ISSN 2281-5147

LA TUTELA DEL MINORE NELL'ERA DELL'INTELLIGENZA ARTIFICIALE: QUESTIONI APERTE SUL METODO DI GESTIONE DEL RISCHIO

Matilde Ratti*

Abstract

La diffusione di sistemi di intelligenza artificiale evidenzia la crescente esigenza di individuare soluzioni di protezione per il minore e i suoi diritti. Sul punto, le diverse normative volte alla tutela dei minori *online*, sia nell'uso di strumenti di intelligenza artificiale sia nella fruizione dei *social network* o nel trattamento dei dati personali, presentano approcci eterogenei riconducibili a differenti metodologie regolatorie. Sono numerosi i punti di contatto tra le criticità affrontate dai provvedimenti sull'impiego di strumenti dotati di intelligenza artificiale, di protezione dei dati personali e di uso dei *social network*. Anche a livello normativo, dal modello statunitense, alla legislazione australiana alla recente normativa italiana, le principali questioni attengono al grado di effettività delle misure individuate nella gestione del rischio per i minori nell'ambiente digitale.

The wide application of artificial intelligence systems highlights the growing need to identify solutions to protect minors and their rights. In this regard, the various regulatory initiatives aiming to protect minors in the digital environment, including both those related to the use of artificial intelligence tools, and the use of social networks, and the processing of personal data, highlight heterogeneous approaches answering to different regulatory methodologies. There are indeed several points of contact between the critical issues addressed by the provisions on the use of artificial intelligence tools, personal data protection, and the use of social networks. Even at the regulatory level, from the US model to Australian framework, and the recent Italian legislation, the main issues concern the degree of effectiveness of the measures identified in managing risks for minors in the digital environment.

* Professoressa Associata di diritto privato, Università di Bologna, matilde.ratti@unibo.it
Il presente contributo è stato sottoposto a referaggio a doppio cieco ed è finanziato su progetto *Children as Vulnerable Users of IoT and AI-based Technologies: A Multi-level Interdisciplinary Assessment* – CURA, PRIN 2022–2022KAEWYF, – Next Generation EU; CUP: J53D23005540006.

ISSN 2281-5147

Indice Contributo

Keywords

Minore – Intelligenza Artificiale – Protezione dei Dati Personali – Piattaforme Digitali – Age Verification

1. Il minore e l'accesso agli strumenti dotati di intelligenza artificiale

La crescente consapevolezza circa gli effetti dell'uso dei dispositivi che consentano l'accesso ad Internet, ai *social media* e ai sistemi dotati di intelligenza artificiale sta

ISSN 2281-5147

plasmando lo scenario politico-legale sul tema del minore che agisce *online*[1]. Alcune tematiche suscitano un particolare interesse poiché presentano evidenti rischi per il minore in quanto tale e, tra queste, vi è certamente quella connessa alla possibilità di avere rapido accesso agli strumenti dotati di intelligenza artificiale. Sul piano internazionale, il Comitato sui diritti dell'infanzia delle Nazioni Unite è intervenuto con il Commento Generale n. 25 esplicitamente estendendo l'ambito di applicazione dei diritti del fanciullo ad Internet (e alle nuove tecnologie) e ribadendo la doverosa attenzione da prestare alla fragilità ontologicamente connessa alla natura del minore[2]. Sebbene tale approccio sia penetrato in certa misura negli atti normativi dell'Unione Europea[3], confermando la rilevanza del tema nell'attuale cultura legislativa, non vi è ad oggi una disciplina europea specificamente rivolta alla protezione del minore che

[1] Tra le più recenti opere che affrontano in modo specifico il tema, cfr. D. Amram, *Non ho l'età ma… Costruire competenze abilitanti per una società dell'informazione a prova di (in)capacità del minore di età* (1° ed., Lefebvre Giuffré 2025); C. Camardi, 'Relazione di filiazione e *privacy*. Brevi note sull'autodeterminazione del minore' (2018) 5 Jus Civ 831ss.; R. Senigaglia, 'L'identità personale del minore di età nel cyberspazio tra autodeterminazione e *parental control system'* (2023) 6 NLCC, 1568ss.; G. Carapezza Figlia, '*Sharenting*: nuovi conflitti familiari e rimedi civili' (2023) 5 NGCC 1104ss.; A. La Spina, 'L'identità del minore nella realtà on-life tra protezione e autodeterminazione' (2024) 10 Famiglia e Diritto, 920ss.; I. Garaci, 'Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale' (2021) 4 NLCC, 800ss.; M. Giandoriggio, 'I minori d'età e i social network: l'insostenibile leggerezza del post' (2024) 3 Danno e resp. 296ss.; I. Garaci, 'La *privacy* del minore d'età nell'ambito familiare' (2023) 1 EJPLT 84ss.; L. Lenti, 'L'identità del minorenne' (2006) 1 NGCC 68ss.; E. Moscati, 'Il minore nel diritto privato, da soggetto da proteggere a persona da valorizzare (contributo allo studio "interesse del minore")' (2014) 10 Dir. fam. pers. 1141ss.

[2] Comitato sui diritti dell'infanzia, *Commento generale n. 25: Sui diritti dei minorenni in relazione all'ambiente digitale,* 2022 <I diritti dei minorenni in relazione all'ambiente digitale | UNICEF Italia> ultimo accesso 1 settembre 2025.

[3] Alcune delle enunciazioni contenute in tale Commento sono state recepite anche nei considerando del Digital Services Act (DSA). In particolare, il considerando 71 sottolinea che la protezione dei minori costituisce un obiettivo politico prioritario dell'Unione europea e definisce le condizioni in cui una piattaforma *online* può considerarsi accessibile ai minorenni, richiedendo ai prestatori l'adozione di misure appropriate e proporzionate, anche attraverso interfacce progettate secondo logiche di *privacy* e sicurezza "*by design*" e "*by default*". In stretta connessione, il considerando 81 stabilisce che le piattaforme e i motori di ricerca di dimensioni molto grandi sono tenuti a considerare, nell'analisi dei rischi sistemici, l'impatto delle proprie interfacce e dei propri servizi sui diritti del minore, con particolare attenzione ai possibili effetti pregiudizievoli sullo sviluppo fisico, mentale e morale, nonché ai meccanismi che possono sfruttare l'inesperienza o la vulnerabilità dei minorenni. Infine, il considerando 89 riafferma la necessità di modellare il *design* dei servizi digitali nel rispetto del superiore interesse del fanciullo e prevede che i meccanismi di tutela e di ricorso offerti dal regolamento siano resi effettivamente accessibili anche ai soggetti minorenni. Tali previsioni riprendono e traducono in chiave normativa europea alcune delle linee direttrici poste dal Commento Generale n. 25, che insiste sulla necessità di una protezione specifica dei minori nell'ambiente digitale, nonché sul riconoscimento del loro diritto a strumenti adeguati, trasparenti e accessibili di partecipazione e tutela.

ISSN 2281-5147

utilizzi sistemi di intelligenza artificiale. Infatti, sebbene il Regolamento europeo 2024/1689 (l'*AI Act*) vieti l'impiego di sistemi che sfruttino le vulnerabilità (anche quando siano connesse all'età)[4] e preveda obblighi di valutazione del rischio che tengano conto la natura dell'utilizzatore[5], il tema del minore non è trattato in modo specifico né è oggetto di una disciplina dedicata. Ci si propone, dunque, di valutare l'opportunità di un approccio organico alla tutela dei diritti del minore partendo da un'analisi delle più rilevanti decisioni in materia e indagando, in seguito, le potenzialità e le criticità delle primissime soluzioni giuridiche adottate nell'ordinamento italiano e in altri Stati che, in modo più o meno diretto, si sono interessati al tema[6].

