(Cyber)sicurezza e infanzia digitale. Oltre la protezione, verso un uso critico e consapevole della tecnologia *

Raffaella Brighi, Valeria Ferrari

Introduzione

Negli ultimi decenni, un numero impressionante di studi ha analizzato gli effetti della tecnologia digitale su bambini e adolescenti [1]. Questi studi hanno migliorato enormemente la nostra comprensione di tale relazione, mostrando come i più giovani possano essere influenzati dai media e dalle tecnologie in modo sia positivo sia negativo. Tuttavia, il rapido sviluppo di prodotti tecnologici mirati proprio ai più giovani impone di rafforzare ulteriormente questa indagine, mossa

* Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU. In particolare, le autrici partecipano al progetto EcoCyber (*Risk management for future cyber-physical ecosystems*), coordinato dall'Università di Bologna, che ha l'obiettivo principale di proporre nuovi metodi e approcci alla gestione del rischio cyber, necessari per garantire la sicurezza, la continuità operativa e l'incolumità fisica, essenziali per la società futura. Una linea di ricerca del progetto è dedicata a promuovere una cultura della sicurezza cyber per sviluppare comportamenti corretti a livello individuale e un approccio consapevole alla sfera digitale.

[1] Tanto che esistono riviste scientifiche interamente dedicate al tema, quali, in ambito internazionale, *Journal of Children and Media* (https://www.tandfonline.com/journals/rchm20/about-this-journal#aims-and-scope) e *International Journal of Child-Computer Interaction* (https://www.sciencedirect.com/journal/international-journal-of-child-computer-interaction).

da preoccupazioni non solamente teoriche ma assai concrete. Le tecnologie e i media che un bambino nato alla fine degli anni '90 incontrava in casa, infatti, non sono le stesse in cui si imbatte un bambino nato nel 2020. Anzi, i cambiamenti sono stati enormi per un periodo di tempo relativamente breve. Cosa comporta questa differenza? Quali vantaggi portano i nuovi strumenti a disposizione? Quali sono i pericoli per i più piccoli? Come cambiano gli adulti del domani con il cambiare delle tecnologie che ne accompagnano la crescita?

Per garantire la tutela dei minori in quanto soggetti vulnerabili di fronte all'innovazione guidata da interessi economici, e per salvaguardare un continuum, una comunicabilità tra una generazione e l'altra, è necessario che uno sforzo critico sia tenuto vivo, tramandato, portato avanti nel tempo, nutrito dai saperi e dalle inquietudini, vecchie e nuove, di molteplici ambiti disciplinari.

Non sorprende che il tema del rapporto tra giovani e tecnologia abbia acquisito importanza in molteplici campi di studio accademico. Nell'ambito della psichiatria e della medicina pediatrica, ad esempio, sono innumerevoli gli studi sugli effetti dell'uso dei media sul disturbo da deficit di attenzione e iperattività (ADHD) [2]. I neuroscienziati stanno cercando di stabilire se l'uso dei media provochi cambiamenti nelle aree cerebrali responsabili del comportamento aggressivo [3], mentre la sociologia studia le dinamiche delle culture giovanili e il comportamento degli adolescenti nelle reti sociali online [4].

D'altronde, è evidente che la ricerca su giovani e tecnologia richiede un approccio interdisciplinare che integri le conoscenze e le teorie di diverse discipline [5]. Per comprendere gli effetti della tecnologia sui bambini e sugli adolescenti, abbiamo bisogno di conoscere le teorie sullo sviluppo cognitivo e socioaffettivo dei giovani, poiché è proprio questo sviluppo a plasmare l'uso della

[2] Si veda ad esempio: M. SETTANNI, D. MARENGO, M.A. FABRIS, C. LONGOBARDI, *The interplay between ADHD symptoms and time perspective in addictive social media use: A study on adolescent Facebook users*, in "Children and Youth Services Review", 89, 2018, pp. 165-170; Y. HARTNETT, E. CUMMINGS, *Social media and ADHD: implications for clinical assessment and treatment*, in "Irish Journal of Psychological Medicine", 41, 2024, pp. 132-136; T. SIEBERS, I. BEYENS, P.M. VALKENBURG, *The effects of fragmented and sticky smartphone use on distraction and task delay*, in "Mobile Media & Communication", 12, 2024, pp. 45-70.

[3] Su questi profili, da ultimo: S. LIN, C. LONGOBARDI, F.G.M. GASTALDI, M.A. FABRIS, *Social Media Addiction and Aggressive Behaviors in Early Adolescents: The Mediating Role of Nighttime Social Media Use and Sleep Quality*, in "The Journal of Early Adolescence", 44(1), 2024, pp. 41-58.

[4] In merito: F. ANGELI, *L'identità corporea digitalizzata: l'utilizzo dei social media nella costruzione dell'immagine di Sé di adolescenti e giovani adulti*, in "Sociologia del diritto", 1, 2022, pp. 34-55.

[5] Come dimostrano, ad esempio, i contributi di BARBARA G. BELLO, *Digital Technologies and Children's Rights: Balancing Control, Protection, and Consent*, in "Revista De Derecho Privado", 48, 2025, pp. 19-45 e di M. MARTONI, *Persuasive Design Technologies, Dark Patterns and the Rights of Children and Adolescents. Online video games as a first area of analysis*, in "Federalismi.it", 14, 2023, pp. 162-179.

tecnologia e i suoi effetti. Domande di tipo tecnico-legali, pertanto, non potranno prescindere da riflessioni provenienti da altri settori di studio che definiscono le effettive cause e conseguenze di un particolare rapporto tra un bambino o adolescente e i *digital devices* che gli vengono messi a disposizione.

Con l'obiettivo di riflettere e in parte riassumere la complessità che caratterizza il tema del rapporto minori-tecnologia, il presente contributo ripercorre i principali movimenti dell'industria tecnologica degli ultimi anni, illustrando gli aspetti, le declinazioni, le applicazioni dei prodotti tecnologici che più hanno destato interesse nella comunità scientifica da un punto di vista socio-umanistico. La trattazione identifica, in particolare, due diversi approcci al problema, che corrispondono a differenti, anche se comunicanti, gruppi di discipline scientifiche: il primo di questi comprende la psicologia dei media e gli studi culturali, impegnati a identificare gli effetti di determinate configurazioni degli ambienti e degli strumenti digitali sul comportamento, sulla psicologia e sulla vita dei giovani. La seconda, di natura tecnico-legale, opera in modo più trasversale rispetto alle singole applicazione tecnologiche: prende atto dei profili di rischio legati a queste ultime e organizza strumenti giuridici e tecnologici per tutelare il soggetto, in questo caso la persona di minore età, che utilizza le tecnologie a scopo ricreativo e, soprattutto, educativo.

