi in cui il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone fisiche. Essa si fonda su un'analisi sistematica delle operazioni di trattamento e impone un bilanciamento tra esigenze tecnologiche e protezione della sfera personale, alla luce dei principi di necessità, proporzionalità e minimizzazione.

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

Il Garante italiano per la protezione dei dati personali ha fornito indicazioni operative e un elenco dei trattamenti per i quali la DPIA è obbligatoria[10].

La *Commission Nationale de l'Informatique et des Libertés* francese (CNIL) ha sviluppato linee guida e un *software* gratuito per accompagnare i titolari del trattamento lungo il percorso valutativo[11]. Questo strumento rappresenta un esempio di come l'approccio valutativo possa essere reso accessibile e operativo anche in ambiti complessi.

In linea con il principio della prevenzione, anche il già richiamato *AI Act* prevede, all'articolo 27, l'obbligo di effettuare una valutazione d'impatto sui diritti fondamentali (*Fundamental Rights Impact Assessment*, o FRIA) per i sistemi di intelligenza artificiale classificati ad alto rischio, ossia quelle soluzioni tecnologiche che possono incidere in modo significativo su aspetti centrali della vita delle persone, in ragione della loro funzione, finalità o contesto d'uso (Cosentini *et al.* 2025; Mantelero e Esposito 2021).

La FRIA esige dai soggetti che immettono sistemi ad alto rischio sul mercato (cosiddetti *deployer*), una riflessione approfondita sugli impatti potenziali in termini di non discriminazione, libertà di espressione, protezione dei dati personali, partecipazione democratica e altre libertà fondamentali. Non solo devono essere individuati e analizzati i rischi, ma è richiesta l'adozione di misure di mitigazione adeguate. Un elemento distintivo della FRIA è inoltre la previsione della consultazione degli *stakeholders* potenzialmente coinvolti o impattati, trasformando così la valutazione in uno spazio di confronto aperto tra le parti interessate.

Anche il *Digital Services Act* (noto come DSA)[12] interviene in questa direzione, istituendo una procedura di valutazione del rischio sistemico a carico delle grandi piattaforme *online*: le *Very Large Online Platforms* (Piattaforme *online* di dimensioni molto grandi) e dei *Very Large Online Search Engines* (motori di ricerca di dimensioni molto grandi). Nel Capo III, dedicato agli *Obblighi in materia di dovere di diligenza, per un ambiente* online *trasparente e sicuro*, all'articolo 34 si dispone l'obbligo della valutazione dei rischi sistemici derivanti dalla progettazione o dal funzionamento dei servizi e dei relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei servizi medesimi, per i diritti fondamentali, il dibattito democratico, la coesione sociale, la dignità umana, la protezione della salute pubblica e dei minori, il benessere fisico e mentale della persona.

10 Per maggiori dettagli si veda https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia- (consultato il 2 giugno 2025).

11 Si rinvia per un approfondimento a https://www.cnil.fr/en/privacy-impact-assessment-pia (consultato il 30 maggio 2025).

12 Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE.

Il DSA attribuisce, in tal modo, rilievo normativo alla capacità delle infrastrutture digitali di incidere sulle dinamiche sociali e democratiche, riconoscendo che la progettazione e il funzionamento delle piattaforme non sono neutri.

Il DSA prevede, inoltre, l'adozione di misure di mitigazione che devono andare ad agire sulle cause, intervenendo su logiche di raccomandazione, architetture informative, *design* delle interfacce, politiche di moderazione.

L'art. 37 prevede, infine, *audit* indipendenti con cadenza annuale, e l'accesso dei ricercatori ai dati delle piattaforme contribuendo così a fondare le valutazioni su evidenze empiriche.

In questa prospettiva, il DSA comincia a delineare una nuova responsabilità d'impresa rispetto allo sviluppo e all'impiego di algoritmi, fondata sulla consapevolezza delle conseguenze delle scelte tecniche.

In tal modo, la valutazione dell'impatto si configura non solo come strumento di conformità, ma anche come spazio di interazione tra discipline – giuridiche, tecniche, sociali – e tra attori istituzionali, accademici e civili.

Il DSA rappresenta, sotto questo profilo, un passo rilevante verso una *governance* del digitale fondata su trasparenza, responsabilità e tutela dei diritti, e l'*Impact Assessment* si delinea come strumento per tradurre principi etici in pratiche verificabili.

D'altra parte, come si è già avuto modo di anticipare, quando l'utente è un soggetto in età evolutiva, gli *standard* valutativi ordinari si rivelano insufficienti poiché non tengono conto in modo adeguato di dimensioni come la vulnerabilità, la capacità di agire, il diritto alla partecipazione e altri elementi caratteristici dell'infanzia.

È in questo spazio che si colloca la CRIA. Nel paragrafo successivo verranno svolte alcune prime considerazioni introduttive sul modello, mettendo in luce il suo contributo essenziale alla costruzione di un ecosistema tecnologico più equo e centrato sulla persona.

6. Prime note sulla CRIA

6.1. Struttura multilivello

La CRC ha segnato un passaggio fondamentale nella rappresentazione del bambino, da soggetto passivo da proteggere a titolare di diritti pienamente esigibili, in forza della sua dignità intrinseca. L'infanzia viene così riconosciuta non solo come una fase transitoria, ma come un momento unico e autonomo dello sviluppo umano, cui si applica l'intero spettro dei diritti umani secondo la logica del *best interest*.

In parallelo, la crescente capacità delle imprese, tramite i servizi digitali, di influenzare – direttamente o indirettamente – le condizioni materiali e

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

simboliche dell'esperienza infantile ha reso necessario un ampliamento del quadro di responsabilità oltre la dimensione statale.

In questo contesto si collocano i Principi Guida delle Nazioni Unite su Imprese e Diritti Umani (UNGPs), adottati all'unanimità dal Consiglio per i Diritti Umani nel 2011, che hanno consolidato il consenso internazionale sull'obbligo delle imprese di rispettare i diritti umani, inclusi quelli dei bambini[13].

L'approccio trifasico *Protect, Respect and Remedy* (proteggere, rispettare, rimediare) offre una struttura operativa concreta ove agli Stati spetta il compito di prevenire le violazioni da parte di attori privati; le imprese devono rispettare i diritti umani a prescindere dagli obblighi normativi nazionali; infine, entrambi i soggetti sono chiamati a garantire accesso a rimedi efficaci in caso di violazione.

Il Principio 17 degli UNGPs introduce la *due diligence* in materia di diritti umani (detta HRDD), quale processo strutturato e continuo per identificare, prevenire e mitigare impatti negativi, effettivi e potenziali, sulle persone, con un coinvolgimento effettivo degli *stakeholder14*.

Con l'introduzione, a livello europeo, della Direttiva sulla *due diligence* delle imprese in materia di sostenibilità (*Corporate Sustainability Due Diligence Directive* o CSDDD), la HRDD si avvia ora a diventare un obbligo giuridico, non più solo etico, per molte imprese operanti nel mercato dell'Unione[15].

D'altra parte, affinché la *due diligence* sia realmente efficace, occorrono strumenti metodologici adeguati. Tra questi, la *Human Rights Impact Assessment* (o HRIA) si configura come una tecnica di analisi partecipativa e contestuale, finalizzata a esaminare in anticipo gli effetti di un progetto o di una decisione aziendale rispetto ai diritti umani. Essa fa parte del processo

13 Per maggiori dettagli si veda https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (consultato il 2 giugno 2025). È disponibile una traduzione italiana a cura di Fasciglione in https://www.cnr.it/sites/default/files/public/media/attivita/editoria/Fasciglione_Principi_Guida_ONU_imprese_diritti_umani.pdf (consultato il 2 giugno 2025). Molto interessante è anche il *Business and Human Right Navigator* disponibile all'indirizzo https://www.globalcompactnetwork.org/it/il-global-compact-ita/strumenti-e-campagne/business-human-rights-navigator.html (consultato il 2 giugno 2025).

14 Il principio 17, più nello specifico, dispone: «In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed […]».

15 Direttiva (UE) 2024/1760 del Parlamento europeo e del Consiglio, del 13 giugno 2024, relativa al dovere di diligenza delle imprese ai fini della sostenibilità e che modifica la direttiva (UE) 2019/1937 e il regolamento (UE) 2023/2859.

di HRDD, in particolare della fase iniziale di identificazione e valutazione degli impatti.

Il Principio 12 degli UNGPs richiama poi l'attenzione su soggetti in condizioni di vulnerabilità, tra cui i bambini, che per caratteristiche evolutive ed esposizione al rischio richiedono tutele rafforzate.

Tuttavia, i UNGPs non forniscono indicazioni metodologiche specifiche su come incorporare i diritti dell'infanzia nelle politiche aziendali.

A colmare tale lacuna intervengono i *Children's Rights and Business Principles* (CRBPs), elaborati nel 2012 da UNICEF, Save the Children e il Global Compact delle Nazioni Unite[16].

I CRBPs offrono un quadro operativo finalizzato a promuovere l'integrazione sistematica dei diritti dei bambini in tutte le aree dell'attività aziendale: dalla *governance* interna alla gestione del personale, dalla filiera produttiva alla strategia di comunicazione e *marketing*.

Il loro contributo innovativo consiste nell'aver riconosciuto i bambini non solo come soggetti vulnerabili da proteggere, ma come titolari di diritti specifici e attori sociali portatori di interessi, bisogni e aspettative propri.

I CRBPs traducono i UNGPs in una prospettiva centrata sull'infanzia e forniscono la base metodologica per la CRIA, declinazione specifica della HRIA. In tal modo, si delinea una struttura multilivello che va dalla fonte primaria (CRC), ai principi guida (UNGPs e CRBPs), fino agli strumenti procedurali (HRDD, HRIA, CRIA), garantendo coerenza tra fondamento normativo, orientamento etico e attuazione pratica.

6.2. Verso uno strumento per la CRIA

In ambito tecnologico, come è stato illustrato, si assiste alla diffusione di strumenti valutativi basati sul rischio e all'introduzione di meccanismi di *impact assessment* anche nei più recenti interventi normativi.

Tuttavia, se si considera il settore delle *IT Company*, la loro implementazione resta parziale, anche a causa della difficoltà di tradurre i principi della CRC in azioni operative, soprattutto in un contesto tecnologico in rapido mutamento.

Le imprese mostrano, poi, una certa riluttanza a rendere pubblici i risultati delle valutazioni per timore di ricadute legali e reputazionali.

Inoltre, le linee guida disponibili su come condurre una CRIA restano ad oggi frammentarie, con indicazioni generiche che non sempre si adattano alle sfide specifiche dell'ambiente digitale (UNICEF 2024, p. 4).

16 Per il documento integrale di veda https://www.unicef.org/documents/childrens-rights-and-business-principles (consultato il 2 giugno 2025).

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

Si consideri, poi, che le più recenti classificazioni OECD (2021) segnalano l'emergere di nuovi rischi legati a tecnologie come l'intelligenza artificiale generativa, i sistemi biometrici, l'analisi predittiva in ambito educativo e la *sentiment analysis* nel settore sanitario, in grado di produrre implicazioni ancora più significative per l'infanzia.

In questo scenario si sono avviate alcune iniziative che hanno l'obiettivo di definire un quadro metodologico per la CRIA. Fra queste ci si soffermerà su alcune che paiono più significative.

Tra le risorse esistenti, una delle prime guide strutturate è il documento realizzato da UNICEF e dall'Istituto Danese per i Diritti Umani nel 2020, che offre un sistema di 58 criteri ispirati ai 10 principi guida dei *Children's Rights and Business Principles*. Tali criteri sono articolati in forma di domande guida e corredati da suggerimenti operativi. Un limite del documento è che, essendo stato redatto oltre un decennio fa, non incorpora i rischi emergenti connessi all'attuale evoluzione del digitale (BSR 2024, p. 25)[17].

Uno strumento utile ma più settoriale è rappresentato dal *Child Rights Impact Self-Assessment Tool for Mobile Operators* (o MO-CRIA), sviluppato da UNICEF nel 2014 e aggiornato nel 2021. È stato pensato per gli operatori di telefonia mobile e si compone di una presentazione, uno strumento di autovalutazione e una guida metodologica con casi studio. L'autovalutazione si basa su sette aree di analisi, associate a dipartimenti aziendali specifici, e prevede risposte a quesiti (sì/no) corredate da evidenze documentali. Il risultato finale è una visualizzazione grafica delle criticità, utile per mappare rischi e aree di miglioramento (BSR 2024, pp. 22 e 23).