2. La protezione dei dati personali volta alla tutela del minore che interagisca con strumenti di IA

Nello scenario italiano, i primi provvedimenti ad interessarsi della tutela del minore che adoperi strumenti dotati di intelligenza artificiale sono proprio quelli del Garante per la protezione dei dati personali, che ha indagato l'opportunità di implementare sistemi di verifica dell'età (o *age verification*) per l'accesso a servizi *online* allo scopo di limitare la potenziale violazione dei diritti del minore. Ci si riferisce in primo luogo al noto provvedimento del 2 febbraio 2023[7], avente ad oggetto il sistema *Replika*, una *chatbot* intelligente che genera un "amico virtuale" a supporto del benessere emotivo dell'utente, a più riprese oggetto dell'attenzione del Garante. Nel caso in commento,

[4] Cfr. AI Act, art. 5, par. 1, lett. b), Peraltro, l'art. 7 dell'*AI Act* attribuisce alla Commissione il potere di adottare atti delegati per modificare i casi d'uso dei sistemi di IA ad alto rischio se questi presentano « un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali» (cfr. lett. b) del par. 1) anche tenendo conto del criterio secondo il quale «esiste uno squilibrio di potere o le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto al *deployer* di un sistema di IA, in particolare a causa della condizione, dell'autorità, della conoscenza, della situazione economica o sociale o dell'età» (par. 2, lett. h).

[5] Cfr. AI Act, art. 9, par. 9.

[6] EDPB, *Linee guida 8/2020 sul targeting degli utenti di social media* (2021). In dottrina, ampiamente in G. Finocchiaro, *Intelligenza Artificiale. Quali regole?,* (1ª ed., Il Mulino 2024); G. Finocchiaro, 'La proposta di Regolamento sull'Intelligenza Artificiale: il modello Europeo basato sulla gestione del rischio' (2022) 2 Dir. inform. Inf. 303ss.; G. Finocchiaro, 'Il perfezionamento del contratto on line: opportunità e criticità' (2018) 1-2 Dir. com. scambi internaz., 187ss.; G. Finocchiaro, *La protezione dei dati personali in Italia – Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* (1ª ed., Zanichelli Editore 2019).

[7] *Provv. del 2 febbraio 2023* [2023] GPDP 9852214, Registro dei provvedimenti n. 39 del 2 febbraio 2023.

ISSN 2281-5147

l'Autorità aveva evidenziato la necessità che il *provider* adottasse dei meccanismi di verifica dell'età per consentire l'utilizzo della *chatbot*[8]. La società implementava dunque un meccanismo di *age gate* in tutte le pagine di registrazione, prevedeva un periodo di raffreddamento (*cooling-off period*) e predisponeva strumenti per consentire agli interessati l'esercizio effettivo dei propri diritti[9]. Due anni dopo, tali misure erano giudicate insufficienti con il provvedimento del 10 aprile 2025[10], che chiariva la prospettiva giuridica adottata dall'Autorità. Considerato che proprio secondo le ricostruzioni della Società il servizio sarebbe stato destinato a soli maggiorenni, il trattamento dei dati del minore avrebbe violato il generalissimo principio di minimizzazione previsto dal Regolamento 2016/679 (in seguito semplicemente "GDPR"). Il trattamento avrebbe inoltre violato gli obblighi di *accountability* incombenti sul *provider* (art. 24 del GDPR) e avrebbe comportato l'ingiusta esposizione del minore ad un servizio inadeguato alla sua età[11].

Un'analoga posizione era emersa anche nel 2024 in riferimento ad un altro provvedimento storico della medesima Autorità, quello avente ad oggetto il servizio di ChatGPT[12]. In questo caso, il Garante rilevava la mancanza di un sistema per

[8] La registrazione, infatti, richiedeva unicamente l'inserimento di nome, indirizzo *e-mail* e genere, senza alcuna procedura di *age verification*. Il Garante aveva inoltre rilevato la mancanza di un sistema di moderazione dei contenuti calibrato in base all'età dell'utente, con la conseguenza che i minorenni risultavano esposti a materiali non adeguati al loro grado di sviluppo. Per completezza, si segnala altresì che in mancanza di informativa sul trattamento dei dati personali l'Autorità ha segnalato l'impossibilità di comprendere le modalità del trattamento e la base giuridica dello stesso. Sul punto, il Garante ha escluso che, per i minori, la base giuridica potesse rinvenirsi nell'accettazione delle condizioni di utilizzo, stante l'incapacità legale a contrarre per la fruizione del servizio.

[9] La misura della limitazione del trattamento ordinata dall'Autorità era in seguito sospesa dal medesimo Garante. *Provvedimento del 22 giugno 2023* [2023] GPDP 10013893, Registro dei provvedimenti n. 280 del 22 giugno 2023.

[10] Cfr. *Provvedimento del 10 aprile 2025* [2025] GPDP 10130115, Registro dei provvedimenti n. 232 del 10 aprile.

[11] Cfr. *ivi*: «Nello specifico, la mancata adozione da parte della Società di misure idonee a salvaguardare l'accesso e l'utilizzo del servizio Replika aveva comportato non solo che Luka trattasse, sistematicamente, dati personali ulteriori rispetto a quelli realmente necessari per conseguire la finalità del trattamento (vale a dire offrire il servizio ad utenti maggiorenni), ma anche che tale trattamento riguardasse dati relativi a soggetti vulnerabili (minorenni, potenzialmente di età anche inferiore ai 13 anni) che, a causa di tale carenza ed attesa la tecnologia innovativa sottesa al servizio e la natura altamente sensibile delle conversazioni fornite dal chatbot, sono stati esposti ad un rischio particolarmente elevato».

[12] *Provvedimento del 2 novembre 2024* [2024] GPDP 10085455, Registro dei provvedimenti n. 659 del 2 novembre 2024. La decisione si inserisce a chiusura della vicenda che aveva coinvolto la Società OpenAI in relazione ai trattamenti di dati personali condotti tramite la sua IA *ChatGPT*. Con primo provvedimento del 30 marzo 2023, doc. web n. 9870832, il Garante aveva comminato la sanzione di limitazione del trattamento dei dati personali degli interessati stabiliti in Italia sulla base di una serie di violazioni intercorse. Spiccavano, in particolare, un *data breach* avvenuto nel marzo 2023, consistente nella visualizzazione da parte degli utenti del servizio di dati personali appartenenti ad altri utilizzatori; l'assenza di informativa adeguata sul sito *web* e la mancanza di meccanismi per garantire i diritti di opposizione e cancellazione degli interessati; l'assenza di base giuridica del trattamento per l'addestramento degli algoritmi sottesi al funzionamento della piattaforma. La sanzione

ISSN 2281-5147

verificare la provenienza del consenso dall'esercente la responsabilità genitoriale[13], consenso richiesto dal *provider* proprio per utilizzare il servizio[14]. Da un lato, l'obbligo di verifica dell'età era posto in capo al titolare del trattamento, ovverosia il *provider*: questi avrebbe dovuto verificare l'età dell'utente con la necessaria diligenza. Dall'altro, l'Autorità ammetteva che il contratto stipulato tra l'infraquattordicenne (con il permesso del genitore) e il *provider* per l'uso del servizio *ChatGPT* potesse costituire un'idonea base giuridica per trattare i dati personali del minore ai sensi del GDPR. Inoltre, pur considerando le diverse caratteristiche del servizio rispetto a quello esaminato nel provvedimento in precedenza richiamato, il Garante anche in questo caso evidenziava il rischio di esposizione del minore a contenuti inappropriati[15] ed individuava quale soluzione sostanziale l'imposizione di un vincolo di accesso a ChatGPT tramite la precostituzione di un idoneo meccanismo di *age verification*.

3. La protezione dei dati e la tutela del minore nell'accesso ai *social network*: profili di analogia

Nel medesimo periodo in cui il Garante italiano affrontava le questioni sul minore che acceda a strumenti dotati di intelligenza artificiale, negli Stati Uniti d'America era

comminata era stata poi sospesa con *Provvedimento dell'11 aprile 2023*, 874702, a seguito dell'adozione di misure organizzative e tecniche da parte della società volte ad adeguare il trattamento dei dati personali alle previsioni normative.

[13] Ancora a titolo di completezza, interessante la replica della Società, avallata dal Garante, che, con riferimento alla mancata adozione di misure idonee per verificare il consenso prestato dai minori, nega l'applicazione dell'art. 8 GDPR in quanto la base giuridica del trattamento non sarebbe rinvenibile tanto nel consenso degli interessati, quanto nell'esecuzione di un contratto ai sensi dell'art. 6 lett. b) GDPR.