La riflessione riassume questi diversi approcci evidenziando come alla base di entrambi debba esserci un comune atteggiamento anti-deterministico che si oppone al mantra dell'ottimizzazione e della velocità proposte dal mercato della tecnologia; di fronte a un soggetto doppiamente vulnerabile come un minore, infatti, è necessario sollevare dubbi su un'industria tecnologica la cui tendenza è quella di inglobare sempre più attività, al fine di *datificare* e monetizzare ogni ambito della vita.

Questo sguardo critico deve informare strumenti giuridici, tecnologici ed educativi che aiutino a tutelare i giovani che si muovono negli ambienti online.

1. Due decenni di internet in casa: i contributi degli studi culturali e della psicologia dei media sulla relazione minori-tecnologia

Lo studio degli effetti dei media e della tecnologia su bambini e adolescenti è ben più antico di internet. Già a partire dagli anni '60 del Novecento, negli Stati Uniti, i *cultural studies* e la psicologia dei media si interessano agli effetti dello schermo, della pubblicità, e in generale della somministrazione dei mass-media ai minori [6]. Le prime ricerche sugli effetti sociali di internet, invece, sono state

[6] P.M. Valkenburg, J.T. Piotrowski, *Plugged In – How Media Attract and Affect Youth*, Yale University Press, Yale, 2017.

pubblicate, sempre negli Stati Uniti, nel 1998 [7]. A quel tempo, internet era principalmente appannaggio degli *early adopters* e solo una piccola percentuale di bambini era online. Il dibattito pubblico su internet si è acceso solo intorno al 2002, quando i tassi di accesso sono aumentati drasticamente e la maggioranza dei giovani americani ed europei era già online. I ricercatori hanno allora iniziato a studiare l'accesso dei giovani a internet: i risultati di questi studi hanno rivelato un quadro più sfumato di quanto molti si aspettassero, aprendo questioni – rilevanti ancor di più oggi – sugli effetti del tempo trascorso online sull'autostima, sulla relazione con il proprio corpo e l'immagine di sé [8] (un aspetto fondamentale per gli adolescenti), sulle competenze sociali, sui comportamenti sessuali, sul rischio di cyberbullismo [9], sul sonno e, più in generale, il benessere psico-fisico [10].

La questione del rapporto tra tecnologia e minori si amplia oggi con l'aumento e la sofisticazione delle tecnologie che entrano nel quotidiano dei giovani. Se negli anni '90 i bambini e gli adolescenti spendevano in media quattro ore al giorno tra tv, radio e telefono, oggi le interazioni con la tecnologia sono molto più lunghe, frequenti e importanti, con lo sviluppo di applicazioni destinate a ragazzi e bambini di età sempre inferiore.

A complicare lo studio della materia vi è il fatto che le piattaforme e i social media dominanti vengono sostituiti da altri con una rapidità impressionante, e i giovani tendono a essere proprio i primi e i più veloci a cambiare. Se nel 2015 praticamente tutti gli adolescenti avevano un account su Facebook, oggi la demografia del colosso della tecnologia è cambiata: gli utenti più giovani sono già altrove – essi si spostano rapidamente da una piattaforma all'altra, sperimentando in ciascuna di esse diverse modalità di interagire, socializzare, esporsi, informarsi e formarsi online [11].

I cambiamenti nel panorama mediatico non sono dovuti solo allo sviluppo di nuove tecnologie, ma anche alla riproposizione dei media tradizionali attraverso

[7] *Ibidem*.

[8] J.M.F. VAN OOSTEN, L. VANDENBOSCH, J. PETER, *Predicting the use of visually oriented social media: The role of psychological well-being, body image concerns and sought appearance gratifications*, in "Computers in Human Behavior", Advance online publication, 2023.

[9] CHILDREN IN THE DIGITAL ENVIRONMENT REVISED TYPOLOGY OF RISKS – OECD DIGITAL ECONOMY PAPERS, No. 302, January 2021. Si veda inoltre il contributo di Marco Mondello in questo stesso volume.

[10] S.R. SUMTER, S.E. BAUMGARTNER, W. WIRADHANY, *Beyond screentime: a 7-day mobile tracking study among college students to disentangle smartphone screentime and content effects on sleep*, in "Behaviour & Information Technology", 44(6), 2024, pp. 1-17.

[11] Sul tema minori e social media, si veda, ad esempio: S. STEINSBEKK, O. BJØRKLUND, P. VALKENBURG, J. NESI, L. WICHSTRØM, *The new social landscape: Relationships among social media use, social skills, and offline friendships from age 10-18 years*, in "Computers in Human Behavior", 2024, 156, pp. 108-235; A. VAN DER WAL, P.M. VALKENBURG, I.I. VAN DRIEL, *In Their Own Words: How Adolescents Use Social Media and How It Affects Them*, in "Social Media and Society", 10(2), 2024, pp. 1-11, https://doi.org/10.1177/20563051241248591.

modelli di business e infrastrutture di distribuzione nuove. I giovani consumano i media in modo diverso da come lo potevano fare nei decenni precedenti: guardano quello che vogliono quando vogliono, consumano contenuti su piattaforme di vario genere, per ore e ore, facendo "binge watching", fino a poco fa su YouTube, oggi sempre di più su servizi di streaming a pagamento (dominante è il modello c.d. *freemium*) come Netflix o Apple TV. Anche per quanto riguarda l'informazione e l'apprendimento di notizie, gli adolescenti e i giovani hanno abbandonato le fonti tradizionali e ricorrono a fonti online, in particolare il social media TikTok [12].