Nel 2023 CEN-CENELEC ha pubblicato un *Workshop Agreement* (CWA) su *Age Appropriate Digital Services Framework18* che si basa sulla *standard* IEEE 2089-2021[19]. Si tratta di indicazioni per la progettazione in base all'età, tenendo conto dei principi e dei diritti sanciti dalla CRC.

Nel 2024, UNICEF ha avviato un'iniziativa per sviluppare un *toolkit* per il *Child Rights Impact Assessment*, con l'obiettivo di promuoverne l'adozione e facilitarne l'implementazione (UNICEF 2024).

In collaborazione con l'organizzazione *no-profit Business for Social Responsibility* (BSR), è stato pubblicato nel 2024 il *report Child Rights Impact Assessments in Relation to the Digital Environment*, che offre una pa-

17 Per ulteriori dettagli sulla ricerca danese si veda https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox (consultato il 30 maggio 2025). Sul punto si veda anche il già richiamato documento dell'OECD *Children in the Digital Environment: Revised Typology of Risks* del 2021 che fornisce indicazioni sui diversi tipi di rischi *online* per i bambini, offrendo una base utile per orientare le valutazioni d'impatto sui diritti dell'infanzia. Per un approfondimento Livingstone e Stoilova (2021).

18 In https://www.cencenelec.eu/news-and-events/news/2023/workshop/2023-03-06-age-appropriate-digital-service-framework/ (consultato il 2 giugno 2025).

19 Si veda https://standards.ieee.org/ieee/2089/7633/ (consultato il 4 giugno 2025).

noramica delle pratiche attuali nel settore industriale, evidenziandone limiti e risorse disponibili (BSR 2024). Il documento sottolinea la necessità di strumenti operativi specifici per condurre valutazioni d'impatto centrate sui diritti dell'infanzia nel contesto digitale. A tal fine, BSR ha coinvolto alcuni *stakeholders* attraverso interviste e tavole rotonde, analizzando otto CRIA – quattro condotte da enti pubblici e quattro da soggetti privati – relative a servizi e prodotti tecnologici, valutandone punti di forza e debolezze. BSR ha, inoltre, contribuito alla predisposizione di diverse HRIA su aziende tecnologiche ancorché solo una sia stata poi pubblicata[20].

In sintesi, allo stato, non c'è una metodologia definitiva per la CRIA.

Tuttavia, il Comitato sui Diritti dell'Infanzia (2013) ha affermato che tutte le CRIA dovrebbero (i) utilizzare la CRC e i suoi protocolli come quadro di riferimento; (ii) considerare gli impatti differenti che i bambini subiscono rispetto agli adulti; (iii) basarsi sul contributo di bambini, società civile, esperti del settore, agenzie governative competenti, ricerche accademiche e tutti i dati disponibili; (iv) impostare azioni adeguate per fronteggiare i rischi; (v) rendere pubblici i risultati (BSR 2024, pp. 27-28).

Inoltre, pur, con alcune variazioni, i processi di CRIA includono quasi sempre i seguenti passaggi: (1) Definizione dell'ambito oggetto della valutazione (es. *policy*, prodotto, funzionalità, programma); (2) Raccolta dei dati (es. dimensione della popolazione interessata, incidenza del problema); (3) Coinvolgimento degli *stakeholders* (bambini, esperti interni ed esterni, società civile e altri *stakeholders* rilevanti, secondo opportunità); (4) Valutazione degli impatti, mediante analisi dei rischi e delle opportunità (utilizzando CRC e i CRBPs); (5) Individuazione delle azioni appropriate, ossia stabilire come evitare, prevenire, mitigare e rimediare agli impatti negativi attuali e potenziali; (6) Comunicazione dei risultati pubblicamente o agli *stakeholders* pertinenti; (7) *Due diligence* continua, , monitoraggio dei progressi e aggiornamento in base al mutare delle circostanze (BSR 2024, p. 28).

7. Conclusione

Nel corso di questo contributo si è cercato di far emergere la necessità di un ripensamento profondo del rapporto tra innovazione tecnologica e diritti dell'infanzia.

Se da un lato le tecnologie digitali accompagnano ormai ogni fase dello sviluppo umano, fin dalla prima infanzia, dall'altro emerge con chiarezza

20 Per un esempio di HRIA si veda quella svolta per Tech Coalition, disponibile in https://www.bsr.org/reports/BSR-Tech-Coalition-HRIA-Report.pdf (consultato il 30 maggio 2025).

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

come bambini e adolescenti si trovino ad abitare ambienti digitali progettati senza un'adeguata considerazione delle loro esigenze, fragilità e prerogative giuridiche.

L'ambiente digitale, come abbiamo visto, non è uno spazio neutro, ma il risultato di scelte progettuali, logiche economiche e assetti normativi che incidono concretamente sulla possibilità per i minori di crescere in modo libero, sicuro e consapevole.

In tale prospettiva, il principio del superiore interesse del minore, pur formalmente riconosciuto a livello internazionale, rischia di restare inapplicato se non viene tradotto in strumenti operativi capaci di incidere sulle fasi di ideazione, progettazione, sviluppo e monitoraggio delle tecnologie.

La CRIA si propone come uno di questi strumenti. La sua adozione sistemica – analogamente a quanto avvenuto con la DPIA e la FRIA – rappresenta una risposta concreta alla crescente esigenza di responsabilità progettuale e giustizia digitale.

In attesa che si consolidi uno *standard* condiviso – tenuto conto, fra gli altri, delle linee guida offerte da UNICEF (2024), BSR (2024), i principi CRBPs e UNGPs, è possibile delineare una struttura metodologica preliminare per la CRIA, articolata in quattro blocchi:

(a) Contesto e scopo della valutazione: descrizione del prodotto, servizio o *policy* analizzati; identificazione dell'età potenziale dei minori coinvolti; obiettivi della CRIA;

(b) Analisi multidimensionale dell'impatto: valutazione qualitativa e quantitativa dei rischi e delle opportunità su diversi assi, per esempio: privacy e dati personali; salute psicofisica; libertà di espressione; sviluppo educativo; partecipazione e *agency*. A ogni impatto si associano indicatori misurabili e soglie di rischio;

(c) Partecipazione e consultazione: coinvolgimento strutturato di bambini, educatori, famiglie ed esperti (es. tramite focus group, sondaggi, laboratori di *co-design*) nella fase di valutazione e revisione;

(d) Azioni, documentazione e revisione: definizione delle misure di mitigazione; assegnazione delle responsabilità; pubblicazione sintetica degli esiti della CRIA; revisione periodica sulla base dell'evoluzione tecnologica o normativa.

Questo primo esercizio di schematizzazione iniziale potrebbe essere utile come base pratica iniziale per tradurre i principi della CRC in processi valutativi operativi, iterabili e verificabili. Costituisce, inoltre, un possibile punto di partenza per future ricerche empiriche o comparative finalizzate alla validazione degli indicatori, alla definizione di soglie comuni di rischio e alla messa a punto di *toolkit* settoriali.

La CRIA non è solo una metodologia valutativa, è anche un'occasione per ripensare la *governance* dell'innovazione, per restituire centralità a chi troppo

spesso resta invisibile nei processi decisionali, e per costruire un ecosistema digitale più equo, trasparente e umano.

Perché la CRIA possa davvero entrare a far parte delle prassi istituzionali e aziendali, occorre procedere lungo più direttrici: la definizione di linee guida condivise; la formazione interdisciplinare di progettisti, giuristi e *policy maker*; l'assunzione di un impegno collettivo – da parte delle istituzioni, del settore privato e della società civile – a riconoscere i bambini non come semplici utenti, ma come soggetti di diritto.

Bibliografia

Acquisti, A., Grossklags, J., (2005), Privacy and rationality in decision making, *IEEE Security & Privacy*, 3, 1, pp. 24-30.

Acquisti, A., Grossklags, J., (2008), What Can Behavioral Economics Teach Us About Privacy?, in A. Acquisti, S. Gritzalis, C. Lambrinoudakis e S. De Capitani di Vimercati, a cura di, *Digital Privacy*, New York, Auerbach Publications, pp. 363-369.

Barassi, V., (2021), *I figli dell'algoritmo. Sorvegliati, tracciati, profilati dalla nascita*, Roma, Luiss University Press.

Baroni, M., (2024), Fundamental Rights Impact Assessment, in AIRIA, a cura di, *Navigare l'European AI Act*, Milano, Wolters Kluwer.

Beerwinkle, A.L., (2021), The use of learning analytics and the potential risk of harm for K-12 students participating in digital learning environments, *Education Tech Research Dev*, 69, pp. 327-330.

Berlingò, V., (2017), Il fenomeno della datafication e la sua giuridicizzazione, *Rivista trimestrale di diritto pubblico*, 3, pp. 641-675.

Bisztray, T., Gruschka, N., (2019), Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality, in Askarov, A., Hansen, R., Rafnsson, W., a cura di, *Secure IT Systems. NordSec 2019. Lecture Notes in Computer Science*, 11875, Cham, Springer.

Breen, C., (2002), *The standard of the best interests of the child: a western tradition in international and comparative law*, Dordrecht, Kluwer.

Business for Social Responsibility (BSR), (2024), *Child Rights Impact Assessments in Relation to the Digital Environment*, in https://www.bsr.org/reports/BSR_UNICEF_D6.pdf (consultato il 2 giugno 2025).

Cominelli, L., (2018), Framing Choices to Influence Behaviors: A Debate on the Pros and Cons of "Nudging", *Diritto & Questioni pubbliche*, XVIII, 1, pp. 293-306.

Comitato sui Diritti dell'Infanzia, (2013), Commento generale n. 14 del 2013, Sul diritto del minorenne a che il proprio superiore interesse sia tenuto in primaria considerazione, in https://www.unicef.it/pubblicazioni/il-superiore-interesse-del-minorenne (consultato il 28 maggio 2025).

Comitato sui Diritti dell'Infanzia, (2021), Commento generale n. 25 del 2021, Sui diritti dei minorenni in relazione all'ambiente digitale, in https://www.unicef.it/pubblicazioni/i-diritti-dei-minorenni-in-relazione-all-ambiente-digitale (consultato il 30 maggio 2025).

Cosentini, A., Pollicino, O., De Gregorio, G., Ermellino, A., Fontanella, D., Inverardi, N., Paolucci, F., Penco, I.G., Regoli, D., Tessaro Trapani, S., (2025), Assessing the Impact of Artificial Intelligence Systems on Fundamental Rights, *Media LAWS*, https://www.medialaws.eu/assessing-the-impact-of-artificial-intelligence-systems-on-fundamental-rights/ (consultato il 2 giugno 2025).

Floridi, L., (2020), *Il verde e il blu*, Milano, Raffaello Cortina Editore.

Galimberti, U., (2018), *I miti del nostro tempo*, Milano, Feltrinelli.

Garapon, A., Lassègue, J., (2021), *La giustizia digitale. Determinismo tecnologico e libertà*, traduzione italiana di F. Morini, Bologna, il Mulino.

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

Heyndels, S., (2023), Technology and Neutrality, *Philosophy & Technology*, 36, 4, 75, pp. 1-22.

Hirsch, M., Binder, A., Matthes, J., (2025), A "drop in the ocean"? Emerging adults' experiences and understanding of targeted political advertising on social media, *New Media & Society*, in https://journals.sagepub.com/doi/epub/10.1177/14614448241306455 (consultato il 30 settembre 2025).

Hof, S. van der, Challis, L., Wanroij, E. van, Schermer, B.W., (2024), *Child rights impact assessment: impact and legal analysis for the development of the CRIA*, The Hague, Ministry for Internal Affairs and Kingdom Relations, in https://hdl.handle.net/1887/4209969 (consultato il 30 maggio 2025).

Hoffman, S., (2020), Ex ante children's rights impact assessment of economic policy, in *The International Journal of Human Rights*, 24, 9, pp. 1333-1352.

Kahneman, D., Tversky, A., (1973), On the psychology of prediction, *Psychological Review*, 80, pp. 237-251.