[14] La decisione, a ben vedere, si pone in contraria direzione rispetto a quanto l'Autorità stessa aveva in precedenza stabilito nel citato Provvedimento del 2 febbraio 2023 in relazione al servizio Replika. In quell'occasione, il Garante aveva escluso *a priori* che la base giuridica potesse rinvenirsi nell'esecuzione di adempimenti nell'ambito di un contratto concluso con l'utente, stante l'incapacità del minore a contrarre nell'ordinamento.

[15] Con riguardo alle modalità di verifica dell'età, la società aveva vagliato alcune misure correttive, quali l'inserimento dei dati di una carta di credito, l'introduzione di appositi meccanismi di IA in grado di misurare l'età, la scansione della carta di identità prima dell'accesso al servizio. OpenAI aveva infine deciso di affidare l'attività ad una società esterna (Yoti), la quale avrebbe restituito ad OpenAI solo l'esito positivo o negativo della verifica previo autoscatto dell'utente e scansione di un documento di identità. Tale sistema è stato tuttavia giudicato insufficiente dall'Autorità. In aggiunta, per ciò che qui interessa ai fini della delineazione di un sistema di responsabilità in merito all'accesso al servizio da parte di minore, si evidenzia che la sanzione è stata comminata al titolare per aver mantenuto esposti i minori al rischio di contenuti inappropriati per un determinato periodo di tempo. Non è peraltro accolta la posizione di OpenAI che imputa alla mancanza di *standard* uniformi sulle misure più idonee per la tutela dei minori, ritenendo il Garante che la responsabilità di individuare le soluzioni idonee alla tutela del minore caso per caso ricada sul titolare del trattamento.

ISSN 2281-5147

adottato il Provvedimento della *Federal Trade Commission* del 2 agosto 2024[16] sull'adeguatezza del trattamento di dati personali di minori svolto dalla Bytedance, proprietaria di TikTok, alle disposizioni del *Children's Online Privacy Protection Act* (COPPA, 15 U.S.C. 6501) e del *Children's Online Privacy Protection Rules* (16 C.F.R. Part 312). Seppur adottato nei confronti di un *social network*, il provvedimento appare incentrato su un tema assai vicino a quello in esame, avendo ad oggetto il trattamento automatizzato dei dati personali degli utenti minorenni (anche con finalità di *marketing*). Nel *social* era consentito che minori di 13 anni creassero *account* personali. In particolare, al momento dell'apertura del profilo erano raccolti nomi, indirizzi *e-mail*, numeri di telefono e immagini, dati successivamente ritenuti eccedenti rispetto a quanto consentito dalla normativa applicabile. Secondo quanto evidenziato dalla *Federal Trade Commission*, infatti, la Sezione 312.4(c) delle COPPA *Rules* prevedeva che il *provider* potesse raccogliere solo alcuni dati del minore prima di ottenere il consenso da parte dell'esercente la responsabilità genitoriale e, comunque, solo al fine di consentire il funzionamento del servizio. Inoltre, come nei casi oltreoceano, era rilevato che il sistema di verifica dell'età dell'utente fosse facilmente aggirabile tramite, ad esempio, una falsa dichiarazione di età o accedendo al *social* attraverso piattaforme terze (come Google o Instagram) che non prevedevano, a loro volta, rigidi sistemi di verifica dell'età[17]. Il procedimento, ancora pendente presso la *Federal Trade Commission* e dall'esito è incerto, pone il problema – se non ancora dal punto di vista legislativo, quantomeno in via di valutazione di opportunità sociale – della possibilità per il minore di agire liberamente in rete sui *social network* e lascia emergere la stretta connessione esistente tra le preoccupazioni avanzate dall'Autorità per la protezione dei dati personali italiana nei confronti dei prestatori di sistemi di IA e la *Federal Trade Commission* in relazione ai prestatori di *social network*. Il fulcro di entrambe le questioni sta proprio nell'applicazione del principio di minimizzazione del trattamento dei dati e nell'appropriatezza degli strumenti normativi e tecnici previsti nell'ipotesi in cui il minore possa accedere ad ambienti virtuali ove, a seconda del caso specifico, potrebbero anche essere utilizzati sistemi di intelligenza artificiale.

[16] Federal Trade Commission, *Provvedimento Bytedance ltd, Us v.* (2024), <https://www.ftc.gov/legal-library/browse/cases-proceedings/bytedance-ltd-us-v> ultimo accesso 17 settembre 2025

[17] È stata inoltre rilevata la mancanza di un'informativa adeguata che spiegasse quali dati personali dei minori trattasse e per quale finalità, violando le Sezioni 312.3(a) e 312.4(d) delle COPPA Rules e non è stato richiesto il consenso da parte dei genitori, violando così le Sezioni 312.3(b) e 312.5(a)(1) COPPA Rules

ISSN 2281-5147

Dell'assenza di misure per la tutela dei minori nei *social network* si sono interessati anche altre autorità per la protezione dei dati personali. In particolare, nell'agosto 2022, l'Autorità irlandese aveva adottato un progetto preliminare di decisione[18] nei confronti di TikTok Technology Limited riguardante l'assenza di strumenti in grado di proteggere il minore sulla piattaforma. Il progetto di decisione si concentrava sulla possibile violazione di alcune delle norme in materia di protezione dei dati personali previste dal GDPR[19]. In particolare, l'Autorità irlandese rilevava la mancanza di un sistema di *parental control*, l'assenza di informazioni circa la diffusione dei contenuti pubblicati dai minori e la carenza di protezione dei profili da questi creati, impostati di *default* come *account* "pubblici" e tramite un sistema di verifica dell'età consistente nella semplice dichiarazione espressa dall'utente al momento dell'iscrizione. A seguito delle osservazioni poste da TikTok sul progetto di provvedimento, l'Autorità irlandese condivideva il progetto anche con l'Autorità tedesca e con quella italiana, le quali presentavano alcune obiezioni[20]. L'Autorità irlandese deferiva dunque la controversia all'EDPB, che interveniva con decisione vincolante[21]. Era così stabilito che la società avesse violato alcune delle norme del GDPR richiamate, ma non l'art. 25 del GDPR in materia di *privacy by design* e *by default*, disposizione solitamente invocata in funzione dell'accertamento di un trattamento di dati eccessivo. Cionondimeno, era osservato il mancato rispetto del principio di correttezza nell'omettere di comunicare al minore le potenzialità di diffusione dei dati personali che questi avrebbe caricato sulla piattaforma[22]. Il Garante irlandese escludeva, a cascata, la violazione dell'art. 25 GDPR, ma ordinava a TikTok di provvedere all'inserimento di una notifica a comparsa durante la registrazione e la pubblicazione di video, riconoscendo il rischio

[18] Data Protection Commission, *In the matter of TikTok Technology Limited: Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Articles 60 and 65 of the General Data Protection Regulation,* (IN-21-9-1 2023) <final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf> ultimo accesso 18 settembre 2025.

[19] In particolare, si trattava degli artt. 5, 12, 13, 24, 25 GDPR.

[20] Anche queste avevano infatti segnalato la violazione delle stesse norme del GDPR da parte di TikTok.

[21] EDPB, *Decisione vincolante 2/2023 relativa alla controversia presentata dall'autorità di controllo irlandese riguardante TikTok Technology Limited (articolo 65 del RGPD)* (2023) <edpb_bindingdecision_202302_ie_sa_ttl_children_it_0.pdf> ultimo accesso 17 febbraio 2025.

[22] Preme osservare che l'EDPB nega la violazione dell'art. 25 non in punto di diritto, ma in quanto ritiene che le informazioni presentate dall'Autorità irlandese circa l'assenza di ulteriori misure adottate dal prestatore per la verifica dell'età sono insufficienti a stabilire se le soluzioni adottate da TikTok siano inadatte a tutelare i minori. Cfr. EDPB, *Decisione vincolante 2/2023,* (n 21) 58.

ISSN 2281-5147

per il minore che utilizzasse la paittaforma[23]. La misura di tutela prescelta era dunque volta alla maggiore sensibilizzazione del minorenne e del genitore nei confronti dei potenziali rischi di utilizzo del *social network*, pur non risultando violato il principio di *privacy by design* e *by default*[24].