Poi c'è il mondo del *gaming*. La tecnologia *touch-screen*, l'utilizzo del cloud, la connettività wi-fi uniti alla formula *freemium* (cioè applicazioni scaricabili gratuitamente e basate su pubblicità e "acquisti in-app"), hanno dato al gioco un'impennata di popolarità. Non solo negli ultimi anni è stata normalizzata l'interazione dei più piccoli con lo schermo a scopo ricreativo e di intrattenimento, ma il gaming non è più una nicchia nemmeno per gli adulti: i parametri del coinvolgimento nei videogiochi si sono espansi con il gioco online in modalità multiplayer e in livestreaming, dando luogo a veri e propri siti di socialità, interazione virtuali e comunità create attorno al gioco. Si può dire che il mondo del *gaming* sia stato il vero campo di prova del metaverso, e che quest'ultimo si sviluppi proprio a partire da pratiche iniziate nel mondo del *gaming*, quali personaggi virtuali, avatar, monetizzazione di oggetti digitali e creazione di sistemi di valore all'interno di una piattaforma [13].

La letteratura esistente ha principalmente valutato come l'esposizione ai contenuti dei videogiochi influisce sul funzionamento sociale e comportamentale. Vari studi hanno osservato come la partecipazione alle comunità di gioco online sia associata a comportamenti problematici (in particolare si è osservata la tendenza attorno ad alcuni giochi ad estremizzare la performatività di un certo modello di mascolinità aggressiva, e la frequenza di comportamenti c.d. "tossici") [14] e sintomi del c.d. "disturbo da gioco su Internet" (GD – *gaming disorder*) [15].

[12] Sul punto: TH. CASADEI, *TikTok: A Legal Perspective on the Digital Environment, Highly Accessed by Minors*, in "Revista de derecho Privado", 48, 2024, pp. 87-116.

[13] UNICRI Centre for AI & Robotics, *Gaming and the Metaverse-The Alarming Rise of Online Sexual Exploitation and Abuse of Children Within the New Digital Frontier*, The Hague, ed. in West Hollywood (CA), 2022.

[14] F. DONNER, *Structures that tilt: Understanding "toxic" behaviors in online gaming*, in "New Media & Society", 2024, pp. 1-20.

[15] J.S. LEMMENS, I.A. WEERGANG, *Caught them all: Gaming disorder, motivations for playing and spending among core Pokémon Go players*, in "Entertainment Computing", 45, 2023; D. LIU, J. LEMMENS, X. HONG, B. LI, J. HAO, Y. YUE, *A network analysis of internet gaming disorder symptoms*, in "Psychiatry Research", 311, 114507, 2022; L.S. LEMMENS, *Play or pay to win: Loot boxes and gaming disorder in FIFA ultimate team. Telematics and Informatics Reports*, 8, 2022; J.S. LEMMENS, M. SIMON, S.R. SUMTER, *Fear and loathing in VR: the emotional and physiological effects of immersive games*, in "Virtual Reality", 1, 2022, pp. 223-234.

Inoltre, i dati hanno mostrato che i giocatori più giovani, i giocatori di genere femminile o non bianchi sono più vulnerabili rispetto ai comportamenti problematici e ai sintomi più gravi del GD [16]. Tali studi possono essere utili per sviluppare uno sguardo critico sui rischi sia del gaming che del metaverso per i più giovani, in cui già sono stati denunciati episodi di violenza a danno di soggetti vulnerabili [17].

Soprattutto a partire dalla pandemia, è poi in forte aumento lo sviluppo di strumenti di *e-learning* che sfruttano i recenti progressi nel campo della tecnologia, inclusi quelli nel campo dell'intelligenza artificiale, per sostenere genitori e insegnanti nei compiti educativi e nelle attività scolastiche.

Nel campo della ricerca sull'intelligenza artificiale, numerosi studi si concentrano sull'interazione tra bambini e assistenti virtuali, inclusi chat bots e social robot, osservando il modo in cui i bambini tendono ad antropomorfizzare l'intelligenza artificiale, e valutando le effettive potenzialità degli strumenti di AI nello sviluppo cognitivo [18].

In Italia, l'investimento statale nel "digitale" e nella "digitalizzazione" è alquanto entusiastico [19]; tale entusiasmo si nutre a volte di una retorica tecnodeterministica che deve essere adeguatamente stemperata da considerazioni, giustamente riflesse in ampia dottrina nazionale e internazionale degli ultimi anni, quali l'impatto ambientale dell'intelligenza artificiale e la sostenibilità, i problemi di *ownership* dei dati e il controllo delle infrastrutture critiche, i *bias* intrinseci al *machine learning* e le possibili discriminazioni, il c.d. *digital divide* [20].

---

[16] E. GANDOLFI, R.E. FERDIG, K. KRAUSE, I. SOYTURK, G. MORRI, S. DELAHANTY, *An exploration of why gaming communities may make younger and non-normative gamers vulnerable to Internet Gaming Disorder*, in "New Media & Society", 2023, pp. 1-19.

[17] Si veda ad esempio il discusso caso: I. DODA, *Una ricercatrice ha subito una violenza sessuale nel metaverso*, in "Wired", 2022: https://www.wired.it/article/metaverso-violenza-sessuale-ricercatrice/.

[18] J. PETER, R. KÜHNE, A. BARCO *et al.*, *Asking today the crucial questions of tomorrow: social robots and the internet of Toys*, in G. MASCHERONI, D. HOLLOWAY (eds.), *The internet of Toys*, Springer, Cham, 2019, pp. 25-46; F. MANZI, G. PERETTI, C. DI DIO *et al.*, *A robot is not worth another: exploring children's mental state attribution to different humanoid robots*, in "Front Psychol", 11, 2020, pp. 1-12; CL. VAN STRATEN., J. PETER, R. KÜHNE, *Child–Robot relationship formation: a narrative review of empirical research*, in "International Journal of Social Robotics", 12, 2020, pp. 325-344; R. VAN DEN BERGHE, M. HAAS, O. OUDGENOEG-PAZ *et al.*, *A toy or a friend? Children's anthropomorphic beliefs about robots and how these relate to second-language word learning*, in "J Comput Assist Learn", 37, 2021, pp. 396-410.

[19] Si pensi all'obbiettivo del PNRR di "Sviluppare la didattica digitale e formare alla transizione digitale", che prevede lo stanziamento di fondi in infrastrutture, competenze e personale che permettano di sfruttare le novità tecnologiche offerte dal panorama aziendale nelle scuole.