Kahneman, D., Tversky, A., (1982), The simulation heuristic, in Kahneman, D., Slovic, P., Tversky, A., a cura di, *Judgment under uncertainty: Heuristics and biases*, Cambridge, U.K., Cambridge University Press, pp. 201-210.

Lalatta Costerbosa, M., (2019), I diritti dei bambini come priorità, *Rivista di filosofia del diritto*, numero speciale, pp. 137-160.

Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., Kidron, B., (2024), *The best interests of the child in the digital environment*, in https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf, 2024 (consultato il 30 maggio 2025).

Livingstone, S., Stoilova, M., (2021), The 4Cs: Classifying Online Risk to Children, in *CO:RE Short Report Series on Key Topics*, in https://www.ssoar.info/ssoar/handle/document/71817 (consultato il 30 maggio 2025).

Livingstone, S., (2020), *Can we realise children's rights in a digital world?*, in https://medium.com/reframing-childhood-past-and-present/can-we-realise-childrens-rights-in-a-digital-world-d4f5f19f298f (consultato il 30 maggio 2025).

Livingstone, S., Third, A., (2017), Children and young people's rights in the digital age: An emerging agenda, *New Media & Society*, 19, 5, pp. 657-670.

Lessig, L., (1999), *Code and other laws of cyberspace*, New York, Basic Books, [Online] Consultabile all'indirizzo: https://lessig.org/images/resources/1999-Code.pdf (consultato il 30 maggio 2025).

Lud, D., (2020), Impact Assessment, in Idowu, S., Schmidpeter, R., Capaldi, N., Zu, L. Del Baldo, M., Abreu, R., a cura di, *Encyclopedia of Sustainable Management*, Cham, Springer.

Maestri, E., (2017), Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio, *Ars Interpretandi*, 1, pp. 15-28.

Mai, J.E., (2016), Big Data Privacy: The Datafication of Personal Information, *The Information Society*, 32, 3, pp. 192-199.

Mantelero, A., Esposito, M.S., (2021), An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems, *Computer Law & Security Review*, 41, 105561.

Martoni, M., (2020), Datificazione dei nativi digitali e società della classificazione. Prime riflessioni sull'educazione alla cittadinanza digitale, *Federalismi.it*, 1, pp. 119-136.

Mascheroni, G., (2020), Datafied childhoods: Contextualising datafication in everyday life, *Current Sociology Review*, 68, 6, pp. 798-813.

Mittica, M.P., (2001), Una cornice giuridica per partecipare: la legge 285/1997, in C. Baraldi, a cura di, *I diritti dei bambini e degli adolescenti. Una ricerca sui progetti legati alla legge 285*, Roma, Donzelli, pp. 27-50.

OECD, (2024), Framework for Anticipatory Governance of Emerging Technologies, in *OECD Science, Technology and Industry Policy Papers*, 165.

OECD, (2021), Children in the Digital Environment. Revised Typology of Risks, *OECD Digital Economy Papers*, 302.

Paolucci, C., Vancini, S., Bex Ii, R.T., Cavanaugh, C., Salama, C., de Araujo, Z., (2024), A review of learning analytics opportunities and challenges for K-12 education, *Heliyon*, 10, 4, e25767, pp. 1-14.

Pariser, E., (2012), *Il Filtro*, Milano, Il Saggiatore.

Payne, L., (2019), Child Rights Impact Assessment as a policy improvement tool, *The International Journal of Human Rights*, 23, 3, pp. 408-424.

Rodotà, S., (1997), *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, Bari-Roma, Laterza.
Ronfani, P., (1998), L'interesse del minore nella cultura giuridica e nella pratica, *Studi Urbinati*, 68, pp. 675-698.
Ronfani, P., (1997), L'interesse del minore: dato assiomatico o nozione magica?, *Sociologia del diritto*, 1, pp. 47-93.
Selwyn, N., (2019), What's the Problem with Learning Analytics?, *The Journal of Learning Analytics*, 6, 3, pp. 11-19.
Solove, D.J., (2013), Introduction: privacy self-management and the consent dilemma, *Harvard Law Review*, 126, 7, pp.1880-1903.
Sunstein, C.R., (2019), Sludge Audits, *Harvard Public Law Working Paper*, 19-21, pp. 1-31.
Sunstein, C.R., (2022), *Sludge. What Stops Us from Getting Things Done and What to Do about It*, Cambridge, The MIT Press.
Thaler, R.H., Sunstein, C.R., (2009), *La spinta gentile*, traduzione italiana di A. Oliveri, Milano, Feltrinelli.
Twenge, J.M., (2018), *Iperconnessi*, Torino, Einaudi.
UNICEF, (2024), Developing Global Guidance for Child Rights Impact Assessment in Relation to the Digital Environment. Summary of Initial Project Findings, aprile 2024, in https://www.unicef.org/media/156046/file/Child%20Rights%20Impact%20Assessments%20in%20Relation%20to%20the%20Digital%20Environment.pdf (consultato il 30 maggio 2025).
UNICEF, (2021), Child Rights Impact Assessment. Template and Guidance for Local Authorities, giugno 2021, in https://www.unicef.org.uk/child-friendly-cities/wp-content/uploads/sites/3/2022/06/CRIA_June-2022.pdf (consultato il 30 maggio 2025).
Van Dijck, J., (2014), Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology, *Surveillance and Society*, 12, 2, pp. 197-208.
Vella, F., (2023), *Diritto ed economia comportamentale*, Bologna, il Mulino.
Zaccaria, G., (2022), *Postdiritto. Nuove fonti, nuove categorie*, Bologna, il Mulino.
Zuboff, S., (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, traduzione italiana di P. Bassotti, Roma, Luiss University Press.

Corpi digitalmente modificati. Law and Humanities per adolescenti nell'epoca della trasformazione digitale

Digitally Altered Bodies: Law and Humanities for Adolescents in the Age of Digital Transformation

M. Paola Mittica[1]

> *La capacità è un modo di stare al mondo, il cui valore di senso si attiva o si disattiva a seconda di come ci se ne impossessa e di come ci si confronta con essa*.
> (Dufourmantelle 2025, p. 47)

Sommario

L'acronimo ADM – *Adolescenti Digitalmente Modificati* – è stato coniato nell'ambito della psicologia psicosomatica per descrivere i cambiamenti profondi che la digitalizzazione sta producendo nei nativi digitali. Il concetto individua una trasformazione psicosociale e neurologica indotta dall'ambiente digitale, che coinvolge i processi affettivi, cognitivi, linguistici, emotivi, relazionali e corporei.

Il rischio per i nuovi adolescenti è di non riuscire a maturare la necessaria competenza somatica per affrontare un rapporto pieno con l'Altro, da cui procede lo sviluppo della soggettività e la capacità di essere presenti a se stessi e agli altri nella relazione.

Nella prospettiva di contribuire all'integrazione delle componenti della sensibilità, nella fase delicata dello sviluppo adolescenziale, si inserisce la proposta educativa di Law and Humanities, osservando il diritto come linguaggio dell'alterità e spazio in cui si negoziano misura, responsabilità e rispetto.

Parole chiave: adolescenti; digitalizzazione; competenza somatica; law and humanities

Abstract

The acronym ADM – *Adolescenti Digitalmente Modificati [Digitally Modified Adolescents]* – was coined within the field of Italian psychosomatic psychol-

1 Dipartimento di Giurisprudenza, Università degli Studi di Urbino. maria.mittica@uniurb.it

Data invio: 1 luglio 2025. Data accettazione: 5 agosto 2025.
DOI: https://doi.org/10.54103/1972-5760/30057

ogy to describe the profound changes that digitalisation is producing in digital natives. The concept identifies a psychosocial and neurological transformation induced by the digital environment, which involves affective, cognitive, linguistic, emotional, relational, and bodily processes.
For today's adolescents, the risk is failing to develop the somatic competence to engage in a fulfilling relationship with the Other, necessary to develop subjectivity and capacity to be present to oneself and the Other.
Aiming to contribute to the integration of the components of sensibility during the delicate phase of adolescent development, the paper proposes an educational approach to Law and Humanities, framing law as the language of otherness and as a space where measure, responsibility, and respect are negotiated.

Keywords: Adolescents; Digitalisation; Somatic Competence; Law and Humanities

1. Metamorfosi

ADM è uno dei molti acronimi che definiscono i nativi digitali[2]. Sta per "adolescenti digitalmente modificati" (Scognamiglio, Russo 2018), un'espressione retorica che forse non ha ancora guadagnato il rango di vera e propria categoria nelle discipline psicologiche, ma efficace nel rappresentare la mutazione psicosociale e neurale, indotta dalla trasformazione digitale, che sta interessando nello specifico le generazioni Zeta e Alpha, vale a dire i nati rispettivamente dopo il 1997 e il 2010.

A differenza dei Millenials – la generazione precedente che, pur avendo abbracciato largamente le dimensioni esperienziali offerte da internet, conserva ancora la memoria dell'analogico e dell'*offline* – i giovanissimi Zeta e Alpha non hanno quasi più alcuno scarto rispetto al mondo digitalizzato, costantemente connesso e progressivamente dominato dall'intelligenza artificiale (Sgorlon 2024). Per loro, il digitale non è una tecnologia, ma un ecosistema naturale in cui esistono e si muovono con estrema facilità[3].

L'immersione in questo ambiente sta plasmando il loro modo di pensare, comunicare e interagire con ciò che li circonda, provocando una vera e propria metamorfosi della loro mente-corpo.

Essendo un organo plastico e sociale (Lingiardi 2024, p. 223), il cervello si configura, infatti, a seconda del contesto e delle relazioni, producendo

2 Sia chiaro sin da queste prime battute che per definire le adolescenti e gli adolescenti, e le varie espressioni a loro collegate (come in questo caso "nativi digitali"), l'impiego del genere maschile è soltanto formale e finalizzato a non rendere il testo ridondante.

3 Per la descrizione e l'analisi critica di questo ecosistema si rinvia al saggio introduttivo in questo dossier di Maestri e Manfré.

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

processi mentali che variamente stimolano o impediscono possibili attività, qualità e competenze al livello del soggetto e della sua capacità di individuarsi. "Siamo corpo-cervello-mente in relazione" sintetizzano efficacemente Gallese e Morelli (2024, p. 17).

Il problema, nel caso degli adolescenti I-Gen, come li definisce Twenge (2018), è che crescere in un contesto che è anche infosfera influenza lo sviluppo della mente-corpo, rafforzando, come vedremo, una serie di abilità utili all'interazione con il medium macchinico, a scapito di qualità fondamentali per "centrarsi" nella propria soggettività e accedere a una dimensione relazionale in modo rispettoso e fecondo. Un quadro, questo, reso ancora più problematico dalla frattura simbolica dovuta alla grande velocità con cui evolve la tecnologia, che in questa fase storica accresce un divario tra adulti e adolescenti particolarmente "traumatico" (Manfré 2018), di cui, peraltro, non si ha ancora piena consapevolezza (Kidron, Rudkin 2023).

Prima di tutto, dunque, è necessario comprendere. Linguaggi, aspettative, abitudini, attitudini. Tutto è segnato da una radicale separazione di senso tra referenti adulti e giovani – tra genitori e figli, insegnanti e alunni, legislatori e "minori" – che ostacola la possibilità di far convergere due universi che sembrano non potersi più comprendere, con la conseguenza di non riuscire a trovare le risposte che il mondo adulto *deve* a queste persone e al futuro.

Su questi temi, nei vari campi che coinvolgono il lavoro sugli e con gli adolescenti, le proposte sia in ambito formativo che educazionale sono numerose. Limitatamente alle letture condotte, la sensazione che ne abbiamo tratto è che la preoccupazione e a tratti un malcelato pregiudizio prevalgano sulla fiducia nelle capacità reali degli ADM, svalutando e forse inibendo ulteriori potenzialità della trasformazione che è già in atto, soltanto perché ancora non riusciamo a immaginare dove possa condurre. Il rischio è di non offrire loro un sostegno concreto e più che mai necessario in questo processo di crescita dai risvolti inediti, ostacolando per di più la costruzione di un ponte intergenerazionale, indispensabile per traghettarci nel futuro in una prospettiva di condivisione (Benasayag, Cohen 2024)[4].