A ben vedere una simile posizione, di delicato equilibrio, è emersa proprio nel provvedimento ChatGPT sopra richiamato, nel quale l'Autorità italiana, pur ordinando la predisposizione di misure tecniche per la tutela del minore, aveva negato l'applicabilità dell'art. 8 GDPR, sostenendo che il consenso a cui tale norma si riferisce non costituisse la legittima base giuridica per il trattamento dei dati personali svolto, con la conseguenza che la sua ipotetica violazione sarebbe risultata in concreto irrilevante.

L'esame dei provvedimenti pone in primo luogo in luce le evidenti incertezze connesse ad un processo, attualmente in atto, di definizione del quadro normativo applicabile. Tutti i provvedimenti citati riconoscono il rischio di ingiusta esposizione del minore e la necessità di adottare idonee misure tecnologiche, di processo o di trasparenza, atte a limitare tale rischio. Nello scenario europeo, non è tuttavia chiarita la norma o il principio di diritto violato. In effetti, il riferimento all'art. 8 GDPR in materia di consenso prestato dall'esercente la responsabilità genitoriale in caso di minore che utilizzi servizi *online* presenta il limite dell'applicabilità materiale della previsione, letteralmente confinata ai casi nei quali la base giuridica da porre a fondamento del trattamento sia proprio il consenso. Tale norma non sarebbe dunque applicabile qualora la base del trattamento dei dati (come precisato dal Garante nel caso ChatGPT) fosse da individuarsi nella conclusione di un contratto tra l'utente del servizio (ancorché tramite il consenso espresso dai soggetti esercenti la responsabilità genitoriale) ed il prestatore titolare del trattamento. Evidenziare un trattamento che non rispetti il *principio di privacy by design* o *privacy by default* (con conseguente violazione dell'art. 25 GDPR) potrebbe costituire una soluzione giuridicamente più appropriata in astratto, considerata la natura ontologicamente elastica dei principi di diritto citati, ma l'EDPB non pare ad oggi confermare la soluzione prospettata dal Garante irlandese. Ciò nondimeno, in tutti i provvedimenti richiamati, è evidente il ricorso alle

[23] Il Garante irlandese, con provvedimento 1° settembre 2023, irroga quindi la sanzione di euro 345 milioni ritenendo violati gli artt. 5, 12, 13 e 24 GDPR. Cfr. Data Protection Commission, *In the matter of TikTok Technology Limited* (n 18).
[24] Cfr. EDPB, *Decisione vincolante 2/2023* (n 21) 67.

ISSN 2281-5147

previsioni in materia di protezione dei dati personali allo scopo di affrontare il tema della tutela del minore. Si osserva, inoltre, che tale tendenza è trasversale ai casi di impiego dei sistemi intelligenti e dei *social media*.

La seconda osservazione che si può svolgere discende proprio da quest'ultima circostanza, nel senso che l'illecito trattamento dei dati, le modalità di accesso al servizio e i derivanti rischi di utilizzo per il minore appaiono intersecare scenari e strumenti assai differenziati. In altre parole, non si tratta solo di impiego di strumenti intelligenti, né unicamente di illecito trattamento dei dati personali o di improprio utilizzo dei *social network*. Spesso, le problematiche in ordine alla tutela del soggetto altamente vulnerabile possono sussistere a prescindere dalla tipologia di servizio prestato e riguardano le modalità di trattamento dei dati personali degli utenti, così come il rischio di esporli a contenuti o servizi inadeguati alla loro età[25]. Analogamente, e in modo logicamente conseguente, la misura alla quale più sovente i Garanti volgono la loro attenzione pare quella connessa alla limitazione di accesso alla rete, alla piattaforma, al *social network* o allo strumento di IA.

4. Le regole in materia *age verification* quali strumenti trasversali di tutela

Le norme in materia di limitazione dell'accesso in ragione dell'età appaiono dunque uno strumento trasversale nell'intento di garantire tutela al minore. Il punto di contatto evidenziato spinge a valutare positivamente l'opportunità di estendere il presente ambito di indagine. Ciò pare utile per più ragioni. In primo luogo, le norme sui *social network* e minori sono state adottate in un'epoca precedente (seppur non distante) a quella attuale, nella quale ci si interroga anche sul più recente tema dell'intelligenza artificiale. L'antecedenza storica, seppur minima, è certamente di interesse poiché consente di esaminare le tendenze legislative e gli orientamenti decisionali che si sono formati in relazione ai *social network*, sì da verificarne l'utilità e l'efficacia rispetto all'eventuale normazione in materia di intelligenza artificiale. In secondo luogo, l'estensione dell'ambito di indagine pare utile in ragione di alcune osservazione di carattere operativo, in quanto da un lato i *provider* potrebbero trovarsi ad impiegare strumenti dotati di intelligenza artificiale proprio nella fornitura dei loro servizi. Dall'altro, la stretta connessione tra le tematiche è altresì data dalla circostanza

[25] Ibid.

ISSN 2281-5147

che tali strumenti potrebbero comunque essere resi disponibili tramite l'identificazione svolta proprio dai *social network*.

Con riferimento a tali fornitori, nello scenario europeo è utile richiamare il *Digital Services Act*[26] e, in particolare, l'art. 28[27]. La norma stabilisce l'obbligo in capo ai fornitori di piattaforme *online* di adottare misure adeguate e proporzionate a garantire un elevato livello di tutela dei minori[28]. Tra i progetti avviati dalla Commissione europea volti all'attuazione di questa previsione[29] rientra il recente *Statement* 1/2025 dell'EDPB a tutela dei minori nell'ambiente digitale, che pure caldeggia l'adozione di sistemi di *age assurance* allo scopo di realizzare un bilanciamento tra gli obblighi derivanti dal diritto dell'Unione europea e il rispetto del GDPR[30]. In particolare, l'atto è indirizzato ai fornitori di servizi *online* (piattaforme, siti, applicazioni, operatori

[26] 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) [2022] OJ L277/1.

[27] Sul punto, la Commissione Europea ha reso disponibile un modello tecnico di verifica dell'età volto a proteggere i minori *online*. Si veda <Commission releases enhanced second version of the age-verification blueprint | Shaping Europe's digital future> ultimo accesso 18 settembre 2025.

[28] La norma dà inoltre la possibilità alla Commissione di adottare orientamenti in merito. Reg. (UE) 2022/2065, art. 28, par. 1 e 4: «I fornitori di piattaforme *online* 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. […] La Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme *online* nell'applicazione del paragrafo 1».

[29] Giova inoltre evidenziare che i progetti avviati dalla Commissione inerenti all'individuazione di meccanismi di verifica dell'età ai sensi dell'art. 28 DSA si intrecciano anche con l'esigenza dell'Unione di sviluppare soluzioni di Portafoglio europeo di Identità Digitale (PEID). La Commissione, infatti, intende vagliare la possibilità che un domani gli attributi relativi "all'età anagrafica" possano essere condivisi dall'utente europeo anche tramite il PEID, nel caso in cui i prestatori di servizi siano tenuti a verificare l'età. Da <Commission releases enhanced second version of the age-verification blueprint | Shaping Europe's digital future>: «The age verification blueprint lays the groundwork for broader deployment of age-appropriate services in the future. It is also referred to as the 'mini-wallet', as it is built on the same technical specifications as the forthcoming European Digital Identity Wallets, ensuring long-term compatibility and providing a stepping stone toward the rollout of the European Digital Identity Wallets before the end of 2026».