[20] Su quest'ultimo profilo: S. VANTIN, *Il diritto antidiscriminatorio nell'era digitale: potenzialità e rischi per le persone, la pubblica amministrazione, le imprese*, Wolters Kluwer, Milano, 2021. Più in generale sulle varie problematiche accennate: S. AMATO, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020; F. PASQUALE, *Le nuove leggi della robotica. Difendere*

Gli anni della pandemia hanno infatti aumentato fortemente il ricorso agli strumenti per il lavoro e l'istruzione "in remoto". In un'ottica di superamento della retorica dello '*smart working*', i critici hanno elaborato nozioni per comprendere fenomeni quali la Zoom fatigue, il deficit di attenzione causato dall'eccesso di informazione, la discriminazione algoritmica riscontrata negli strumenti di *e-learning* che devono essere presi in considerazioni nello sviluppo e nell'adozione di tecnologie all'interno di istituti educativi [21].

Queste critiche non vogliono negare la possibilità di aspetti positivi che la disponibilità di nuove tecnologie può offrire al minore. I ricercatori che studiano l'interazione tra pari online sono interessati non solo al cyberbullismo, ma anche al fatto che i social media possano rappresentare per gli adolescenti un luogo in cui esercitarsi e sviluppare le loro abilità sociali. Oltre a chiedersi se l'uso precoce dei media possa essere dannoso per lo sviluppo cerebrale, i ricercatori contemporanei cercano di stabilire se l'uso precoce delle app educative possa favorire l'apprendimento. Tuttavia, tali vantaggi possono essere legittimamente riconosciuti soltanto se si adotta un approccio che si distanzi dalla retorica del determinismo tecnologico e prenda atto dei rischi oltre che dei benefici della digitalizzazione. In quest'ottica, l'adozione degli strumenti tecnologici non deve essere vista come un'inevitabile fatalità, ma come *un'opzione*; la digitalizzazione non come un obiettivo in sé, ma come strumento per il raggiungimento di determinati obiettivi.

2. Vulnerabilità della persona di minore età e tutela giuridica: i rischi delle piattaforme digitali tra disinformazione, *data protection* e profilazione

Quanto illustrato sin qui dimostra che l'ambiente commerciale che circonda i giovani sta vivendo cambiamenti profondi. Se, da un lato, si aprono possibilità di mercato, dall'altro, emerge sempre di più quanto le logiche di accumulazione di dati e monetizzazione della presenza online (strategie di marketing che puntano a "incollare" l'utente allo schermo per più tempo possibile) da parte di poche potenti piattaforme sollevino dubbi di legittimità sotto molteplici punti di vista.

Sono diverse le normative adottate negli ultimi due decenni a livello sia europeo (General Data Protection Regulation, Digital Market Act, Digital Service

la competenza umana nell'era dell'intelligenza artificiale, LUISS University Press, Roma, 2021; S. SALARDI, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, Giappichelli, Torino, 2023; F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in "Federalismi.it", 11, 2020, pp. 85-110; B.G. BELLO, *(In)Giustizie digitali. Un itinerario su tecnologie e diritti*, Pacini Giuridica, Pisa, 2023.

[21] In una letteratura in espansione si può vedere: E. FALLETTI, *Discriminazione algoritmica: una prospettiva comparata*, Giappichelli, Torino, 2023.

Act) sia nazionale volte a contrastare i rischi insiti nell'espansione del nuovo mercato digitale verso modelli sempre più chiusi e monopolistici.

Proprio dalle normative di settore emerge la persona di minore età inquadrata come soggetto doppiamente vulnerabile: sia in quanto consumatore, utente di servizi per natura poco trasparenti e caratterizzati da una forte disparità di potere, sia appunto in quanto minore, aprendo quindi la necessità di trovare meccanismi di tutela di fronte a un'offerta di prodotti tecnologici in continuo cambiamento.

In primis, si delineano le problematiche relative alla tutela della privacy e alla protezione dei dati personali dei minori.

Nelle fasi della crescita e dello sviluppo le tecnologie diventano importanti nel processo di autodeterminazione, in quanto le piattaforme digitali, entrate a far parte sempre più intensamente della vita dei bambini e dei ragazzi, offrono nuovi percorsi per esplorare e sviluppare la propria identità personale. Il mondo digitale è il luogo in cui bambini e ragazzi imparano, si intrattengono, coltivano relazioni e partecipano alla vita sociale e civica [22]. In questo contesto, la condivisione di un'immagine reale online, ad esempio, non è vista come un rischio, ma come un mezzo per comunicare e affermare il proprio sé agli altri. È facile dunque immaginare la mole dei dati condivisi dai più giovani online, più o meno consapevolmente.

Il Regolamento Generale sulla Protezione dei Dati (GDPR) [23] ha rappresentato un passo significativo rispetto a questo fenomeno, riconoscendo la maggiore vulnerabilità dei soggetti più giovani negli ambienti digitali, in quanto «meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali» e richiamando perciò la necessità di una protezione specifica per «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» [24].

Tuttavia, nonostante l'introduzione di misure mirate – quali il riconoscimento di un'età minima per il consenso, libero e informato, alle attività di trattamento [25] e l'imposizione di requisiti rafforzati in termini di semplicità, trasparenza e accessibilità delle informazioni fornite ai minori in merito ai loro diritti e alle

[22] M. MARTONI, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in "Federalismi.it", 1, 2020, pp. 119-136.

[23] Regolamento (UE) 2016/679.

[24] GDPR, Considerando 38.

[25] Il GDPR dispone all'art. 8 che il consenso per aderire ad un servizio della società dell'informazione che implichi un trattamento di dati personali sarà espresso dal minore a partire dal sedicesimo anno di età, ma gli Stati membri possono abbassare questa soglia fino a 13 anni (in Italia il limite è 14 anni), oppure da chi esercita la responsabilità genitoriale se il minore ha una età inferiore al limite stabilito.

modalità di trattamento dei dati – tale tutela si rivela spesso insufficiente [26]. I giovani sono *datificati* sin dalla nascita, o anche da prima, e il GDPR lascia i bambini particolarmente vulnerabili alla diffusione dei loro dati attraverso la condivisione online da parte dei genitori e tutori (*sharenting*) [27]; tra questi molti non ne comprendono le implicazioni oppure non hanno le competenze digitali necessarie per proteggere la privacy dei propri figli.