Nell'economia del presente contributo, ragioneremo di corpi e di competenza somatica come vie di accesso all'esperienza relazionale dell'adolescente e al legame sociale. L'idea è di elaborare possibili strategie di intervento in ambito formativo impiegando il diritto attraverso le nozioni protogiuridiche del pudore e della giustizia, per fare emergere come la sensibilità giuridica possa offrire un'apertura importante, e Law and Humanities una meto-

4 La scarsa attenzione a un ascolto effettivo del punto di vista degli adolescenti e della loro partecipazione in prima persona alle politiche che li riguardano è più volte sottolineato da Favretto, Ferrara e Colangelo in questo dossier (cui si rinvia), con specifico riguardo ai fenomeni del bullismo e del cyberbullismo, e in parte anche da Martoni nel contributo dedicato – sempre in questo dossier – al CRIA (*Child Rights Impact Assessment*).

dologia utile per incidere sugli adolescenti, scartando da scientismi sterili o da visioni improvvide di certa parte della didattica.

2. A partire dal corpo

Cosa accade al corpo di un adolescente esposto sin dalla nascita al digitale e alla connessione online?

Gli psicologi in linea con le neuroscienze affettive ci dicono che la digitalizzazione intacca e precarizza i processi primari – attaccamento affettivo, funzionamento cognitivo, rapporto con il linguaggio, gestione delle emozioni e delle relazioni, competenza somatica – limitando lo sviluppo della soggettività. Ciò a fronte di una reattività corporea che, con l'esposizione continua al codice digitale, si fa sempre più ingombrante, poiché altera le capacità e le azioni degli adolescenti, influenzando la loro esperienza di crescita, fino a provocare anche gravi forme di disagio (Scognamiglio, Russo 2018).

Già McLuhan (2008) scriveva che gli effetti della tecnologia non si verificano soltanto al livello delle opinioni o dei concetti, ma alterano costantemente e senza incontrare resistenza le reazioni sensoriali e le forme di percezione. Oggi, a fronte della consapevolezza che la mente-corpo è "una" (Damasio 2022), sappiamo che è il corpo a segnare la continuità spaziale e temporale tra soggettività e ambiente. L'esperienza che nasce dall'interazione con l'ambiente (fisico e sociale) sollecita la mente-corpo avviando il processo di costruzione del dialogo tra i due emisferi del cervello: quello destro più intuitivo, emotivo, visivo, tattile; e quello sinistro, più linguistico e analitico. Ed è proprio in questo continuo dialogo implicito, mediato dall'emisfero destro, la matrice originaria preverbale da cui prende vita il nucleo del nostro sé. Nelle prime fasi della crescita, l'esperienza è sensoriale; poi, quando cominciamo a parlare e a capire il mondo intorno a noi, si attiva l'emisfero sinistro. Una volta adulti, i due emisferi lavorano insieme per creare un'esperienza unitaria e fluida (Lingiardi 2024, pp. 16-18).

Il punto è che nel corso della crescita, sotto l'influsso di stimoli esterni, il cervello si modifica tanto da irrobustire le capacità mentali a servizio delle attività che si fissano in routine, mentre quelle non impiegate vengono di molto indebolite, se non del tutto sopite (Scognamiglio, Russo 2018, p. 63). Più nello specifico, il cervello dell'adolescente è caratterizzato dal *pruning*, un processo di "sfoltimento sinaptico", "una specie di potatura" per cui alcune aree cerebrali si rinforzano e altre meno utilizzate vengono eliminate o ridimensionate, incidendo direttamente sulla struttura definitiva del cervello adulto (Lingiardi 2024, p. 226). Si comprende bene, dunque, quanto possa diventare problematico l'impatto della digitalizzazione su un'architet-

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

tura cerebrale così in movimento, anche in vista delle future capacità degli adolescenti una volta divenuti adulti.

2.1 Surplus corporeo

Quando nell'adolescente, per effetto di un'eccessiva reattività del corpo, prende il sopravvento la dimensione somatica, si parla di "surplus corporeo".

Diversamente da quello delle generazioni passate, "governato" da una soggettività che si sviluppava, nel bene e nel male, sotto la guida di robuste agenzie di socializzazione, il corpo del nuovo adolescente non risulta sufficientemente organizzato da una funzione regolativa interna. Si tratta di una condizione di vuoto simbolico che con il passaggio dall'analogico al digitale va sempre più aggravandosi, esponendo un adolescente senza sufficienti difese[5] al rischio di disperdere la propria soggettività tra modelli di comportamento stereotipati, cristallizzati nella logica computazionale (Han 2015), e macchinici, funzionali all'efficienza della macchina (Benasayag, Cany 2022).

È una corporeità "anarchica" che può modificare l'organizzazione della mente. In balìa di un corpo che non governa dall'interno, l'adolescente inconsapevolmente "agìto", sviluppa la reattività, l'immediatezza e la velocità richieste dalla macchina, esponendosi a un progressivo indebolimento di altre risorse.

Esemplifica questa dinamica l'uso di videogiochi. Nell'interazione con i videogame, la comunicazione con la macchina, che attinge direttamente al sistema sensoriale, può prevaricare gli altri processi di natura cognitiva e relazionale. Si tratta di un condizionamento che dipende tanto dall'arricchimento dell'esperienza sensoriale degli utenti (si pensi al frequente ricorso alla realtà aumentata), quanto dalla capacità di risposta del giocatore, sfidato a confrontarsi con immagini in sequenza rapidissima e in modo sempre più performativo.

D'altronde, la competizione avviene con l'applicazione stessa. Non c'è un vero e proprio antagonista: è la macchina che allena il giocatore al gioco, e ciò condiziona la configurazione della mente, inibendo il pensiero. "Il coinvolgimento cresce con l'apprendimento ripetitivo di automatismi di risposta che producono un'iperattivazione corporea a scapito della stimolazione co-

5 Il riferimento è alle competenze digitali, che, in particolare, per gli adolescenti italiani, rappresentano un fattore di preoccupazione. Nella mappa europea sulle competenze digitali dei 16-19enni, infatti, l'Italia si posiziona quart'ultima: quasi il 42% degli intervistati ha competenze scarse o nessuna competenza, contro una media europea del 31% (Save the Children 2023). Su ciò che deve intendersi per "competenze digitali" si rinvia all'articolata definizione che ne dà Pascuzzi in questo dossier.

gnitiva e metacognitiva. Non si può pensare, o meglio, non si deve pensare, in quanto il pensiero rallenta l'azione" (Scognamiglio, Russo 2018, p. 50)[6].

Un ulteriore esempio può essere colto nel modo di leggere di molti adolescenti. La massiccia esposizione ai testi digitali e alle infinite informazioni che sono abituati a scorrere rapidamente rende i loro movimenti oculari velocissimi. Mentre il testo viene "scrollato" da dita altrettanto abili, gli occhi dei nativi digitali fotografano e catturano i dati che li interessano in modo rapido e intuitivo. Di conseguenza l'attività della lettura si riduce al reperimento di informazioni, e, poiché a prevalere è l'impiego di quelli digitali, gli ADM si abituano ad approcciare nello stesso modo anche i testi su supporto cartaceo. Così disposta, questa funzionalità stimola lo sviluppo dell'area del cervello deputata al *problem solving*, ma non sollecita anche altre zone, in genere attivate dalla lettura analogica, preposte alla memoria, all'elaborazione degli stimoli visivi, nonché al linguaggio e alle sue qualità sensoriali e metaforiche, facendo venire meno la capacità di mantenere la concentrazione, creare connessioni e inferenze, di immaginare.

Stesso discorso vale per il *multitasking*, una nuova abilità in capo ai nativi digitali che, pur presentando indubbi aspetti positivi, andrebbe valutata tenendo conto che gli stati di iperattivazione corporea, che rendono possibile lo svolgimento di più attività in contemporanea, indeboliscono anche la verticalizzazione del pensiero.

Si tratta giusto di pochi esempi. L'importante qui è osservare che, a fronte delle numerose e diverse prestazioni pretese dai loro corpi, gli adolescenti si ritrovano a rispondere agli stimoli del codice digitale in modo sempre più efficiente, riducendo lo sviluppo delle capacità cognitive necessarie per penetrare dimensioni complesse.

D'altronde, le abilità allenate dalla macchina sono di tipo "riflesso", ma non "riflessivo". La velocissima acquisizione delle informazioni è senza attenzione, né concentrazione: superficiale e frammentata, priva dell'elaborazione dei contenuti, per cui la densità del pensiero non può che uscirne ridotta, e con essa la comprensione anche del proprio sentire.

Detto in sintesi, sopraffatto dal proprio corpo, l'ADM rischia di non ragionare e di non sentire, o meglio *di non riconoscere ciò che sente*. E i sintomi ci sono tutti: fatica nella gestione delle emozioni e nell'elaborazione di narrazioni, poca autobiografia, impiego modesto di memoria, di fantasia.

6 Certamente, quanto più si fa massivo l'uso dei videogame, tanto più l'adolescente si espone al rischio di contrarre il disturbo del comportamento noto come *Internet Gaming Disorder*, ovvero una forma di dipendenza dovuta alla gratificazione fornita dal gioco, cui spesso si accompagna il ritiro sociale. Detto ciò, in nessun modo, l'uso ordinario dei video giochi provoca *addiction*. Né va demonizzato. Tutt'altro. Sono tanti e vari gli aspetti positivi di questa pratica, tanto che in ambito psicologico i videogame si prestano anche all'impiego per fini terapeutici (Lancini 2019).

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

2.2 Competenza somatica

L'imporsi di un corpo reso avido di codice rende bulimici: "È come mangiare da una scodella sempre piena: non si smetterebbe mai!" (Bormetti 2019, pp. 80-81).

Eppure, paradossalmente, è proprio questo stesso corpo esposto al digitale a erigersi a maggiore ostacolo di fronte alla realizzazione dell'uomo macchina. È "nella corporeità che resiste", insegna Baudrillard (2015, p. 129), che il soggetto può trovare il proprio centro rimettendo sulla scena la soggettività estromessa dalla digitalizzazione "esattamente in ciò che del corpo le sfugge".

La lezione del sociologo francese è preziosa. L'incorporeità, che Twenge (2018) adduce come caratteristica ricorrente nei nativi I-Gen, potrebbe essere dovuta a una sorta di "incompetenza somatica". Più l'adolescente si sposta verso il codice digitale, più rischia di diventare "macchinico" e incapace di attingere al complesso delle proprie risorse. L'interazione tra cervello-mente-corpo e mondo potrebbe sbilanciarsi e impedire la vicinanza e il confronto con l'Altro da sé, indispensabile, per individuarsi e relazionarsi.

Questa, in estrema sintesi, l'ipotesi da cui vogliamo muovere per riflettere su come contattare e accompagnare questi adolescenti nel recupero della loro corporeità in vista di uno sviluppo equilibrato.

Ci avventuriamo, pertanto, e non senza timidezza, nel vasto campo di ricerca interdisciplinare noto come *Embodied Cognitive Science*, che coinvolge quanti si interessano di "cognizione incarnata", in generale psicologi, neuroscienziati, studiosi delle scienze umane.

La tesi di fondo che accomuna questi ricercatori è che il nostro modo di pensare, comprendere e interagire con il mondo è strettamente legato all'esperienza corporea: il cervello non opera in modo isolato, ma in completa integrazione con il corpo e l'ambiente esterno; per ciò stesso l'esperienza corporea è in uno con il processo cognitivo.

Si tratta, peraltro, di un orientamento, che integra e rafforza un indirizzo che vanta illustri antecedenti nella storia del pensiero, accreditatosi in questi ultimi anni come "filosofia del corpo" (Marzano 2010, Galimberti 2013), in aperta critica del paradigma razionalistico che ancora informa la cultura occidentale (Benasayag, Schmit 2013). Su questa linea teorica, senso, sentire e sentimento non possono essere scissi. Il pensiero va osservato come forma del sentire, che guida la ricerca di un senso anch'esso sensibile (Mittica 2022). *Non abbiamo un corpo, ma siamo corpo: "il senso del corpo"* afferma Nancy (2004).