[30] EDPB, *Dichiarazione 1/2025 sulla garanzia dell'età* (2025) <*edpb_statement_20250211ageassurance_it.pdf*>. Il Garante europeo ha stabilito che i sistemi di *age assurance* debbano essere conformi ai principi sanciti dal GDPR, in particolare necessità, proporzionalità, minimizzazione dei dati, correttezza e trasparenza. L'implementazione deve fondarsi su un'idonea base giuridica di cui all'articolo 6 GDPR (ed eventualmente, ove rilevante, su una delle eccezioni di cui all'articolo 9, paragrafo 2), ed essere preceduta, nei casi di trattamenti ad alto rischio, dalla redazione di una valutazione d'impatto *ex* articolo 35 GDPR. È fatto divieto che l'*age assurance* si traduca in attività ulteriori rispetto alla finalità propria di verifica dell'età, quali identificazione, localizzazione o profilazione degli utenti, in violazione dei principi di limitazione della finalità e di minimizzazione del trattamento. I dati trattati devono essere limitati agli attributi strettamente necessari a dimostrare il superamento o meno di una determinata soglia anagrafica, anche attraverso soluzioni di tokenizzazione o tecniche crittografiche. Infine, i titolari e i responsabili del trattamento sono tenuti ad adottare un quadro di *governance* che assicuri la piena *accountability* ai sensi dell'articolo 5, paragrafo 2, GDPR, garantendo tracciabilità delle decisioni, la possibilità di svolgere *audit* dei processi e la possibilità di controllo da parte delle autorità competenti.

ISSN 2281-5147

digitali) che devono limitare l'accesso dei minori o offrire contenuti e servizi adeguati alla loro età. Questi, unitamente ai fornitori dei servizi di verifica dell'età (*Identity Provider*) dovrebbero limitare l'accesso a contenuti vietati o non appropriati, adottare misure specifiche contro le differenti casistiche di rischio (a titolo esemplificativo abusi, *grooming*, violenza, pornografia, etc.) e attivare sistemi di *parental control* e segnalazione.

A livello internazionale, la maggior parte delle regolamentazioni a tutela dei minori *online* suddividendo la responsabilità e l'onere della tutela del minore tra l'apparato latamente statuale, le famiglie (sovente tramite meccanismi di richiesta del consenso al genitore) e le imprese (tramite meccanismi di autoregolamentazione e previsione di obblighi di diversa natura)[31]. Nella gran parte degli scenari, il minore può, tramite meccanismi più o meno stringenti, navigare *online*, ma la sua capacità naturale o giuridica è limitata da meccanismi di acquisizione del consenso dell'esercente la responsabilità genitoriale.

In Inghilterra, è stato adottato l'*Online Safety Act* nel 2023[32], il quale prevede una serie di adempimenti precauzionali in capo ai fornitori dei servizi *online* per la valutazione dei rischi sulla base di una logica progressiva decrescente, secondo la quale più intense misure sono necessarie al diminuire dell'età del minore. I servizi interessati sono quelli che pongono in contatto gli utenti tra loro (i cd. *user-to-user services*) e i servizi di ricerca (i cd. *Search services*). Entrambi devono adottare misure proporzionate per mitigare i rischi per i bambini e proteggere le diverse fasce d'età da contenuti dannosi[33]. Sul punto, le modalità di attuazione di tali *duty of care* sono esplicitate nel Children's Code

[31] Anche la Legge sulla Protezione dei Minori della Repubblica Popolare Cinese (中华人民共和国未成年人保护法) del 17 ottobre 2020 demanda ai genitori la regolamentazione dell'utilizzo della rete e l'accesso dei minori a Internet, attribuendo tuttavia un rilevante ruolo nella formazione dei minori anche allo Stato e alle scuole. La normativa, in vigore dal 1° giugno 2021, sottolinea fortemente il ruolo dell'alfabetizzazione digitale dei minori e impone in capo allo Stato e alle famiglie il compito di prevenire il fenomeno di indipendenza da Internet. Una disciplina specifica è inoltre prevista per i fornitori di servizi *online* di gioco, i quali sono tenuti ad adottare misure per limitare l'accesso dei minori. A titolo esemplificativo, la legge prevede l'istituzione di un sistema di autenticazione elettronica dell'identità e la classificazione dei giochi offerti sulla base degli standard nazionali. I fornitori sono inoltre tenuti a fornire suggerimenti adatti all'età dell'utente e ad adottare misure tecniche per non consentire ai minori di accedere a giochi o funzioni di gioco inappropriate. Ulteriore misura prevista consiste nel vietare la fornitura ai minori di giochi *online* in capo ai fornitori dalle 22:00 alle 8:00 del giorno successivo.

[32] *Online Safety Act* 2023 del 26 ottobre 2023.

[33] Rileva in particolare il *Chapter 2* «Providers of user-to-user services: duties of care», la cui *Section* 12 dispone verso i fornitori l'obbligo di implementare politiche chiare nei termini di servizio per garantire la sicurezza dei bambini.

ISSN 2281-5147

ad opera dell'Autorità garante inglese (*Information Commissioner's Office* – più brevemente "ICO")[34]. Per limitare l'accesso ai contenuti vietati, gli operatori possono avvalersi di specifici meccanismi di verifica dell'età previsti dall'Autorità, che vanno dall'autodichiarazione all'impiego di documenti di identificazione[35]. Il Children's Code distingue poi cinque fasi di sviluppo (ad es. fase di pre-alfabetizzazione, adolescenziale etc.) in relazione ai quali gli operatori sono tenuti ad adottare diversi approcci precauzionali[36]. Sono previste regole sulla trasparenza e di limitazione delle tecniche manipolatorie. In particolare, vengono posti limiti al cosiddetto *nudge,* l'uso di tecniche per guidare o incoraggiare bambini a fornire dati personali non strettamente necessari come, ad esempio l'impiego di colori specifici per favorire associazioni mentali. È necessario adottare misure che rendano evidenti eventuali operazioni di raccolta o registrazione dei dati personali, tramite luci o segnali visivi[37].

Anche negli Stati Uniti sono previste numerose indicazioni in merito alla trasparenza. L'impianto normativo in materia si compone di due diversi atti, il *Children's Online Privacy Protection Act* del 1998, 15 U.S.C. 6501–6505 (in seguito semplicemente "COPPA Act") e il part 312— *Children's Online Privacy Protection Rule* (in seguito solo "*COPPA Rule*"). La normativa COPPA prevede una serie di obblighi per prestatori di servizi *online*, che possono essere distinti in obblighi di trasparenza e di diligenza. Ad esempio, quanto alla trasparenza, i *provider* sono tenuti a fornire un avviso riguardo alle informazioni raccolte sul minore, alle modalità con cui si domanda al genitore il

[34] Information commissioner's officer, *Children's code* (2020) <Age appropriate design: a code of practice for online services | ICO> consultato il 17 settembre 2025.

[35] Il *Children's code, Section 3,* fa riferimento a diversi metodi di verifica dell'età. Sono annoverati: l'autodichiarazione, sulla base della quale gli utenti dichiarano autonomamente la loro età senza fornire alcuna prova ulteriore; l'uso di sistemi di IA, che in base all'analisi delle interazioni dell'utente è in grado di stimare l'età; il ricorso a servizi di verifica di terze parti, le quali si impegnano a non raccogliere dati sensibili; la conferma da parte del titolare adulto avente un *account* presso lo stesso servizio; l'uso di misure tecniche che scoraggino dichiarazioni false, come il blocco automatico di *account* ripetutamente non confermati; l'uso di documenti di identificazione, che consentano di confermare l'età. L'ICO ha cura, tuttavia, di precisare che tale ultimo metodo appare sproporzionato rispetto all'esigenza di tutelare i minori, in quanto produrrebbero impatti eccessivi sulla *privacy* dell'utente.

[36] Le differenti fasce si suddividono in: 0 – 5 anni, periodo della pre-alfabetizzazione e sviluppo iniziale; 6 – 9 anni, periodo dell'apprendimento scolastico di base; 10 – 12 anni, anni di transizione; 13 – 15 anni, adolescenza iniziale; infine, 16 - 17 anni, periodo dell'avvicinamento all'età adulta. La tabella che consente di individuare le capacità cognitive dei minori per ogni fascia d'età è disponibile *online*: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>

[37] Ad esempio, una luce che si accende quando il dispositivo sta registrando.