Del resto, oggi è evidente la facilità con cui i dati personali riferibili alle persone di minore età possono essere raccolti, elaborati e utilizzati per alimentare sistemi di apprendimento automatico finalizzati a processi di profilazione a carattere predittivo o prescrittivo, esponendo concretamente il minore ai rischi intrinseci alla natura stessa della società dell'informazione quali pratiche di sorveglianza comportamentale e diffusione di disinformazione e *fake news* [28]. In questo contesto, la profilazione può degenerare in forme subdole di manipolazione e sfruttamento commerciale: i minori, infatti, sono bersaglio privilegiato di strategie pubblicitarie personalizzate e di tecniche persuasive opache – i cosiddetti *dark pattern* [29] – che rischiano di compromettere la loro autonomia decisionale, indebolendone la capacità critica e inducendo scelte di consumo poco consapevoli. A ciò si aggiunge la tendenza a rinchiudere gli utenti in bolle informative autoreferenziali, all'interno delle quali si amplificano *bias* cognitivi e disinformazione, favorendo una visione del mondo parziale e potenzialmente fuorviante, cui i più giovani risultano particolarmente vulnerabili.

Ai problemi legati alla trasparenza dei servizi e la diffusione della disinformazione hanno cercato di rispondere le più recenti normative europee, tra cui il Digital Market Act (DMA) [30] e il Digital Service Act (DSA) [31], due strumenti giuridici con cui si cerca di regolamentare e porre dei limiti di legittimità a pratiche commerciali tipiche del modello piattaforma.

Il DMA riconosce gli squilibri di potere tipici del mercato digitale identificando le figure dei 'gatekeeper' (ad oggi: Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft), e obbligando gli stessi a garantire che gli utenti possano accedere ai dati sulle prestazioni delle campagne pubblicitarie e alle informazioni sui prezzi degli annunci, consentire agli sviluppatori di utilizzare sistemi di pagamento in-

[26] Il tema della protezione dei dati dei minori rispetto ai servizi della società dell'informazioni è affrontato in modo ampio in dottrina, *ex multis* F. Di Tano, *Minori, consenso privacy e vulnerabilità online: riflessioni alla luce del Regolamento generale sulla protezione dei dati (UE) 2016/679*, in "Notizie di Politeia", 35/136, 2019.

[27] Su questo specifico aspetto si rinvia al contributo di Michele Balbinot in questo stesso volume.

[28] In merito si veda il contributo di Casimiro Coniglione in questo stesso volume.

[29] P. Perri, *I dark patterns tra tecniche di manipolazione degli utenti e protezione dei dati personali*, in "Notizie di Politeia", 38, 147, 2022, pp. 93-111.

[30] Regolamento (UE) 2022/1925.

[31] Regolamento (UE) 2022/2065.

app alternativi e prevedere opzioni di interoperabilità per i sistemi di messaggistica. Il DSA ha invece come obiettivo principale quello di prevenire le attività illegali e dannose online e la diffusione della disinformazione.

Proprio sulla base del DSA e dei nuovi poteri di *enforcement* sui social media previsti dalla legge, nel 2024 la Commissione europea ha avviato un procedimento formale per valutare se TikTok possa aver violato la legge in aree legate alla protezione dei minori, alla trasparenza della pubblicità, all'accesso ai dati per i ricercatori, nonché alla gestione del rischio di creare dipendenza e contenuti dannosi.

Sulla base delle indagini preliminari, compresa l'analisi del rapporto di valutazione dei rischi inviato da TikTok nel settembre 2023, nonché delle risposte di TikTok alle richieste formali di informazioni della Commissione circa i contenuti illegali, la protezione dei minori e l'accesso ai dati, la Commissione ha deciso di avviare un procedimento formale contro l'azienda per valutare la legittimità dei sistemi algoritmici, che possono stimolare dipendenze comportamentali e/o creare i cosiddetti "effetti rabbit hole". Tale valutazione – afferma la Commissione – è necessaria per contrastare i potenziali rischi per l'esercizio del diritto fondamentale al benessere fisico e mentale della persona, il rispetto dei diritti dei minori e l'impatto sui processi di radicalizzazione. Inoltre, la Commissione valuta le misure di mitigazione in atto, in particolare gli strumenti di verifica dell'età utilizzati da TikTok per impedire l'accesso dei minori a contenuti inappropriati (c.d. *age verification*). Si menziona inoltre il rispetto degli obblighi posti dal DSA di mettere in atto misure appropriate e proporzionate per garantire un elevato livello di privacy, sicurezza e protezione dei minori, in particolare per quanto riguarda le impostazioni di privacy predefinite per i minori nell'ambito della progettazione e del funzionamento dei loro sistemi di raccomandazione; il rispetto degli obblighi del DSA di fornire un archivio ricercabile e affidabile per le pubblicità presentate, le misure adottate per aumentare la trasparenza della piattaforma.

L'iniziativa della commissione – tutt'altro che isolata: procedimenti ai sensi del DMA sono infatti stati avviati nel marzo del 2024 anche contro Alphabet, Apple e Meta [32], anche se non riguardano in modo specifico la tutela dei minori – dimostra la consapevolezza da parte delle istituzioni europee rispetto ai rischi posti dalle Big Tech americane, e offre un esempio di come il legislatore possa elaborare strumenti capaci di responsabilizzare i fornitori di servizi digitali prendendo in considerazioni le specificità dei rischi posti dagli stessi [33].

[32] EU COMMISSION – DIRECTORATE-GENERAL FOR COMPETITION, DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY, *Press Release: Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act* (https://digital-markets-act.ec.europa.eu/commission-opens-non-compliance-investigations-against-alphabet-apple-and-meta-under-digital-markets-2024-03-25_en).

[33] Sul dibattito sul tema: R. JAHANGIR, *Tracking Recent Statements on the Enforcement of EU Tech Laws*, Tech Policy Press, 2025; https://digital-markets-act.ec.europa.eu/commission-opens-non-compliance-investigations-against-alphabet-apple-and-meta-under-digital-markets-2024-03-25_en.

3. Cyber minacce e (in)sicurezza online: verso una tutela del minore *by design*

La verifica dell'età degli utenti in sede di accesso alle piattaforme online costituisce una delle questioni più complesse in tema di protezione dei minori [34]. I sistemi di *age verification* si occupano di stabilire l'età dell'utente del servizio digitale, onde evitare che un minore fruisca di contenuti non destinati a lui e potenzialmente dannosi. Nella pratica, tuttavia, numerosi ragazzi riescono ad accedere a contenuti e servizi digitali inadeguati con un semplice *click*, senza che dall'altra parte si attui un controllo effettivo sull'idoneità del potenziale fruitore.