La nozione di "competenza somatica", che a pieno titolo si colloca in questo quadro, si sviluppa nel campo della psicosomatica, dove, su base teorica e sperimentale, si sta mettendo a punto il modello terapeutico della *Somatic*

Competence. L'obiettivo è trattare le varie forme di deficit che affliggono i nuovi adolescenti esposti alla digitalizzazione, definiti appunto ADM.

Sebbene il tipo di approccio desti ancora resistenza tra gli addetti ai lavori, il modello sta ricevendo numerosi riscontri positivi nell'esperienza. È quanto dimostrano Scognamiglio e Russo (2018, p. 206), esponendo i vari casi affrontati nella pratica.

Per questi due psicologi, punto di partenza ineludibile perché una relazione di cura sia efficace è che il *caregiver* abbia competenza somatica e sappia trovare con l'adolescente un contatto "sensibile" ancor prima che dialogico. La competenza somatica dell'ADM deve essere sollecitata da chi è in grado di mettere in gioco la propria. Vale a dire che il *caregiver* deve lasciare che siano le sensazioni e le emozioni a trovare una strada verso l'adolescente, mettendolo nella condizione di poter contattare innanzi tutto la sua di corporeità, sconosciuta a lui stesso. Per questi studiosi, quindi, è fondamentale disporsi verso un'interazione primaria, dove non sono le parole, ma i sensi, gli sguardi, il respiro, i movimenti del corpo a costituire i feedback relazionali. L'attenzione deve rivolgersi all'ambito preverbale. Bisogna cercare di comprendere come sta l'altro attraverso l'uso del corpo, senza tradurre subito lo scambio in convinzioni razionali. Per aprirsi all'ascolto e muoversi verso l'adolescente che non sa di sé, il *caregiver* deve partire, in definitiva, dall'identificazione delle proprie emozioni e sensazioni. Si entra in relazione quando si avvia un ascolto *reciproco* e *di se stessi*, in un processo continuo di andata e ritorno dall'uno all'altro, in cui i "come ti senti" e poi i "come mi sento", sono i feedback che permettono all'interazione di non astrarsi dai vissuti corporei. Perché il dialogo diventi esperienza, insistono Scognamiglio e Russo (2018), è necessario mantenere la "focalizzazione somatica". Soltanto su questa base si può procedere con ulteriori pratiche di approssimazione per riuscire a far emergere le emozioni, le sensazioni e i sentimenti che conducono alle cause profonde del disagio.

Dal nostro punto di vista, sebbene sia evidentemente rivolta al trattamento di patologie, la *Somatic Competence* suggerisce una metodologia e strumenti di intervento potenzialmente utili anche al di là del contesto di cura riservato a psicologi e psicoterapeuti. D'altra parte, non sembra affatto un azzardo, soprattutto in considerazione dello spettro teorico in cui la stessa si inscrive, e del focus sull'evoluzione dei nativi digitali[7].

7 A questo proposito è di grande interesse una recente ricerca dell'Istituto Superiore di Sanità volta a individuare i fattori di rischio relativi alle dipendenze comportamentali degli adolescenti esposti alla digitalizzazione. L'analisi dei dati si basa sul confronto tra gruppi "a rischio" e "non a rischio". E quindi, insieme ai dati che rilevano e misurano l'effettiva esposizione al rischio di *addiction* di una parte degli intervistati, la ricerca misura anche le condizioni di coloro che non rischiano forme di dipendenza, e che risultano essere la maggioranza, dimostrando, sebbene limitatamente agli elementi considerati, che anche gli adolescenti non esposti al rischio di patologie, maturano comunque forme di malessere (Mortali et al. 2023).

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

In tal senso, impiegheremo la nozione di competenza somatica in modo più esteso: da una parte, osservando la mutazione delle generazioni Zeta e Alpha come un fatto che incide in varia misura sulla configurazione delle loro competenze, anche quando non sfocia in forme di disagio grave; dall'altra parte, riconoscendo al "pensare" radici profonde nella corporeità, osservandolo, con Han (2025, p. 68), come *innervato da sensazioni, emozioni, affetti*, ed esito di processi mentali in cui si integrano tutte le risorse cognitive dell'essere umano.

3. Senza l'Altro

Così rielaborata, la nozione di competenza somatica ci consente di considerare anche la scarsa familiarità degli ADM con il dolore.

Il dolore è un sentimento cruciale, esistenziale, qualunque sia la forma o l'intensità con cui si manifesta. È indispensabile per accedere all'esperienza e al conoscere, afferma Natoli (2008). L'adolescente che non riesce a riconoscerlo – in se stesso come negli altri esseri viventi – rischia di non sviluppare profondità di pensiero.

Si può provare dolore soltanto se si ha la capacità di emozionarsi. Ogni e-mozione comporta uno spostamento dalla propria *comfort zone*. Qualunque sia la natura dell'emozione o la modalità dello "stare al riparo", l'e-mozione sorge dal farsi avanti di un Altro che espone a qualcosa di sconosciuto, scomodo, teso verso un altrove. È una sorpresa dolorosa perché rende tangibile il limite che l'Altro rimanda: l'enigma che non si scioglie, il mistero destinato a non svelarsi. La prima manifestazione dell'Altro non è nel "Tu" o nel "mondo", ma nel dolore che l'esporsi in questa apertura ha provocato. Se non si giungesse a questa soglia, il pensare e la conoscenza resterebbero preclusi. La *comprensione* non può prescindere da una forma di pathos (Masullo 2003), non può esistere "senza un *esser smossi*" (Han 2025, p. 68).

Ma c'è di più. Quando l'Altro è un altro essere umano, contattare il dolore è ciò che consente di disporsi alla *compassione* (Prete 2013), dove il *cum* del *com*-patire rivela come la *com*-prensione emerga dall'intima connessione tra la corporeità del *pathos* e il *noi* del legame tra "altri".

Nella società "palliativa" che occulta il dolore (Han 2021), assuefatti dalla cultura della felicità fittizia, gli adolescenti che *non sanno di soffrire*, rischiano di non sviluppare la capacità di comprendere e di *legarsi nel profondo*. Il dolore li abita, li agita, ma non riconoscendolo, né sapendolo attraversare, lo subiscono scambiandolo con altro. Piuttosto che farne una risorsa, tentano

Sulla crescita del disagio tra gli adolescenti al livello internazionale vedi anche i rapporti dei Centers for Disease Control and Prevention (2024) e del WHO Regional Office for Europe (2025).

di restarne indifferenti, lasciandosi stregare da maghi e fattucchiere del mercato (per lo più digitale) dell'evasione, mentre maturano frustrazioni che possono condurli anche a comportamenti violenti o autolesivi.

L'incompetenza somatica dell'ADM coincide, in altre parole, con la deprivazione del sentimento doloroso dell'Altro.

Senza l'Altro l'esposizione al mondo non può concretizzarsi in un processo esperienziale. Se l'adolescente non incontra l'Altro da sé, non può individuarsi nella propria soggettività, né attivare il confronto che gli consente di osservare il limite suo e dell'Altro, coglierne la misura, sperimentare una relazione.

Immerso nell'infosfera, da "persona", "nodo di legami", parte viva di un essere in comune, l'ADM si avvia a diventare "profilo": destinazione finale del processo di frammentazione e svuotamento del soggetto, dispiegato dal mondo delle tecnologie digitali. Un processo, i cui meccanismi di dominio e deregolamentazione mirano a dislocare ciò che rimane delle forme di alterità, distruggendo la persona dal suo interno (Benasayag, Cany 2022, p. 15 ss.).

Come abbiamo visto, l'espulsione dell'Altro (Han 2017) è un rischio tangibile a fronte dei comportamenti adattivi dell'adolescente sollecitati dall'interazione digitale. Preso dal consumo massivo di "non cose" (Han 2022), l'ADM non si accorge che, nel filtrare ogni suo accesso all'esperienza, il medium digitale diviene inavvertitamente il suo unico interlocutore. Non riuscendo a portare lo sguardo al di là della realtà confezionata per lui, rischia di non potersi rapportare ad alcunché o ad alcuno, nemmeno a se stesso. L'intimità potrebbe andare perduta e la connessione costante con "gli altri" fornita della rete risultare un tranello, inducendolo a un progressivo ritiro dal mondo e dalla propria persona.

3.1 ON-OFF

Se limitata alla mediazione digitalizzata, la relazionalità degli ADM si sviluppa con un'intensità ridotta (Lancini 2019)[8].

Nonostante ne moltiplichi le occasioni, il medium digitale consente di "stare in contatto" ma non il *con-tatto*. A differenza del *toccare* e del *sentirsi toccati* da qualcosa o qualcuno (Lingiardi 2024, pp. 54 ss., 249), non crea alcuna *vicinanza* (Han 2025, p. 19). Le conversazioni tra adolescenti canalizzate da chat o social network sono asincrone, mediate da emoji e messaggi; non richiedono la messa in campo di sensibilità che interverrebbero

8 È importante precisare che attualmente, e per fortuna, per quanto concerne gli adolescenti italiani, quello mediato digitalmente investe ancora soltanto una parte dei tanti modi di relazionarsi. Si rinvia per un'analisi accurata ai rapporti ISTAT 2025 e Gruppo HBSC-Italia 2023.

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

necessariamente nella conversazione *face to face*, anzi ne osteggiano anche lo sviluppo, favorendo il ritrarsi dal coinvolgimento con l'Altro.

In questi casi, la relazione sembra rispondere, più che al desiderio di interagire con i propri pari, al bisogno di riempire il vuoto, il silenzio: di rimediare alla noia che l'adolescente, abituato alla reattività macchinica, mal tollera. Nel continuo scambio di messaggi, spesso non viene detto nulla che abbia un senso preciso o un inizio e una fine. È un (non)comunicare del tutto contingente finalizzato essenzialmente a un "esserci olografico": uno spazio in cui l'interazione è del tutto appiattita sui bisogni di un Io inconsapevole e incurante dell'Altro.

Più in generale, la compromissione della relazionalità comporta numerose conseguenze. Ne consideriamo soltanto alcune.

La prima è l'oggettivazione del proprio sé e dell'Altro. Non riuscendo a cogliere, insieme alla propria, l'alterità dell'Altro, l'ADM non elabora la propria soggettività e produce identità per così dire "di risulta", dettate da contenuti variamente veicolati. Si pensi a come gli adolescenti costruiscono il proprio *brand* combinando qualità, nella rappresentazione di sé e degli altri, in base alle quantità di *like* ricevuti o di *follower* (Sgorlon 2024). Le identità di questi giovanissimi si avviano a essere l'esito di metriche, oggetti da esporre, scambiare. Soltanto merci confezionate in pacchetti predefiniti e consacrate alla *cultura dell'Uguale* (Han 2017).

Una seconda conseguenza è l'aumento del disimpegno nel coinvolgimento. La pratica del *ghosting* è sempre più diffusa (Bormetti 2019, pp. 68-69). Una chat si può chiudere senza doversi anche confrontare, basta un click. La stessa quantità di sforzo è sufficiente per bloccare l'interlocutore non gradito. Se qualcosa "non piace" mentre si sta giocando a un videogame (forse si sta rischiando di perdere e non è sopportabile), basta "tiltare", cioè mandare in tilt il gioco, provocando la fine della partita (Lancini, Zanella 2019, p. 27). Ma attenzione. Il disimpegno non è che l'effetto dell'assenza del coinvolgimento. L'interazione digitale non è necessariamente preludio di una relazione, soprattutto se l'incontro è destinato a restare all'interno del circuito cibernetico.

Nell'esposizione massiva al digitale, le risorse affettive degli ADM si riducono, lasciando spazio a un'interazione che è più vicino a un meccanismo di risposta ON-OFF, funzionale/disfunzionale, tipico del linguaggio macchina, che non a un rapporto sentimentale.

Incapaci di gestire emozioni e sensazioni, gli ADM svicolano. Inconsapevolmente assecondano la paura di non risultare adeguati. Temono l'esposizione di un sé che non controllano, di cui *non sanno bene*. L'espressione gergale *catching feeling* rivela quanto siano trattenuti verso i sentimenti: *prendersi un sentimento* suona come *prendersi un raffreddore*, una iattura.