ISSN 2281-5147

consenso al loro impiego, il loro utilizzo e le pratiche di divulgazione[38]. I genitori devono avere la possibilità di accedere ai dati raccolti sui figli[39]. Ancora, è fatto divieto di condizionare la partecipazione a giochi o attività alla fornitura di informazioni personali non necessarie[40]. Il COPPA prevede poi la possibilità di aderire a programmi *Safe Harbour* disciplinati dal § 312.11, uno strumento di autoregolamentazione volontaria per i *provider*, proposti da gruppi industriali o soggetti privati e approvati dalla *Federal Trade Commission* (FTC) qualora garantiscano protezioni equivalenti o superiori a quelle stabilite dalla normativa[41]. Nello scenario statunitense, si precisa, il divieto di accedere[42] ai siti internet per i minori di 13 anni è strutturato come una mera possibilità per il *provider*.

Nell'opposta direzione si muove invece l'*Online Safety Act* australiano del 2021[43] che, alla Sezione 63 D, definisce come *age restricted social media platform,* ossia come

[38] Children's Online Privacy Protection Rule 16 CFR Part 312 §312.4(b): «*Direct notice to the parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented».

[39] Children's Online Privacy Protection Rule 16 CFR Part 312, § 312.6(a(1)): «Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following: A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities».

[40] Children's Online Privacy Protection Rule 16 CFR Part 312, §312.7: «An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity».

[41] Alcuni dei progetti attualmente in corso sono reperibili al seguente link <https://www.ftc.gov/enforcement/coppa-safe-harbor-program> ultimo accesso: 14 marzo 2025.

[42] L'indicazione è reperibile tra le FAQ del COPPA: «Can I block children under 13 from my general audience website or online service? Yes. COPPA does not *require* you to permit children under age 13 to participate in your general audience website or online service, and you may block children from participating if you so choose. By contrast, you may not block children from participating in a website or online service that is directed to children as defined by the Rule, even if the website or online service is also directed to users age 13 or older».

[43] Online Safety Act 2021, come modificato da Act No. 127, 2024. L'Online Safety Act 2021 (OSA) intende assicurare che Internet rimanga uno spazio sicuro intervenendo secondo due linee di azione: la prima consiste nell'attribuire ampi poteri di controllo all'Autorità garante australiana (*eSafety Commissioner*), la quale assume un ruolo attivo nei rapporti tra i prestatori di servizi *online* e gli utenti; la seconda consiste nell'individuare le cd. "Expectations" nei confronti dei prestatori di servizi per garantire un ambiente digitale sicuro (*Part 4 – Basic online safety expectations*), senza tuttavia entrare nello specifico delle modalità con le quali tali "Expectations" possono essere raggiunte. Con riferimento alla prima linea di azione, ai sensi del *Part 3 – Complaints, objections and investigations, Division 1- Introduction, No. 29* ss., i minori possono rivolgersi direttamente al *Commissioner* lamentando episodi di cyberbullismo o segnalando contenuti a loro vietati. Il *Commissioner* può, a sua volta, ai sensi del *Part 5, No 65* e *No. 109,* emettere un avviso di rimozione al fornitore di *social media* qualora l'oggetto dei contenuti sia stato accertato essere in violazione dell'OSA; inoltre, ai sensi del *No. 49* e *No. 56,* può richiedere ai prestatori un "*periodic reporting notice*" sullo stato di conformità alle cd. "Expectations". Sono infine previsti

ISSN 2281-5147

piattaforme *online* vietate ai minori di 16 anni[44], quei servizi elettronici[45] che consentono l'interazione tra due o più utenti o che consentono di caricare materiali *online*[46]. Il divieto in esame è di natura sostanziale. In altre parole, a differenza di

ulteriori poteri per il controllo della compliance e monitoraggio (*Part 10 -Enforcement)*. Con riferimento alla seconda linea d'azione, il legislatore australiano prevede gli obiettivi che i prestatori devono raggiungere per garantire un ambiente digitale sicuro (*Part 4, Division 2 – Basic online safety expectations, No. 46 Core Expectations*), delegando ai codici di condotta la definizione delle modalità tecniche ed organizzative per raggiungerli. La *Part 9 – Online content scheme* definisce comunque uno schema minimo che tali codici di condotta devono seguire, specificando i contenuti vietati ai minori di diciotto anni (*No. 106 – 107*) e fornendo esempi di "argomenti" da disciplinare nei codici. A titolo esemplificativo, la *Subdivision B—General principles relating to industry codes and industry standards, No. 138 "Examples of matters that may be dealt with by industry codes and industry standards"* prevede che i codici di condotta debbano individuare le procedure atte sia ad assicurare che gli account *online* non possano essere creati dai minori senza il consenso dei genitori sia a fornire ai genitori informazioni circa i modi e gli strumenti con cui possono monitorare o controllare l'attività dei propri figli sui loro servizi. Anche nella redazione di tali codici di condotta si prevede un diretto coinvolgimento del *Commissioner*, che può aggiornare gli indirizzi degli standard tecnici ed organizzativi da adottare, gli ambiti nei quali i codici devono intervenire, ed organizzare delle consultazioni pubbliche al fine di agevolare la stesura dei codici di condotta (*Part 9, Division 7, Subdivision C – E*). L'approccio che traspare è di mantenere la sfera d'azione pubblica separata dalla sfera d'azione privata. In altre parole, il legislatore australiano dell'OSA 2021 non intende obbligare in concreto il prestatore a determinati "comportamenti" nella prestazione del suo servizio, limitandosi piuttosto a fissare i risultati che i prestatori di servizi devono raggiungere attraverso proprie scelte d'azione.

[44] Giova precisare che la *Part4A - Social media minimum age*, adottata il 2 dicembre 2024 con l'*Act No. 127, 2024* e in vigore a partire dal 10 dicembre 2025, è l'unica parte del testo normativo australiano che impone direttamente l'obbligo a determinati prestatori di vietare l'accesso ai loro servizi ai minori di 16 anni. In tale contesto normativo si inseriscono inoltre le eSafety Commissioner, *Basic Online Safety Expectations* (2024) in <Federal Register of Legislation - Online Safety (Basic Online Safety Expectations) Determination 2022> ultimo accesso 14 febbraio 2025. "*The Expectations"* integrano l'OSA attraverso l'individuazione più specifica di misure standard minime che i fornitori di servizi devono assicurare per il raggiungimento dei risultati previsti dalla *Part 4* OSA.

[45] La normativa si concentra sui *social network*, ma al contempo prevede norme specifiche qualora siano impiegati sistemi di IA. Nella *Division 2 – Basic Online safety expectations, Section 8A "Additional expectations—provider will take reasonable steps regarding generative artificial intelligence capabilities* vi è espresso rimando all'adozione di misure in grado di consentire solo un utilizzo sicuro di IA generativa per tutti. Tuttavia, mentre a Settembre 2024, il *Commissioner* australiano ha formalmente richiesto a YouTube, Facebook, Instagram, TikTok, Snap, Reddit, Discord e Twitch di indicare quali meccanismi di *age assurance* avessero adottato, nessuna richiesta in tal senso è stata avanzata nei confronti di fornitori di sistemi di IA. In eSafetyCommissioner, *eSafety calls on social media giants to reveal just how many Aussie kids are signing up* (2024) <eSafety calls on social media giants to reveal just how many Aussie kids are signing up | eSafety Commissioner> consultato il 14 febbraio 2025.

[46] Specificamente, le piattaforme che vi rientrano sono: «(a) an electronic service that satisfies the following conditions: (i) the sole purpose, or a significant purpose, of the service is to enable online social interaction between 2 or more end users; (ii) the service allows end users to link to, or interact with, some or all of the other end users; (iii) the service allows end users to post material on the service; (iv) such other conditions (if any) as are set out in the legislative rules; OR (b) an electronic service specified in the legislative rules but does not include a service mentioned in subsection. For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes». È inoltre previsto che il *provider* di tali piattaforme non possa raccogliere strumenti identificativi emessi dallo Stato australiano né utilizzare servizi di accreditamento previsti dal Digital IA Act del 2024. Cfr. OSA, s(63DB): «A provider of an age restricted social media platform must not: (a) collect government issued identification material; or (b) use an accredited service (within the meaning of the Digital ID Act 2024); for the purpose of complying with section 63D, or for purposes that include the purpose of complying with section 63D». In altre parole, la piattaforma non può avvalersi né delle carte di identità rilasciate nell'ambito del Commonwealth, né

ISSN 2281-5147

quanto prevede l'art. 8 del GDPR o, seppur in maniera graduata, la normativa britannica, il legislatore australiano non si limita ad imporre il rispetto di regole in materia di accesso, capacità giuridica o moderazione dei contenuti, bensì vieta in modo radicale l'impiego di tali piattaforme ai minori di 16 anni. La responsabilità non è in questo caso allocata in capo al genitore, ma vi è una chiara scelta di politica legislativa che riconosce a priori la rischiosità dell'impiego dei *social media*.