Questa lacuna di sicurezza, unita alle molteplici vulnerabilità tipiche di ecosistemi digitali complessi, incide negativamente sulla protezione dei minori, esponendoli a una serie di minacce che spazia dai crimini tradizionali a nuove forme di persecuzione e aggressione, come adescamento online, truffe ed estorsioni, cyberbullismo [35]. Il rapporto del OCSE "*Children in the digital environment: Revised typology of risks*", aggiornato nel 2021 [36], individua quattro tipologie di rischio che possono avere una vasta portata sulla vita di bambini e ragazzi: i) i rischi legati ai contenuti, ii) i rischi legati ai contatti, iii) i rischi legati alle condotte e iv) i rischi dei consumatori. Il rapporto UNICRI, istituto di ricerca delle Nazioni Unite, del 2022 ha approfondito le prime tre categorie di rischio negli ambienti di gaming e nei mondi virtuali [37].

I rischi relativi ai contenuti riguardano l'esposizione a materiale inappropriato o illegale, come immagini esplicite a sfondo sessuale, pornografia, contenuti violenti, razzisti o discriminatori, disinformazione e discorsi d'odio, oltre a siti che promuovono comportamenti dannosi (sfide pericolose, autolesionismo, anoressia) [38]. I rischi di contatto emergono quando un bambino interagisce con adulti

[34] Oltre alle complessità tecniche e applicative dell'operazione, l'adozione di sistemi di identificazione elettronica e di verifica dell'età implica anche attività di trattamento dei dati personali (ai sensi dell'art.4 GDPR) e conseguentemente l'esigenza di rispettare i principi generali di necessità e minimizzazione dei dati personali raccolti. Si veda, *ex multis*, M. MARTONI, *Sistemi di* age verification. *Una prima esplorazione fra salvaguardia dell'interesse prioritario del minore e protezione dei dati personali*, in "Cyberspazio e diritto", 24, 75 (3) 2023, pp. 307-322.

[35] Per un approfondimento si rinvia al contributo di Marco Mondello in questo stesso volume.

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

[37] Lo studio di UNICRI, intitolato *Gaming and the Metaverse* e pubblicato nel mese di novembre del 2022, è disponibile in internet all'indirizzo https://unicri.it/Publication/Gaming-and-the%20Metaverse.

[38] Si veda, M. MARTONI, *I diritti dei minori e i rischi connessi all'esposizione a contenuti on-line pericolosi. Primi spunti per una riflessione etico-giuridica sulla protezione prioritaria del minore quale presupposto di una società moderna sostenibile*, in "Notizie di Politeia", 37, 2021, pp. 91-107.

che ricercano relazioni inadeguate o scopi sessuali, o con persone che esprimono opinioni estreme e cercano di spingerlo verso comportamenti pericolosi o radicalizzazione. I rischi di condotta, infine, si verificano quando il minore stesso genera o contribuisce a contenuti rischiosi, ad esempio creando immagini sessualizzate, diffondendo immagini sessuali di terzi senza consenso o producendo contenuti d'odio contro altri bambini [39].

Questi rischi risultano ulteriormente amplificati dalla presenza di molteplici vulnerabilità e minacce cyber, dall'assenza di misure di sicurezza adeguate – come, ad esempio, sistemi efficaci di verifica dell'età – dalla mancanza di sistemi interni alle piattaforme di segnalazione e blocco, e dalla carenza di controlli e supervisione da parte delle famiglie e degli educatori.

Le tecnologie avanzate, infatti, sono vulnerabili a numerose minacce informatiche – compromissione dei sistemi e delle reti, *phishing*, *malware*, *social engineering*, furto di identità e l'uso improprio dell'intelligenza artificiale [40] – che, in ambienti immersivi e virtuali, assumono forme particolarmente sofisticate e pervasive. Nelle piattaforme qualificate come *metaversi* (i cosiddetti mondi virtuali), dove tutto ruota attorno alle identità digitali, tali vulnerabilità possono compromettere direttamente la sicurezza fisica e il benessere degli individui, alterando dinamiche sociali e relazionali.

La compromissione dei dispositivi cyber-fisici – quali visori per la realtà virtuale, sensori di movimento e interfacce aptiche, che fungono da punti di accesso alle piattaforme di *gaming* – consente all'attaccante di manipolare l'esperienza immersiva, estendendo potenzialmente l'intrusione anche alla sfera emotiva e corporea dell'utente. Gli avatar, autentiche estensioni digitali dell'identità personale, diventano bersagli privilegiati per attacchi finalizzati al furto d'identità, alla clonazione e alla manipolazione. Il grado di anonimato offerto da tali ambienti favorisce l'instaurarsi di relazioni con sconosciuti e l'emergere di comportamenti aggressivi [41].

Considerato che tali problematiche hanno già impatti significativi sul mondo degli adulti, appare ancora più urgente garantire un elevato livello di sicurezza

[39] In argomento, F. DI TANO, *Hate speech e molestie in rete. Profili giuridici e prospettive de iure condendo*, Aracne, Roma, 2019. In particolare, sulla diffusione di immagini sessuali di terzi senza consenso, si veda il contributo di Valeria Barone in questo stesso volume.

[40] I report pubblicati da associazioni e agenzie istituzionali in materia di cybersicurezza evidenziano un continuo incremento delle minacce e del numero di incidenti informatici significativi a livello globale. Tra tutti, ENISA, *Threat Landscape* 2024; Relazione annuale (2023) al Parlamento della Agenzia per la Cybersicurezza nazionale; Rapporto Clusit 2024 sulla sicurezza ICT.

[41] EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Metaverse: Opportunities, risks and policy implications*, 2022. Per una riflessione etico giuridica si veda, A. IANNUZZI, *Metaverso, Digital Twins e diritti fondamentali*, in "Rivista italiana di informatica e diritto", 6, 2, 2024, pp. 36-55; W. D'AVANZO, *Il Metaverso. Le nuove frontiere della tecnologia tra etica e diritto*, Rubbettino, Soveria Mannelli (CZ), 2025.

per i dispositivi, i sistemi e i servizi destinati soprattutto a bambini e ragazzi. La sicurezza dei bambini rimane, però, trascurata da gran parte delle piattaforme. Se è vero che il legislatore, di fronte al crescente numero di vittime, non ha esitato a introdurre strumenti di tutela molto forti, è anche vero che queste misure proteggono il minore *a posteriori*, cioè quando il fatto è già stato commesso e il minore ha subito il danno. È quindi necessario impostare il sistema di protezione in modo diverso.