Il rischio è di affidarsi alle scorciatoie digitali che consentono loro di evitare lo sguardo dei pari. Uno sguardo che il più delle volte è il proprio, poiché nel suo interlocutore l'adolescente impersona la proiezione ideale del suo sé. Il narcisismo è, del resto, una delle conseguenze più evidenti del rapporto Io-Tu istaurato dalla macchina. Il digitale offre una proiezione di possibilità all'infinito, ma tutte a servizio del rispecchiamento di se stessi. L'Altro, come mondo fuori, diventa sempre più evanescente. Il rapporto con l'altro essere umano si accende e si spegne, senza particolari implicazioni.

Quello che si offre in queste dinamiche, come dicevamo, è uello che

un tipo di legame sospeso su un vuoto simbolico. Non è sostenuto da valori o regole. Non si inscrive in un contesto di senso. E in nessun caso è autonomia. Gli attori dell'interazione digitale *agiscono per funzionare* (Benasayag 2019). La dimensione della responsabilità del proprio agire non ha alcuna incidenza in riferimento all'Altro (che sia l'essere umano o il vivente in generale), semplicemente perché dell'Altro non si ha percezione né cognizione. L'adolescente potrebbe finire con l'interpretare la responsabilità soltanto come "dovere di assecondare la propria volontà". La libertà e la giustizia potrebbero annullarsi nell'autoreferenzialità, nell'imperativo "ho il diritto di".

4. il posto del diritto

In estrema sintesi, l'espulsione dell'Altro dall'infosfera impedisce all'adolescente impreparato di cogliere l'esistenza del limite: un limite che si incarna nell'altro essere umano, nel mondo fisico che lo circonda, e di riflesso inevitabilmente nel suo stesso corpo.

Nella prospettiva di contribuire all'integrazione delle componenti della sensibilità nella fase delicata dello sviluppo adolescenziale, introdurre al diritto, nei suoi contenuti più originari, potrebbe intervenire su questa lacuna, portando all'attenzione di questi giovani in crescita l'esperienza del limite nella relazione con l'Altro, e l'ineludibile e incessante ricerca della sua misura, in cui consistono il rispetto e la responsabilità.

Soffermandoci su questa idea, non ragioneremo del diritto e della sua giustizia sul profilo della legislazione o della regolamentazione anche informale circa l'uso del digitale. La proposta è, come anticipato, di far emergere dalla semantica delle nozioni di diritto e giustizia, alcuni concetti in grado di introdurre, per quanto possibile, al rapporto con il vivente e alla relazionalità complessa che sono a fondamento del legame sociale.

In tal senso la scelta è ricaduta sui sentimenti protogiuridici del pudore e della giustizia come cura, entrambi espressione della simbolica dell'alterità e dell'accesso "sensibile" alla ricerca della misura nel rispetto di sé e della "relazione riguardosa", che sia con l'altro essere umano o con il mondo.

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

4.1 Pudore

Il pudore è per Vico ciò che distingue l'essere umano dalle altre specie animali, rendendolo creatura cosciente, pensante. La particolare coloritura giuridica che lo connota emerge dall'idea che il pudore sia quella qualità che consente all'uomo di scoprire di possedere *la libertà di frenare se stesso* (Capograssi 1959, p. 400). Il pudore si manifesterebbe come *sentimento dei confini*: sentimento portante della relazione giuridica originaria e per questo alla base del legame sociale (Limone 2019; Savona 2005, pp. 47-48).

La giuridicità della nozione di pudore affiora dal ricordo platonico del mito di Prometeo ed Epimeteo, attraverso il termine *aidos* in associazione a *dikē*. Come ha ben ricostruito D'Agostino (1979, p. 36): "*aidos* non solo è un'autolimitazione dell'io, ma una pretesa che l'altro si limiti nei confronti dell''io'".

Del tutto diverso dalla reazione al giudizio negativo (anche auto-inflitto) che caratterizza la vergogna, il pudore è una forma di riserbo, di ritegno, che si realizza nella resistenza che un essere umano oppone all'altro essere umano tenendolo appunto nella distanza: è la difesa dall'oggettivizzazione che l'altro potrebbe imporre, anche inconsapevolmente (Tagliapietra 2006, p. 150 ss.).

Il pudore è, dunque, una forma di sottrazione nel "rapportarsi a", affinché un'apertura, la tensione, verso l'altro possa essere mantenuta, senza che ciò comporti la negazione della relazione. Il fatto che implichi il misurarsi e il rispetto reciproco, ne fa una risorsa per il legame sociale e il vivere in comune (Cotta 1978, pp. 125-127; Guardini 1980; Orazi 2020).

Il pudore serve al *riguardo* (Han 2015, p. 11). Si tratta di evitare che la vicinanza diventi invadenza, per consentire anche all'altro di essere per se stesso. La relazione è dunque "riguardosa", animata dal senso del limite, e per questo giuridica. Ma è anche una dimensione affettiva che attinge il diritto dalla corporeità, e ci consente di dire che *la norma è misura nata dal sentimento*.

Gli adolescenti vivono tendenzialmente di imbarazzi, che spesso, mentre si ritraggono dalle relazioni, scambiano per pudore, confondendolo con la vergogna di sentirsi inadeguati. Ragionare e misurarsi col pudore potrebbe servire loro per accostare la corporeità che non padroneggiano, risvegliare o potenziare le risorse cognitive e affettive inibite, imparare a riconoscere l'intimità del proprio privato per sperimentare l'Altro nella distanza come nella vicinanza. In altre parole, per apprendere la complessità del *noi*, del vivere in comune.

4.2 Giustizia

Vale lo stesso per la giustizia. Nel mito di Prometeo ed Epimeteo, *aidos* è condizione di *dikē.* Come abbiamo appena visto, al sentimento dei confini

Platone associa quello rivolto alla giustizia. La distanza aperta dall'alterità è terzietà: è spazio in cui il sentimento del limite si concretizza nella ricerca della misura. La giustizia accade in questa dimensione terza, quando ognuno si assume l'impegno del limite e il riconoscimento della misura trovata è reciproco.

Prima di essere procedura per dirimere le liti, la giustizia è dunque sentimento di cura del legame sociale: originaria attenzione che si principia come cura dell'Altro e responsabilità per l'Altro, davanti all'Altro.

Nello spazio della convivenza, la giustizia si realizza quando si permette all'altro essere umano, al quale si è legati, il libero sviluppo di se stesso. Ma non è sufficiente il rispetto, il mantenersi nella distanza. Perché ciò accada è necessario prendersi carico dell'esistenza dell'altro, e come esseri umani avere cura, non soltanto reciprocamente l'uno dell'altro, ma di tutto il vivente.

A questa giustizia servono attenzione, compassione. Ma più di ogni cosa serve la dolcezza.

Mentre ci richiama alla nostra responsabilità di esseri umani nei confronti del mondo che ci circonda, degli esseri che lo compongono e persino dei pensieri che vi investiamo, la dolcezza, che ci rende familiari "con l'animale, il minerale, il vegetale, lo stellare", è intelligenza che attraversa il corpo: "occasione di una festa sensibile. Il tatto e il tattile, il toccare, il gusto, i profumi, i suoni ne aprono l'accesso. [...] Se la dolcezza fosse un gesto, sarebbe carezza [...] nel non impadronirsi di niente, nel sollecitare ciò che sfugge continuamente dalla sua forma verso un avvenire, nel sollecitare ciò che si sottrae come se non fosse ancora. Essa cerca, fruga. Non è un'intenzionalità di svelamento, ma di ricerca: cammino nell'invisibile" (Dufourmantelle 2022, pp. 26, 35, 75).

Anche la giustizia si appella, dunque, a risorse di una sensibilità del corpo che l'adolescente non sperimenta, almeno non consapevolmente. Per certo non siamo davanti a persone anaffettive, ma resta il problema, come anche per il pudore, di trovare il modo per attivare in questi giovanissimi anche le potenzialità cognitive della sensibilità.

4.3 Qualità della debolezza

Per stimolare le sensibilità appartate nel corpo dell'ADM, piuttosto che i *talenti che servono per funzionare*, possono risultare più interessanti alcune, per così dire, "disposizioni d'animo" che rendono gli adolescenti di ultima generazione particolarmente esposti e fragili, ma proprio per questo anche più inclini a un'apertura.

Ci riferiamo all'incertezza, al senso di precarietà, agli stati d'ansia e alla ricerca di conforto che accrescono in modo significativo il loro desiderio di comunicare e la capacità di avvicinare gli altri, e di inclusione.

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

Sono qualità deboli, che si manifestano nella fluidità e nella frammentarietà del contesto in cui gli ADM vanno svolgendo la loro esistenza, ma potrebbero rivelarsi delle vere e proprie risorse. Proprio perché inadatto alla struttura, un pensiero "indebolito" rende gli adolescenti più plastici, aperti, disposti a "ciò che non si sa". L'incertezza, il senso di precarietà, la tensione affettiva sono qualità che più facilmente lasciano emergere l'Altro e la possibilità del *noi*. Sono forme patiche, legate a filo doppio con la sensibilità. In tal senso, presentano un grande potenziale cognitivo che potrebbe sfociare in modi di pensare e agire importanti per la costruzione di alternative volte al futuro.

La sfida si pone dunque a più livelli. Innanzi tutto, bisogna valorizzare le qualità degli ADM, evitando, per inciso, l'errore ricorrente di molti adulti di confrontarle pregiudizialmente con le proprie alla loro stessa età, non considerando la profonda diversità dei vissuti da cui emergono; secondariamente, è necessario mettersi in ascolto di queste generazioni con rispetto; su questi presupposti, infine, è importante provare a elaborare strategie di intervento, per tentare di restituire ai nativi digitali l'accesso allo sviluppo di tutte le loro risorse, in modo che siano attrezzati al meglio per affrontare il loro difficile compito evolutivo.

5. Lavorare con Law and Humanities

Come anticipato, restando nel perimetro del presente contributo, la nostra proposta è di impiegare la metodologia di Law and Humanities, ritenendo che possa intervenire sulla (in)competenza somatica degli ADM almeno su due profili: consentendo di sperimentare la sensibilità che l'arte suscita in ogni sua forma; e facendo affiorare alla consapevolezza i sentimenti protogiuridici del pudore e della giustizia come cura, per ragionare di legame sociale e vita in comune. Si cercherà pertanto di individuare (ancorché a titolo meramente esemplificativo) alcune pratiche che possano far contattare agli ADM la propria affettività, e attivare e/o integrare una consapevolezza del corpo, colmando, almeno in parte, il "vuoto simbolico" sofferto dagli adolescenti.

Il campo di applicazione che abbiamo individuato è quello della didattica[9]. Ciò di riflesso al fatto che le generazioni Zeta e Alpha incontrano nella scuola una delle agenzie formative più importanti. A questo proposito vale per i docenti quanto detto per gli specialisti che si occupano di disagio.

9 È soltanto uno dei numerosi ambiti di applicazione implicati nello sviluppo e nel benessere digitale degli adolescenti che, come ben argomentano Thomas Casadei e Giovanni Ziccardi in questo dossier, richiede una progettazione che adotti un *approccio complesso e integrato*, in cui far convergere aspetti normativi, tecnologici, educativi e culturali, facendo dialogare competenze diverse e il coinvolgimento dei vari attori istituzionali.

Perché un'interazione volta a valorizzare la competenza somatica abbia successo, è necessario che chi guida il percorso non soltanto sia un "competente somatico", ma si affidi alla sensibilità per arrivare al suo discente, esponendosi al suo proprio coinvolgimento e allo stesso tempo governandolo.

In questo processo di avvicinamento ciò che conta maggiormente è la familiarità. Gli adolescenti devono *potersi trovare*, e questo può avvenire più facilmente se cominciano il proprio percorso su strade che in parte già conoscono. Per questo, come vedremo, anche il ricorso alla tecnologia va contemplato, e non soltanto per le sue enormi potenzialità di intervento su una popolazione che ne fa uso in modo disinvolto. Si tratta di intervenire prendendo in carico il fatto che la vita di queste generazioni si sviluppa in un ambiente che è ibrido, materiale e virtuale allo stesso tempo. Ignorare la necessità dei nativi digitali di fruire dei dispositivi informatici equivarrebbe a negare loro l'accesso al mondo, nella stessa misura in cui ignorandone le difficoltà si nega a un disabile di svolgere la propria esperienza in un universo analogico. Ha ragione Benasayag (2021), per non assecondare la brutale assimilazione alla tecnologia cui andiamo assistendo, non va demonizzato il mutamento antropologico che probabilmente sta interessando la nostra specie, bisogna elaborare piuttosto un modello di vita in cui si integrino la tecnica e il vivente.