5. La recente legge italiana sull'impiego degli strumenti di IA

Nello scenario italiano, il tema della tutela del minore è stato recentemente oggetto di specifica normazione. A differenza di quanto è avvenuto in Australia con riferimento alla limitazione dell'uso dei *social network*, ove il legislatore ha scelto di imporre un limite di natura sostanziale con riferimento allo specifico servizio, la legge del 23 settembre 2025, n. 132 (Legge sull'IA) ha adottato un approccio più mediato, che appare ispirato dall'art. 8 del GDPR. L'art. 4 della Legge sull'IA, astenendosi da valutazioni circa la rischiosità del mezzo, prevede infatti che «l'accesso alle tecnologie di intelligenza artificiale dei minori di anni quattordici richied[a] il consenso di chi esercita la responsabilità genitoriale»[47]. Tale formulazione sembra poter includere l'accesso ai sistemi di IA tramite ogni tipo di piattaforma o fornitore, privilegiando la

utilizzare servizi di identità digitale. La Sezione 63DB, *Use of certain identification material and services*, prevede infatti che per «government issued identification material» sia da intendersi «identification documents issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory (including copies of such documents); and (b) a digital ID (within the meaning of the Digital ID Act 2024) issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory». È inoltre previsto dalla *Section 63DA* che il Ministero per le Comunicazioni possa individuare con propri provvedimenti quali informazioni le *social media platform* non devono raccogliere per assolvere all'obbligo.

[47] Cfr. L. 132/2025, art. 4 c. 4: «L'accesso alle tecnologie di intelligenza artificiale da parte dei minori di anni quattordici nonché il conseguente trattamento dei dati personali richiedono il consenso di chi esercita la responsabilità genitoriale, nel rispetto di quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196. Il minore di anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili». Sempre nello scenario europeo, lo Stato del Vaticano ha adottato con Decreto n. DCCII le *Linee guida in materia di intelligenza artificiale* (2024) <*Linee guida in materia di intelligenza artificiale del Governatorato dello Stato della Città del Vaticano*> ultimo accesso: 17 settembre 2025. Pur non entrando nell'ambito della tutela dei minori, le linee guida intendono promuovere uno sviluppo ed uno utilizzo di sistemi di IA in ottica antropocentrica, con ciò adeguandosi alla direzione intrapresa dal legislatore europeo. Sebbene con formulazione differente, sono infatti presenti sia gli stessi divieti disposti dall'art. 5 AI Act sia l'obbligo di rispettare i principi di trattamento dei dati personali nell'ambito dello sviluppo ed utilizzo del sistema di IA.

ISSN 2281-5147

natura particolare del minore e la sua fragilità. La scelta circa l'idoneità del servizio o del prodotto dotato di IA è dunque rimessa in primo luogo al *provider* che lo renda disponibile sul mercato. Qualora il servizio non fosse dichiaratamente ritenuto adeguato al minore infraquattordicenne, sarebbe poi il genitore o l'esercente la responsabilità a poter rendere il consenso al suo utilizzo. Da ultimo si osserva che, come è avvenuto per l'art. 8 GDPR nei provvedimenti sopra richiamati, l'onere di consentire l'applicazione in concreto della disposizione ricadrà (in una misura che occorrerà determinare) sul *provider* che (in modo autonomo o tramite un *Identity Provider*) predisporrà il sistema di riconoscimento del genitore o, in ottica di minimizzazione, di *age verification* del minore, prima, e dell'esercente la responsabilità genitoriale poi.

Quanto all'effettività della previsione, il ruolo degli *Identity Provider* è evidentemente cruciale e, nello scenario italiano, è già stato declinato con riferimento ad uno specifico settore nella delibera dell'AGCOM 96/25/CONS [48] di attuazione dell'art. 13-*bis* del Decreto Caivano[49]. Si tratta della norma che impone ai fornitori di piattaforme che diffondono in Italia «immagini e video a carattere pornografico» di verificare la maggiore età degli utenti, allo scopo di «evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto». La delibera dell'AGCOM ha un contenuto del tutto specifico e settorialmente indirizzato, in quanto contiene obblighi diretti ai soggetti che diffondono in Italia contenuti pornografici. Tuttavia, in relazione alla corrente analisi, pare utile evidenziare le osservazioni formulate dall'Autorità in merito alle soluzioni tecniche per la limitazione dell'accesso ai servizi citati, in quanto appaiono potenzialmente rilevanti ogniqualvolta ci si accinga ad imporre un sistema di *age limitation* in relazione ad un servizio, sia questo quello del *social network* o quello

[48] AGCOM, *Delibera 96/25/CONS: adozione delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge del 13 novembre 2023, n. 159* (2025) <delibera 96-25-CONS.pdf> ultimo accesso 17 settembre 2025: «In via di premessa, è importante sottolineare che la Commissione ha condiviso l'obiettivo perseguito da Agcom attraverso il progetto notificato inteso a proteggere i minori *online*, in particolare dai contenuti a carattere pornografico, che possono nuocere alla loro salute e al loro sviluppo fisico, mentale e morale. Si tratta, infatti, di obiettivi allineati a quelli del quadro giuridico europeo per i servizi online, in particolare il regolamento (UE) 2022/2065 (di seguito il «regolamento sui servizi digitali o DSA) e la direttiva 2000/31/CE (direttiva sul commercio elettronico)».

[49] D.l. 15 settembre 2023, n. 123, art. 13-*bis*: «I gestori di siti web e i fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto. […] L'Autorità per le garanzie nelle comunicazioni stabilisce, […] con proprio provvedimento, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i soggetti di cui al comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti».

ISSN 2281-5147

connesso all'impiego di un sistema dotato di intelligenza artificiale. Pur non imponendo univoche soluzioni tecnologiche, l'AGCOM ha rilevato rischi trasversali connessi alla previsione di *age gate,* raccomandando che a procedere alla verifica dell'età siano soggetti terzi rispetto al gestore del servizio e scoraggiando i prestatori dall'avvalersi di meccanismi interni per la verifica dell'età[50]. Si tratta del sistema del "doppio anonimato", secondo il quale da un lato i dati personali dell'utente devono essere tutelati nei confronti della piattaforma che offre il servizio e, dall'altro, i siti visitati non possono essere conosciuti dall'*Identity Provider*. Da ultimo, non può non evidenziarsi come nella delibera emerga altresì la valutazione dell'Autorità sull'efficacia della soluzione tecnica proposta: nessuno dei sistemi di *age verification* è considerato completamente sicuro rispetto a meccanismi elusivi da parte degli utenti[51].