In questo contesto, la "Strategia Nazionale di Cybersicurezza" del 2021, coordinata da ACN – Agenzia Nazionale per la Cybersicurezza [42], alla misura 73 del suo Piano di implementazione, prevede la messa in campo di una strategia nazionale autonoma, con relativo piano d'azione, dedicata «alla protezione online dei minori dai crimini informatici, che includa iniziative quali la realizzazione di campagne di sensibilizzazione rivolte non solo ai minori, ma anche a genitori, tutori ed educatori» [43].

Un primo elemento di preoccupazione è senza dubbio l'educazione e la sensibilizzazione, che possono essere realizzate solo con il coinvolgimento delle famiglie e di tutti coloro che partecipano all'educazione digitale dei minori. Esempi virtuosi in questa direzione sono i cosiddetti "patti per l'educazione digitale", intesi come "patto di corresponsabilità" tra famiglie, scuole, enti locali e, più in generale, il mondo dell'associazionismo, per dare regole chiare ai ragazzi e alle ragazze [44].

Un ulteriore elemento di preoccupazione è l'efficacia delle misure tecniche volte a proteggere i minori quando accedono a una determinata piattaforma.

A questo proposito le piattaforme possono ridurre frodi, abusi sessuali, molestie online e altri reati integrando nell'architettura stessa dei giochi l'approccio della *security by design*, vale a dire prevedendo sin dall'inizio funzionalità concepite per tutelare gli utenti. In tale prospettiva, la protezione e la sicurezza dei minori diventano l'elemento cardine attorno a cui sviluppare l'intero sistema. Tra le soluzioni più immediate figurano: (i) un'effettiva verifica dell'età, (ii) il controllo esercitato da genitori o familiari, (iii) l'adozione di meccanismi interni di

[42] L'Agenzia, che è il cardine della infrastruttura italiana di cybersecurity, è stata istituita con il d.l. 82/2021 e organizzata con il d.p.c.m. 223/2021.

[43] L'Italia ha rivisto la sua Strategia di cybersecurity nel 2022, prevedendo il raggiungimento di 82 misure entro il 2026. In particolare, le misure 59-70 si concentrano sull'educazione, mentre le misure 71-73 sono incentrate sulla promozione di una cultura della cybersecurity. Quest'ultima serie di misure riguarda in generale iniziative volte a promuovere un comportamento responsabile nel cyberspazio, a combattere la disattenzione digitale e a sensibilizzare sui rischi dell'uso delle tecnologie digitali. Sullo sfondo di queste riflessioni rimangono le questioni critiche legate al *digital divide*, o *onlife divide*, cioè non solamente l'esclusione dalla sola dimensione della connettività, ma dalla vita sociale nel suo complesso.

[44] In merito si veda il contributo di Claudia Severi in questo stesso volume. Per ulteriori approfondimenti; M. Gui, B. Fiore, S. Garassini, M. Grollo, S. Lanza, *I Patti Digitali: un approccio comunitario all'educazione mediale*, in "Comunicazionepuntodoc", 28, 2023, pp. 81-104.

segnalazione e blocco di contenuti e comportamenti illeciti e (iv) una moderazione efficace delle attività, eventualmente supportata dall'intelligenza artificiale [45].

A fronte degli sforzi compiuti dalle autorità competenti per applicare i sistemi di verifica dell'età [46], l'Autorità per le Garanzie nelle Comunicazioni (AGCOM) con la delibera 9/2023 – entrata in vigore il 21 novembre 2023 – ha adottato specifiche Linee Guida per gli ISP per la corretta implementazione dei sistemi di "parental control" [47]. In particolare, sono state individuate diverse categorie di siti web che gli operatori devono filtrare. Tra questi, i siti con contenuti pornografici; quelli che forniscono informazioni o promuovono il gioco d'azzardo o la vendita di armi; quelli che presentano o promuovono la violenza, l'odio e la discriminazione, le sette o le pratiche dannose per la salute; quelli che forniscono strumenti e metodi per rendere l'attività online non rintracciabile. Sul fronte della verifica dell'età, invece, di recente pubblicazione è il provvedimento, posto in consultazione pubblica dall'AGCOM con delibera 61/24/CONS al fine di addivenire ad un documento condiviso circa gli strumenti attuali e successivamente approvato, con il quale l'Autorità ha delineato le caratteristiche che i sistemi di verifica dell'età devono implementare, proponendone uno specifico modello [48]. Non vi è, tuttavia, allo stato delle cose, una soluzione tecnico-giuridica pronta e di agevole attuazione. Le difficoltà sono molteplici e così le esigenze da contemperare e le ambiguità da superare [49].

Nello scenario attuale, un tassello fondamentale è rappresentato dalla formazione di genitori, familiari e di tutte le figure incaricate di guidare le persone di minore età nel loro percorso digitale. L'adozione di strumenti sempre più

[45] G. ZICCARDI, *I minori online tra videogiochi e metaverso*, in "Ciberspazio e diritto", 3, 2023, pp. 325-338.

[46] Autorità Garante per la protezione dei dati personali, Provvedimento del 22 gennaio 2021 [9524194] che impone una limitazione immediata al trattamento effettuato da TikTok in relazione ai dati degli utenti di cui non è stato possibile stabilire con certezza l'età; Provvedimento del 30 marzo 2023 [9870832] che impone una limitazione temporanea immediata al trattamento dei dati degli utenti italiani da parte di OpenAI anche in relazione alla mancanza di meccanismi di verifica dell'età. Da ultimo, Provvedimento del 2 novembre 2024 [10085455] con il quale il Garante sanziona OpenAI per diverse violazioni del GDPR. In particolare, il Garante ha ritenuto che la mancata adozione di sistemi di verifica dell'età integrasse una violazione degli artt. 24 e 25 GDPR. Si veda, sul punto, P.G. CHIARA, *Italian DPA Fines OpenAI for GDPR Non-Compliance: The Last Episode of the Garante – OpenAI Saga?*, in "European Data Protection Law Review", 11, 1, 2025 (*forthcoming*).

[47] Per un primo commento: TH. CASADEI, C. CONIGLIONE, B. ROSSI, C. SEVERI, *Al via il "nuovo" Parental Control. Ma serve anche più cultura*, in "Agenda Digitale", 21 novembre 2023: https://www.agendadigitale.eu/sicurezza/privacy/minori-online-al-via-il-nuovo-parental-control-system-ma-serve-anche-piu-cultura/.