5.1 Incontrare l'opera

Nell'attraversare le varie forme che si dispiegano nei suoi molti linguaggi, l'arte dispone al senso evocando la sensibilità. La sua *parola* è poetica. Ci *tocca* con immagini, suoni, odori, sapori, colori, emozioni. Ci dispone al pensare sensibile: alla sensibilità che coinvolge l'insieme delle sensazioni e delle emozioni attraverso cui sperimentiamo il mondo. Una storia sarà sempre possibile fin quando questa "parola", in qualunque forma la si vorrà esprimere, continuerà a narrare una vita da condividere tra "altri" (Jedlowski 2000; Han 2025).

Il primo problema da affrontare in questa impresa è "agganciare" l'ADM. Affinché l'adolescente possa attivare una propria elaborazione, serve un coinvolgimento in prima persona. Ma come stimolare l'interesse per un'opera d'arte?

Dimentichiamoci della storia dell'arte, e degli innumerevoli termini tecnici per descrivere un manufatto artistico che popolano i libri di testo delle nostre scuole: l'adolescente va messo in rapporto diretto con l'opera. La chiave è puntare sulla sorpresa.

Conta certamente la scelta dell'opera. Meglio se lontana dalla "cultura per ragazzi" e da contenuti tematici espliciti individuati dagli adulti a fini educativi. L'opera non deve fare la morale, ma avere l'arte. È l'arte che sorprende

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

e questa può essere colta in un'opera classica, così come in una che incontra il gusto dei più giovani o ne è lontanissima. La sorpresa è tanto più efficace quanto più irrompe nel loro ordinario. Ciò che conta è come l'adolescente vi si accosta. In tal senso, in un contesto come quello della didattica, potrebbe essere sufficiente essere irrituali, uscire dagli schemi e dai programmi preconfezionati, mettendo in campo un contenuto inaspettato con una modalità non prevedibile. Un'azione simile susciterebbe di per sé curiosità.

Ma questo è solo l'espediente per catturare l'interesse. La sorpresa accade quando l'incontro con l'opera provoca uno spostamento e, nel *toccare*, spiazza.

Avremo colto nel segno soprattutto quando l'ADM reagisce con manifestazioni di imbarazzo, reticenza, quando entra in ansia o dissimula il suo disagio con la noia o trincerandosi narcisisticamente su di sé. Significa che l'incontro con l'opera sta già toccando quei sentimenti messi da parte, che l'adolescente non sa o non vuole dire o dirsi, custoditi dalla sua corporeità nella parte che resiste alla tecnologia: il senso di inadeguatezza se non di vergogna; il vuoto; la paura di non essere accettato, della solitudine.

Questo primo contatto dovrebbe avvenire in un contesto rassicurante, anche ludico, nella cornice di un'esperienza condivisa con i docenti e in gruppo con i pari, nella complicità, in modo da ridurre l'esposizione personale davanti agli altri, limitando la preoccupazione, per consentire che le sensazioni provocate dalla sorpresa siano accolte.

È fondamentale, infatti, che la sorpresa provocata dall'esterno si trasformi in stupore per l'inaspettato, che l'opera suggerisce in immagini, emozioni, pensieri: sensazioni che possono aprire uno spiraglio sull'intimità di se stessi e la voglia di starci dentro.

Una volta agganciato, l'ADM va trattenuto.

5.2 Mettersi in-opera

Il suggerimento è che l'adolescente si *soffermi* sull'opera d'arte prestando attenzione a ogni dettaglio, lasciandosi trasportare (muovere) da tutto il portato sensibile che la stessa gli evoca. L'opera l'ha *toccato*. Ora è necessario che l'ADM si metta in-opera (Andreotti 2018, Mittica 2016).

Proviamo a immaginare alcune pratiche esemplificative.

Ascoltare un brano musicale dall'inizio alla fine, possibilmente ad occhi chiusi per agevolare l'individuazione dei dettagli, e meglio se bendati. Se si tratta di una canzone, non dissociare le parole dalla musica. Oltre all'esercizio dell'attenzione in una condizione di intimità, è importante allineare il proprio tempo con quello del pezzo, impedendo alla componente "bulimica" del proprio corpo di prendere il sopravvento, interrompendo l'ascolto, per scrollare una delle tante playlist, e ridurre così l'esperienza.

Osservare un'opera visiva e/o materica predeterminando un limite minimo di tempo e cronometrandolo. L'esperienza è più proficua se l'opera è astratta. Senza un tema o un soggetto riconoscibile è ineludibile soffermarsi sui colori, le sfumature, le forme, le ombre, le pieghe. Qui l'allenamento è dello sguardo, cui segue contestualmente la scoperta della propria capacità di individuare così tanti contenuti in qualcosa che, senza questo trattenersi, ne sarebbe risultato privo. Pensiamo per esempio a un quadro di Rotzco: a uno sguardo superficiale è poco più di una macchia di colore, ma più lo si guarda, più si accende l'immaginazione e si vede.

Leggere un breve testo poetico ad alta voce, soppesando ogni parola, facendolo risuonare attraverso le proprie corde vocali, la gola, la lingua, i denti. Ricostruendo il loro suono tramite il proprio, l'ADM dà corpo alle parole e si fa lui stesso opera. Come per il brano musicale, il tempo qui è quello del componimento poetico, nella sua estensione e nel suo ritmo. Bisogna suonare anche la poesia, senza spiegarla né parafrasarla. Soltanto così è possibile "sentirsi" e sentire il mistero racchiuso nella parola poetica, fatta di enigmi, metafore, ossimori, che muove ulteriori emozioni.

Comporre un'opera impiegando uno dei linguaggi dell'arte, può essere utile per allenare la creatività, e a farlo nell'unico modo costruttivo possibile, cioè prendendo confidenza con la dimensione del limite. La creatività combatte costantemente con la finitezza, trovando la propria via di uscita in una nuova finitezza che prende corpo nella forma dell'opera: apertura e limite della creatività. Per il contenuto della composizione il suggerimento è di soffermarsi sulle sensazioni e le emozioni vissute che riaffiorano dai ricordi in modo da allenare la memoria e, nel riviverle, imparare a riconoscerle. Completata l'opera, l'ADM potrebbe istruire un chatbox di AI fornendo la descrizione dettagliata del lavoro immaginato e valutare lo scarto tra il prodotto della macchina e ciò che egli ha immaginato.

Sperimentare la *Immersive Art Experience* per rafforzare le capacità sinestetiche. Nonostante questa forma di ibridazione tra la tecnica e il corpo esponga l'adolescente al rischio di assimilazione e perciò vada impiegata con la più grande cautela, risulta strategica perché implica non soltanto l'esperienza immersiva con un esteso coinvolgimento sensoriale, ma anche l'impiego di dispositivi come estensioni del corpo che sono congeniali all'ADM, nonché la compromissione dell'esperienza ludica che per lui è particolarmente attraente. In altre parole, passare per il gioco, impiegando giocattoli familiari e/o ambìti, è un modo agevole per l'adolescente di andare incontro alla propria sensibilità.

Le pratiche sin qui riportate sono soltanto alcune tra le molte possibili e variamente declinabili, ma servono a mostrare come l'ADM, condotto al suo insondato dallo stupore di ciò che sente, potrebbe cominciare a individuare la propria intimità e ad abitarla. L'adolescente che "ascolta", "osserva", "legge con la voce" ha l'occasione per trattenersi con se stesso, scartando

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

dall'intra-t-tenimento macchinico. "Sentendosi nel corpo" inizia a individuarsi e a riqualificare il proprio tempo: ad aprire le porte a un pensare più pesante (Nancy 2009), a prendere il timone della sua interazione con il digitale in modo critico, a immaginare.

5.3 Incontrare l'Altro

Più l'ADM si riappropria di sé, più l'Altro comincia ad affiorare. Si annuncia con uno straniamento, poi, a mano a mano che l'ADM si individua, prende corpo facendosi limite. L'Altro è il se stesso e il mondo fuori che torna a essere percepito, il Tu con il quale l'adolescente si relaziona.

Questo incontro che può farsi legame è il fondamento della vita associativa e della cura del vivente, ma affinché l'adolescente possa assumerne su di sé il peso è necessario che abbia la sufficiente competenza somatica, vale a dire che abbia imparato a muovere la sua comprensione e le sue azioni da un pensiero anche sensibile.

A tal fine, possiamo immaginare ulteriori pratiche.

Esercitare il tatto. Il tatto è "senso umano e reciproco, squisitamente interazionale" (Zanetti 2019, p. 122). Il con-tatto coinvolge una parte della propria intimità, *quella che tocca e da cui si viene toccati nel corpo attraverso la pelle*. "Involucro e confine, luogo del contatto e della separazione", nonché primo apparato sensoriale a svilupparsi nell'uomo (Lingiardi 2024, p. 14), la pelle riassume sul piano simbolico il senso più pieno dell'alterità come vicinanza nella distanza, o come unione nella separazione. Il tatto è gentilezza, dolcezza, carezza: approssima alla relazione con il Tu.

Un esercizio interessante è stringersi la mano. Nella liturgia cattolica è un segno di pace; nel mondo sociale sugella un patto di fiducia – il gesto che segue alla presentazione di uno sconosciuto del quale *si fa conoscenza*, il saluto dell'ospite che viene accolto e che si congeda in amicizia; in quello giuridico, la stretta di mano conclude un accordo negoziale. Il punto qui è che nel darsi la mano i due ADM si espongono reciprocamente alle tante sensazioni che giungono dal con-tatto dell'altro corpo, anche inattese. L'altra mano è fredda, umida, calda, forte, piccola, sfuggente, avvolgente. La pelle rimanda precise e reciproche informazioni di chi si è, al di là delle rappresentazioni o delle proiezioni che il proprio Io ha dell'altro, determinando, nell'intimità affiorata in ognuno, la possibilità o comunque la qualità e l'intensità della relazione con la persona alla quale si è stretta la mano e dalla quale abbiamo scartato grazie a quel tocco.

Ma è carezzevole anche la brezza del vento in un tiepido pomeriggio marino. Si esercita il tatto pure quando si presta attenzione alla piacevolezza o al fastidio che si prova nel contatto con tutto l'Altro vivente (animale, vegetale, minerale...).

Esercitare l'olfatto. "Il sistema olfattivo è collegato all'ippocampo, la parte del cervello che presiede alla memoria e, con l'amigdala e il sistema limbico, è la regione delle esperienze emotive" (Lingiardi 2024, p. 77). L'olfatto precede ogni interazione con l'Altro e ne condiziona lo sviluppo di un possibile legame. Lo svela sul piano simbolico la semantica custodita nel "fiutare". Come altre specie animali, anche noi umani ci "annusiamo" e ci orientiamo all'Altro a seconda che il suo odore ci piaccia o meno. L'olfatto è il senso che più si impone. In questo caso, l'esercizio è provare a frenare la propria reattività, e tenendo la distanza, avvicinarsi all'Altro anche quando l'odore ci respinge, attendendo il tempo che serve perché l'incontro possa divenire esperienza e pensiero consapevole. Evocando il ricordo, inoltre, l'olfatto interviene anche sulla capacità di osservare il tempo in modo prospettico: allena alla memoria e, grazie a questo accesso al tempo passato, provvede alla tensione verso il futuro.

Vale per l'olfatto quanto appena detto per il tatto quando l'Altro è il vivente. Il profumo dell'acacia può essere avvolgente e avvicinare, quanto l'odore del *surströmming* respingere. L'importante è prestare comunque attenzione.