[50] L'Autorità non esclude, poi, che tale verifica potrà essere soddisfatta, a partire dal 2026, anche con il PEID. Infatti, i nuovi *digital wallet* potranno essere in grado di condividere anche solo l'attributo dell'età anagrafica con i prestatori di servizi, senza per ciò stesso rivelare l'identità dell'utente. Cfr. Allegato B) alla delibera n. 96/25/CONS cit., 14: «Nella maggior parte dei casi, i cittadini non possono scambiare digitalmente a livello transfrontaliero, in modo sicuro e con un livello elevato di protezione dei dati, informazioni relative alla loro identità quali indirizzi, età e qualifiche professionali, patenti di guida e altri permessi e dati di pagamento. Pertanto, l'*EUDI wallet* consentirebbe di superare tali limiti offrendo la possibilità di scambiare attributi minimi dell'identità necessari ad accedere determinati servizi online per cui è richiesta l'autenticazione, come ad esempio la prova dell'età. Inoltre, il nuovo Regolamento eIDAS prevede che, qualora le piattaforme online di dimensioni molto grandi, come definite dal DSA, impongano agli utenti di autenticarsi per accedere ai servizi online, queste dovranno accettare anche l'uso dei portafogli europei di identità digitale, rigorosamente su richiesta volontaria dell'utente, anche per quanto riguarda gli attributi minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione, come la prova dell'età». L'allegato riporta anche il rapporto del regolatore inglese OFCOM, che si è espresso in relazione all'*Online Safety Act*. L'autorità inglese ha ritenuto che la verifica dell'età tramite PEID sia altamente efficace. L'AGCOM non ritiene, invece, che lo SPID possa considerarsi una soluzione ottimale, almeno fino a quando i relativi prestatori avranno accesso alle informazioni circa i siti visitati dagli utenti che richiedono l'identificazione. Cfr. Allegato A), Delibera 96/25/CONS, cit., 4-5: «[…] tale sistema di autenticazione SPID consente all'*Identity Provider* di conoscere il particolare sito/piattaforma visitato dall'utente e non è da escludere che tale informazione venga memorizzata all'interno dei sistemi dell'Identity Provider. […] Si evidenzia, pertanto, la possibilità, con un sistema pubblico, di poter disporre in breve tempo di un insieme di Identity Provider certificati e di una rete di connessioni e accordi (basati su obblighi normativi esistenti), in grado di fornire, all'utente e per il tramite di questo alla piattaforma, la cosiddetta prova dell'età. Quanto detto vale sia per la modalità di verifica dell'età collegate a sistemi di verifica dell'età non basati su applicativi installati nel terminale utente sia per quelli basati su applicativi installati nel terminale utente (cosiddetti *digital wallet*), fermo restando la necessità di preservare la libertà di scelta dell'utente in merito all'utilizzo di uno o dell'altro sistema, anche considerando la potenziale invasività dell'installazione di determinate app sul proprio dispositivo personale. L'Autorità, pertanto, solo laddove soddisfatti i requisiti di cui alla sezione seguente sul doppio anonimato (protezione dei dati personali nei confronti del sito/piattaforma e non conoscenza del sito visitato/piattaforma da parte dell'Identity Provider), ritiene che sistemi pubblici siano utilizzabili».

[51] Allegato A), Delibera 96/25/CONS, cit., 10: «Per quanto riguarda i dispositivi attualmente offerti sul mercato, diversi regolatori evidenziano che attualmente tutte le soluzioni proposte possono essere in qualche modo aggirate. Ad esempio, l'utilizzo di una VPN, che nasce per garantire sicurezza nell'utilizzo di Internet agli utenti,

ISSN 2281-5147

6. Considerazioni conclusive: verso un approccio trasversale alla tutela del minore *online*?

Le soluzioni normative esaminate in materia di tutela del minore *online*, sia che questo utilizzi sistemi di intelligenza artificiale, *social network* o che semplicemente coincida con il soggetto interessato del trattamento dei dati personali, possono essere raggruppate per metodologie. Mentre Stati Uniti e Regno Unito hanno adottato approcci basati rispettivamente sulla co-regolamentazione e sulla valutazione del rischio, senza prevedere specifici divieti, l'Australia ha introdotto un divieto sostanziale in merito all'uso dei *social network* ai minori di sedici anni. L'Italia e l'Europa sembrano aver adottato una posizione intermedia. L'art. 28 del DSA impone un obbligo sui prestatori di servizi *online* di garantire «un elevato livello di tutela» per il minore. Con riferimento all'accesso agli strumenti dotati di intelligenza artificiale, nel solo scenario italiano, è da ultimo stato attribuito al soggetto esercente la responsabilità genitoriale il compito di acconsentire a che il minore vi sia esposto, mentre è allocata sul *provider* la responsabilità di implementare un sistema di verifica[52] della provenienza del consenso dal soggetto legittimato ad esprimerlo o di verifica dell'età del minore *tout court*. Appare corretto l'approccio del legislatore europeo (e italiano) nell'astenersi dall'individuare un metodo specifico per lo svolgimento dell'*age verification*, dimostrando di intendere che di una rincorsa tra metodi di verifica e sviluppo tecnologico potrebbe trattarsi in concreto.

In ognuno dei casi qui richiamati, però, l'efficacia in concreto delle norme che si pongono l'obiettivo di limitare l'accesso agli strumenti dotati di intelligenza artificiale, ai *social network* o al trattamento dei dati personali *online*, è subordinata alla possibilità tecnica di aggirare il divieto. Come anticipato, l'AGCOM conferma che tutte le soluzioni tecniche per garantire la sicurezza dei processi di *age verification* esaminate nella Delibera 26/95/CONS. si prestano, ad oggi, a meccanismi elusivi mediante l'uso di VPN da parte degli utenti. A ben vedere, la medesima conseguenza è trasversale a

può allo stesso tempo consentire a un minore di eludere un sistema di verifica dell'età. Il soggetto tenuto, ai sensi della legge, a realizzare il sistema di controllo dell'età per l'accesso ai contenuti, non deve promuovere o fare comunque riferimento a qualsiasi meccanismo di elusione dei sistemi di age *assurance*».

[52] Già oggi obbligatoriamente basato sul sistema del doppio anonimato per quanto concerne il ristretto ambito di applicazione della Delibera 96/25/CONS.

ISSN 2281-5147

tutti i sistemi normativi esaminati, sia nel caso in cui non sia previsto alcun limite di utilizzo per i minori (quando questo venga ad esempio imposto dal *provider*), sia nel caso in cui vi sia l'imposizione di un divieto assoluto di utilizzo (come nel caso australiano), sia nel caso in cui la scelta circa la possibilità di accedere al servizio venga affidata al consenso del genitore (come prevedono la legge italiana ed il GDPR). In ognuna delle situazioni richiamate, il minore che voglia aggirare il divieto si scontrerà con le misure di sicurezza adottate dal fornitore del servizio e, a seconda dell'ordinamento, dall'*Identity Provider*.

Ne consegue la necessità di approcciare la questione della tutela del minore non solo dal punto di vista legislativo e prescrittivo, ma anche a livello culturale, includendo nel dialogo non solo i legislatori ma gli stessi *provider*. Ad accrescere il livello generale di consapevolezza dei consociati circa i rischi connesso all'utilizzo dell'IA *online*, accentuati dall'intrinseca fragilità del minore, possono contribuire alcuni strumenti, già evidenziati nei provvedimenti esaminati, quali le tecniche anti *nudge*, i processi di co-regolamentazione con gli stessi fornitori e, pur con i limiti già emersi negli studi in materia di protezione dei dati personali, i sistemi di notifica informativa (si pensi al provvedimento Tik Tok). Tuttavia, una riflessione di carattere culturale sui rischi per i minori che utilizzino strumenti di IA, non può prescindere dal considerare, al contempo, i rischi impliciti e connessi all'accesso e all'impiego di questi strumenti *online*. Dati i numerosi livelli di sovrapposizione che possono esistere tra le attività svolte dai minori sui *social media*, quando accedono a strumenti dotati di intelligenza artificiale e quando divengono interessati del trattamento dei dati personali, oltre a regole puntuali nei differenti settori di interesse sembra utile prendere in considerazione una visione più ampia, quella del minore, soggetto vulnerabile, che agisce *online*. L'esame dei rimedi emersi nei differenti ordinamenti sia a livello normativo (emergono gradualmente limiti di età e divieti d'accesso) sia provvedimentale (i rischi rilevati nell'esame di casistiche apparentemente dissimili appaiono i medesimi) ha infatti posto in luce come, in tutti gli scenari esaminati, il rischio evidenziato e la relativa misura correttiva siano direttamente collegati al momento in cui il minore accede al servizio che, in molti casi, coincide con la possibilità per questi di accedere *online*. A prescindere dal settore, deve dunque emergere la consapevolezza che la vulnerabilità del minore è descritta in relazione a rischi condivisi (in modo più o meno acuto a seconda della specifica tipologia dello

ISSN 2281-5147

strumento o dei servizi utilizzati) quando questi accede alla rete, luogo di amplificazione dei diritti, ma anche delle vulnerabilità.

ISSN 2281-5147