[48] Si veda L.M. LUCARELLI TONINI, *Strumenti di* age verification *alla luce del contributo del Garante privacy e dell'AGCOM: il rischio di obsolescenza tecnologica e conoscitiva*, in "Rivista Italiana di Informatica e Diritto", 2, 2024, pp. 435-447.

[49] M. MARTONI, *Sistemi di Age Verification*, cit.

sofisticati, i rapidi mutamenti del contesto tecnologico e i persistenti divari digitali rendono ancora più complesso il compito affidato agli adulti.

La Commissione europea, nell'ultima Strategia UE in materia di cybersicurezza [50], insiste particolarmente sulla necessità di investire nell'educazione e nella sensibilizzazione. In Italia, la Strategia nazionale di cybersicurezza mira a sviluppare diversi programmi di formazione sulla cybersecurity a diversi livelli (ad esempio, corsi specifici nelle scuole superiori e nelle pubbliche amministrazioni), un sistema di certificazione nazionale per valutare le conoscenze e le competenze in materia di cybersecurity e uno strumento di formazione e sensibilizzazione online rivolto al grande pubblico per l'autoverifica delle competenze acquisite. In una società digitale, una cultura della cybersecurity dovrebbe essere imperativa.

Conclusioni

Le discipline che storicamente si dedicano allo studio degli effetti sociali e psicologici dei media hanno precocemente dimostrato come i bambini e gli adolescenti siano particolarmente influenzati dall'esposizione alla tecnologia. Tali studi hanno subito un'impennata negli ultimi due decenni, quando la diffusione di internet ha portato l'interazione col mondo digitale nel quotidiano dei minori. Il presente contributo ha mappato le preoccupazioni attuali che guidano la ricerca scientifica sul problema, in relazione al crescente utilizzo dei social media, al gaming e all'emergere dei c.d. "metaversi", alla diffusione di tecnologie a scopo educativo, inclusa l'intelligenza artificiale a sostegno dell'insegnamento e della genitorialità.

A fronte di tali preoccupazioni il legislatore europeo adotta strumenti giuridici – sia trasversali rispetto alle tecnologie (come nel caso del GDPR, del DMA e del DSA) che specifici (ad esempio, l'AI Act [51]) – che prendono atto delle problematiche sottostanti l'industria tecnologica contemporanea, enfatizzando la necessità di un maggior grado di tutela quando gli utenti siano soggetti minori di età.

Il già citato rapporto dell'OCSE aggiornato al 2021 [52], riconosce quanto l'ambiente digitale sia fondamentale nella vita dei bambini, offrendo loro un maggiore accesso all'istruzione e alle relazioni sociali. Nel fare ciò, l'OCSE registra anche i rischi che esso comporta, tra cui l'aumento del *cyberbullying* e la violazione della privacy dei bambini a causa di condotte quali lo *sharenting*. Pertanto, sottolinea l'importanza di progettare prodotti online che siano sicuri per i bambini per

[50] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020), 18 final.

[51] Regolamento (UE) 2024/1689.

[52] Si veda la nota 33.

impostazione predefinita; invita i legislatori ad addottorare ed aggiornare strumenti giuridici a difesa del minore nel mondo digitale, e le comunità ad assicurare la *digital literacy* dei bambini e dei ragazzi nonché a disporre misure tutela *by design*.

In questa prospettiva si muovono, come accennato, iniziative quali i patti educativi digitali: un approccio al problema della tecnologia che non passa solo dalla regolamentazione *top-down*, ma dall'educazione collettiva, dal coinvolgimento della comunità nella formazione e nella prevenzione dei rischi e dalla responsabilizzazione, al contempo, di adulti e minori.

In una visione più ampia, numerosi interventi legislativi, sia a livello europeo sia nazionale, nonché politiche e piani di investimento dedicati, promuovono un approccio coordinato e globale alla cybersicurezza [53]. Per garantire un cyberspazio sicuro è necessario adottare paradigmi di comunità o olistici, in cui un quadro normativo solido si affianca a misure tecniche avanzate – sostenute da controlli rigorosi e standard ben definiti – e a una diffusa consapevolezza dei rischi e dei valori in gioco. La cybersicurezza, dunque, emerge come una *sfida collettiva* che richiede la partecipazione attiva di tutti i portatori di interesse [54].

L'attenzione al problema da parte del legislatore e della comunità civica sono senz'altro un'importante passo verso la tutela del singolo, e in particolare della persona di minore età, di fronte a un'industria tecnologica che tende a massimizzare il tempo passato online a scapito di autonomia, informazione e trasparenza del consumatore. La *digital literacy* è oggi giustamente posta tra gli obiettivi principali dell'istruzione. Gli studi più recenti, tuttavia, dimostrano che non sempre la conoscenza dello strumento può bastare a evitare le trappole (i c.d. *dark patterns*; i meccanismi di gratificazione volti a generare dipendenza, ecc.) che in esso sono inscritte [55].

La promozione di strumenti che facilitino l'educazione digitale e l'adozione di tecnologie a beneficio dei più piccoli non deve, pertanto, prescindere da considerazioni sugli interessi che muovono lo sviluppo di tali tecnologie, nonché le conseguenze delle stesse sul benessere sociale e psicologico dei minori.

[53] In merito si veda il contributo di Pier Giorgio Chiara in questo stesso volume.

[54] Per un'analisi del concetto di cybersecurity, V. PAPAKONSTANTINOU, *Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?*, in "Computer Law & Security Review", 44, 2022, pp. 1-15; M. TADDEO, *Is Cybersecurity a Public Good?*, in "Minds and Machines", 29, 3, 2019, pp. 349-354; R. BRIGHI, P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in "Federalismi.it", 21, 2021, pp. 18-42; G. ZICCARDI, *La Cybersecurity nel quadro tecnologico (e politico) attuale*, in G. ZICCARDI, P. PERRI, *Tecnologia e Diritto*, 3 voll., Giuffrè Francis Lefebvre, Milano, 2019, vol. III, pp. 207-210; S. PIETROPAOLI (a cura di), *Cybersecurity*, Epieikeia, Torino, 2025.

[55] Sul punto, si veda M. MARTONI, *Un'autonomia ostacolata. Limiti cognitivi, incompetenze e design ingannevoli nella trasformazione digitale*, in "Sociologia del diritto", 51, 1, 2024, pp. 7-32.