Fare esperienza del silenzio. Il silenzio ha a che fare con l'intimità e l'ascolto. Non si tratta soltanto di tacere o di mettere a tacere, ma di imparare a fare vuoto dentro di sé: tacitare se stessi per ascoltare l'Altro e ascoltarsi nella propria intimità sollecitata da questo ascolto così radicale. Ma sappiamo bene che non è un compito facile, soprattutto per un adolescente. Un esercizio che si può proporre, anche se parte come provocazione, è l'ascolto di *4'33"* di Cage nella trascrizione per orchestra. Indispensabile in questo caso il ricorso al video affinché l'effetto sia il più possibile spiazzante. Dopo la prima manciata di secondi e i vani tentativi di far aumentare il volume del dispositivo, negli ADM si avvia lo sgomento per la costrizione al silenzio cui sono esposti. È probabile che la preoccupazione affolli i loro pensieri. Dopo un minuto, però, nel silenzio di parole e musica, comincia ad affiorare il suono del mondo: i rumori dell'impazienza dei corpi, i colpi di tosse, il turbinio del vento, una porta che sbatte, una penna che cade. Ognuno sta già ascoltando l'Altro, anche se non ne ha la consapevolezza. L'esercizio potrebbe concludersi semplicemente facendo notare quanto si è udito.

Condividere l'esperienza. "Il silenzio è presenza, ma per essere presenza deve essere presenza di qualcosa, perché nella sola presenza di se stesso esso è assente. Per questo è condivisione" (Andreotti 2014, p. 44). La pratica più intensa per l'ADM che si è fatto opera è la condivisione del suo sentire con l'altro essere umano, nella reciprocità. Si tocca anche con lo sguardo, e lo si fa silenziosamente, amplificando l'ascolto dell'altro. Nel 2010, al Moma di New York, Marina Abramović mette in opera *The Artist is Present*, forse la più famosa delle sue perfomance. Durante tre mesi, davanti alla Abramović si avvicendano quasi 1400 persone, alcune per pochi minuti, altre per un giorno intero. È un'opera basata sulla presenza all'altro. Il pubblico vi pren-

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

de parte singolarmente come co-creatore, avendo come unica indicazione quella di rimanere in silenzio e di non distogliere lo sguardo. La scena prevede due sedie e un tavolino vuoto. L'artista siede composta, in silenzio, con lo sguardo basso, mentre attende che il visitatore prenda posto davanti a lei dall'altra parte del tavolo. Il tavolo separa e unisce. È l'espressione fisica del limite[10]. L'azione prende avvio quando l'altro giunge e si siede davanti a lei. È allora che l'artista alza lo sguardo e mette i suoi occhi negli occhi dell'altro. Ed è a questo punto che l'azione diventa esperienza di presenza condivisa, che consente di addentrarsi in territori sconosciuti di sé e dell'altro, toccando i tanti sentimenti sottochiave, arrivando a volte sino al dolore. Quanto più emerge l'emozione, tanto più la presenza all'altro si fa compassione, dando spazio a un affioramento del *noi* e a una narrazione silente che unisce nella distanza. L'esercizio in questo caso consiste nel riadattare questa esperienza al livello di un gruppo di adolescenti. Nello specifico, creando coppie attraverso un sorteggio, in modo che l'altro che si ha davanti, anche se non sconosciuto, sia comunque eletto dal caso. Ogni ADM dovrebbe almeno cimentarsi, per un tempo minimo, in tre esperienze, e successivamente comparare ciò che di diverso ogni incontro ha suscitato in lui, elaborando questo vissuto in un racconto da condividere.

Queste pratiche di incontro con l'Altro sono a servizio della relazione. L'attenzione si fa più densa, il pensiero patico e riflessivo. La memoria si riattiva, consentendo al tempo di sfuggire all'eterno presente della tecnica. È l'inizio di una condivisione che consente di ragionare di legame sociale e vita in comune.

5.4 L'ultimo tassello

L'ultimo tassello è far affiorare alla consapevolezza dei giovanissimi ADM i sentimenti protogiuridici del pudore e della giustizia, per ragionare della sensibilità che cementa il legame con l'altro essere umano. La stessa che muove il senso di responsabilità e di una cura che si estendono anche oltre la relazione, nei confronti di tutto il vivente. La speranza è di colmare almeno in piccola parte il vuoto simbolico che li affligge attraverso un ancoraggio al sentire che faccia da riferimento costante nel tempestoso sviluppo che si trovano ad affrontare.

L'adolescente che avrà integrato le proprie competenze cognitive, sviluppando un pensiero anche sensibile, non avrà difficoltà a ritrovare nel proprio pudore il sentimento dei confini, capendone ora la portata. Saprà che il pudore e la giustizia sono la linfa della relazione, ciò che consente di tenere

10 Nel corso dei tre mesi l'artista decide di fare a meno del tavolo per dare maggiore spazio all'approssimarsi, mantenendo comunque la distanza dall'altro.

la giusta distanza, di trasformare lo sguardo in riguardo, di approssimarsi all'altro con dolcezza e tatto, di prestare cura anche nel silenzio. Grazie allo spazio terzo aperto dall'alterità, che permette il libero sviluppo di ognuno per chi è, l'ADM saprà individuarsi come "singolarità", senza che il legame venga meno. Potrà essere se stesso con l'Altro, facendosi carico del permanere dell'alterità in un divenire aperto al futuro.

A noi spetta soltanto impedire che venga preclusa loro la possibilità di un libero sviluppo, sostenendoli, affinché possano trovare le parole per raccontare il domani.

Bibliografia

Andreotti A., (2014), *Il silenzio non è detto*, Milano, Mimesis.

Andreotti A., (2018), *Il nascosto dell'opera Frammenti sull'eticità dell'arte*, Ancona, Italic.

Baudrillard J., (2015), *Lo scambio simbolico e la morte*, Milano, Feltrinelli.

Benasayag M., Schmit G., (2013), *L'epoca delle passioni tristi*, Milano, Feltrinelli.

Benasayag M., (2019), *Funzionare o esistere?*, Milano, Vita e pensiero.

Benasayag M., (2021), *La singolarità del vivente*, Milano, Jaca Book.

Benasayag M., Cany B., (2022), *Corpi viventi. Pensare e agire contro la catastrofe*, Milano, Feltrinelli.

Benasayag M., Cohen T., (2024), *L'epoca dll'intranquillità. Lettera alle nuove generazioni*, Milano, Vita e pensiero.

Bormetti, M., (2019), *Egophonia. Gli smartphone fra noi e la vita*, Milano, Hoepli.

Capograssi G., (1959), L'attualità di Vico (1947), in Id., *Opere*, v. 4, Milano, Giuffrè, pp. 395-410.

Centers for Disease Control and Prevention, (2024), *Youth Risk Behavior Survey Data Summary & Trends Report: 2013–2023*, U.S., Department of Health and Human Services, Youth Risk Behavior Survey Data Summary & Trends Report: 2013-2023 (ultimo accesso il 27 settembre 2025).

Cotta S., (1978), *Perché la violenza? Un'interpretazione filosofica*, L'Aquila, Japadre.

D'Agostino, F., (1979), *Per un'archeologia del diritto. Miti giuridici greci*, Milano, Giuffrè.

Damasio A., (2022), *Sentire e conoscere*, Milano, Adelphi.

Dufourmantelle A., (2022), *La potenza della dolcezza*, Milano, Vita e pensiero.

Dufourmantelle A., (2025), *L'intelligenza del sogno*, Milano, Vita e pensiero.

Galimberti U., (2013), *Il corpo*, Milano, Feltrinelli.

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

Gallese V., Morelli U., (2024), *Cosa significa essere umani? Corpo, cervello e relazione per vivere nel presente*, Milano, Cortina.
Guardini R., (1980), *Virtù*, Brescia, Morcelliana.
Han B.-C., (2015), *Nello sciame. Visioni del digitale*, Milano, Nottetempo.
Han B.-C., (2017), *L'espulsione dell'Altro*, Milano, Nottetempo.
Han B.-C., (2022), *Le non cose*, Torino, Einaudi.
Han B.-C., (2021), *La società senza dolore. Perché abbiamo bandito la sofferenza dalle nostre vite*, Torino, Einaudi.
Han B.-C., (2025), *Contro la società dell'angoscia*, Torino, Einaudi.
Gruppo HBSC-Italia, (2023), *La sorveglianza HBSC 2022. Health Behaviour in School-aged Children: principali risultati dello studio italiano tra I ragazzi di 11, 13, 15 e 17 anni*, HBSC - Schede Sintesi.pdf - Google Drive (ultimo accesso il 27 settembre 2025).
ISTAT, (2025), *Bambini e ragazzi: comportamenti, atteggiamenti e progetti futuri* - Anno 2023, Bambini e ragazzi: comportamenti, atteggiamenti e progetti futuri – Istat (ultimo accesso il 27 settembre 2025).
Jedlowski P., (2000), *Storie comuni. La narrazione nella vita quotidiana*, Milano, BrunoMondadori.
Kidron B., Rudkin A., (2023), *Digital Chilhood. Addressing Childhood Development Milestones in the Digital Environment*, 2nd edition, 5Rights Foundation, Digital-Childhood-Report-2023.pdf (ultimo accesso il 27 settembre 2025).
Lancini M., (2019), a cura di, *Il ritiro sociale negli adolescenti. La solitudine di una generazione iperconnessa*, Milano, Cortina.
Lancini M., Zanella T., (2019), *Internet. Nuove normalità e nuove dipendenze*, in Lancini M., a cura di, *Il ritiro sociale negli adolescenti. La solitudine di una generazione iperconnessa*, Milano, Cortina, pp. 21-36.
Limone G., (2019), *Il pudore, la responsabilità. Il* Protagora *di Platone interroga i tempi contemporanei?*, in Id., a cura di, *Il pudore delle cose, la responsabilità delle azioni*, Quaderno n. 11-*L'era di Antigone*, Milano, Angeli, pp. 7-74.
Lingiardi V., (2024), *Corpo, umano*, Torino, Einaudi.
Manfré G., (2018), *Il disagio delle generazioni*, in Corradini A., Manfré G., *Diventare ciò che si è. Educazione e società*, Bologna, I libri di Emil.
Marzano M., (2010), *La filosofia del corpo,* Genova, Il Nuovo Melangolo.
Masullo A., (2003), *Paticità e indifferenza*, Genova, Il melangolo.
McLuhan M., (2008), *Gli strumenti del comunicare*, Milano, Il Saggiatore.
Mittica M.P., (2016), *In-opera. Forme e alterità*, in Foi M.C., a cura di, *Per una critica della giustizia: testi letterari e contesti storici a confronto*, Trieste. EUT, pp. 152-159.
Mittica M.P., (2022), *Il pensiero che sente*, Torino, Giappichelli.
Mortali C., Mastrobattista L., Palmi I., Solimini R., Pacifici R., Pichini S., Minutillo A., (2023), *Dipendenze comportamentali nella Generazione Z:*

uno studio di prevalenza nella popolazione scolastica (11-17 anni) e focus sulle competenze genitoriali, Roma: Istituto Superiore di Sanità (Rapporti ISTISAN 23/25), ISTITUTO SUPERIORE DI SANITÀ (ultimo accesso il 27 settembre 2025).

Nancy J.-L., (2004), *Corpus*, Napoli, Cronopio.

Nancy J.-L., (2009), *Il peso di un pensiero. L'approssimarsi*, Milano-Udine, Mimesis.

Orazi M., (2020), *Del pudore. Per una filosofia dell'alterità e della misura*, Torino, Giappichelli.

Prete A., (2013), *Compassione. Storia di un sentimento*, Torino, Bollati Boringhieri.

Save the Children, (2023), Atlante dell'infanzia (a rischio) in Italia 2023 "Tempi digitali", Layout 1 (ultimo accesso il 27 settembre 2025).

Savona P.F., (2005), In limine juris. *La genesi* extra ordinem *della giuridicità e il sentimento del diritto*, Napoli, Edizioni Scientifiche Italiane.

Scognamiglio M.R., Russo S.M., (2018), *Adolescenti digitalmente modificati (ADM). Competenza somatica e nuovi setting terapeutici*, Milano, Mimesis.

Sgorlon A., (2024), *Relazioni connesse. Come essere felici nell'era digitale*, Centro di Formazione e Salute Digitale, Youcanprint.

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.

Tagliapietra A., (2006), *La forza del pudore*, Milano, Rizzoli.

WHO Regional Office for Europe, (2025), *European health report 2024: keeping health high on the agenda. Highlights*, Copenhagen, content (ultimo accesso il 27 settembre 2025).

Zanetti G., (2019), *Filosofia della vulnerabilità*, Roma, Carocci.