Di Cerbo A, Quali tutele online per I minori (2026) 2 EJPLT.
DOI : https://doi.org/10.57230/EJPLT252ACD

EJPLT
ISSN 2704-8012



Quali tutele online per i minori?

How are minors protected online?

ANTONELLA DI CERBO (ORCID)
Dottore in diritto civile.
Funzionaria presso l'Autorità Garante per la protezione dei dati personali.

Abstract

Il presente contributo mira ad analizzare le misure di derivazione nazionale ed europea che i fornitori di servizi, che operano nel mondo digitale, sono tenuti ad adottare per salvaguardare il benessere psicofisico dei minori. Il focus è in particolare posto sulle disposizioni del cd decreto Caivano, sul decalogo dei principi dell'Autorità di protezione dei dati personali spagnola, sugli orientamenti della Commissione europea in materia di verifica dell'età e protezione delle persone minori di età da contenuti inadeguati e sulle previsioni della legge n.132/2025 relative al consenso richiesto al minore per accedere ai sistemi di Intelligenza artificiale.

This article aims to analyze the national and European measures that digital service providers are required to adopt to protect the well-being of minors. In particular, the focus will be on the provisions of the Caivano Decree, the principles developed by the Spanish Data Protection Authority, the Guidelines on measures to ensure a high level of privacy, security, and protection for minors online, and the provisions of Law No. 132/2025 regarding the consent required for access to artificial intelligence systems.

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: minori; mondo digitale; age verification; age assurance; IA.

Summary: Introduzione – 1. Il decreto legge 23 settembre 2025, n.132 (il cd del Decreto Caivano) – 1.1 L'articolo 13 *bis* – 1.2 Il controllo parentale – 2. Gli orientamenti della Commissione relativi alle misure per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online – 3. Il decalogo dei principi dell'Autorità di protezione dei dati personali spagnola in materia di verifica dell'età e protezione delle persone minori da contenuti inadeguati – 4. Il consenso del minore in Europa – 4.1. il consenso digitale del minore in Italia – 4.1.2. Il consenso ai sensi dell'articolo 4, comma 4, della legge in materia di intelligenza artificiale – 4.2 Il consenso digitale del minore in Francia – 4.3 Il consenso digitale del minore in Spagna – 4.4. Il consenso dei minori in Australia e in Nuova Zelanda – 5. Considerazioni conclusive.

Introduzione

Il presente contributo, formulato a titolo personale e senza alcun vincolo per l'Amministrazione di appartenenza (Ufficio del Garante per la protezione dei dati personali), mira ad analizzare le misure di derivazione nazionale ed europea che i fornitori di servizi, che operano nel mondo digitale, sono tenuti ad adottare per salvaguardare il benessere psicofisico dei minori.

L'incremento dell'uso delle reti telematiche e la diffusione di applicazioni mobili come mezzi di espressione della personalità, della socializzazione e dello scambio a distanza, stanno offrendo un notevole ampliamento dei diritti e delle libertà dei singoli, come quello all'informazione ed all'autodeterminazione e, al contempo, stanno permettendo lo sviluppo della curiosità, della creatività e del pensiero critico. Ma tali benefici non sono privi di risvolti negativi[1] specie per le persone più vulnerabili, come i minori, che possono essere esposti, con facilità e frequenza, a contenuti inadeguati e pericolosi per il loro sviluppo fisico, mentale e morale[2].

Per "contenuti inadeguati" si intendono le immagini, i video e i messaggi di testo illegali, o comunque dannosi, di cui i minori fruiscono in misura crescente e che sono capaci di comprometterne la vita privata, la sicurezza e la protezione, ovvero di dar luogo a fenomeni come la radicalizzazione, l'estremismo violento, il bullismo online ed il cd child grooming, vale a dire l'adescamento dei minori in rete.

Si tratta di fenomeni che danno luogo a problemi diversi riconducibili alla

[1] S. VACCARI e G. BAROZZI REGGIANI, *Gli strumenti di c.d. age verification per la protezione dei minori nell'ecosistema digitale,* in Wolters Klumer, 1.05.2025; M.C. GAETA, *Smart toys and minors' protection in the context of the Internet of everything,* in European Journal of Privacy Law & Technologies, 2020/2; E. BATTELLI, *I soggetti vulnerabili: prospettive di tutela della persona*, in Dir. fam. pers., 2020.

[2] B. AGOSTINELLI, *Informazioni e minori: una lettura integrata per una tutela uniforme*, in Jus civile, 2022; A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Giuffré 2019; G. COSCO, *Protezione e autodeterminazione del minore nell'ambiente digitale*, in Ordine internazionale e diritti umani, 2025; E. BATTELLI, *Il trattamento dei dati nel prisma della tutela della persona minore di età*, in Dir. Inf. e inform., 2022; L. BOZZI, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in Eur. dir. priv., 2020.

medesima esigenza: la tutela dei c.d. web-baby o mobile born[3], vale a dire di coloro che sono nati in un contesto talmente digitalizzato da essere in grado di utilizzare i dispositivi digitali contemporaneamente o addirittura prima di muovere i primi passi. "Il rischio è lasciare scoperte zone in cui siano violati o compromessi i diritti di coloro che sono più deboli non nell'uso del mezzo, rispetto al quale mostrano abilità, ma per una limitata capacità di comprensione sotto il profilo valoriale ed emotivo: più il minore naviga con destrezza, più ha bisogno di protezione"[4].

Negli ultimi anni i legislatori hanno tentato di regolare l'accesso da parte dei minori a contenuti inadeguati, tramite specifici obblighi rivolti ai gestori di siti web e piattaforme. Tra gli atti di derivazione europea che mirano a porre degli argini alle nuove sfide digitali, il presente scritto fa menzione al Regolamento generale sulla protezione dei dati personali[5] (più noto come "RGPD" o con l'acronimo inglese "GDPR"), al Regolamento sui servizi digitali[6] (anche noto come "*Digital service act* o anche "DSA"), agli Orientamenti della Commissione europea sulle misure per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online ed al Regolamento 2024/1689[7], che unitamente alla legge di attuazione nazionale[8] n.132/2025, regola la materia dell'intelligenza artificiale. Più nello specifico, tra le misure di recente introduzione atte a fronteggiare i rischi di un mondo iperconnesso, sono analizzate le misure di accertamento dell'età, previste come obbligatorie nei casi in cui i contenuti proposti dai servizi della società dell'informazione possano nuocere allo sviluppo psicofisico del minore e l'introduzione dell'obbligo della raccolta del consenso del titolare della responsabilità genitoriale per l'accesso ai servizi di intelligenza artificiale da parte di un minore di quattordici anni.

1. Il decreto legge 23 settembre 2025, n.132 (il cd Decreto Caivano)

1.1 L'articolo 13 bis

Con il decreto legge del 13 novembre 2023, n. 159 (cd Decreto Caivano) il Governo italiano ha introdotto il divieto di accesso per i minori a contenuti a carattere pornografico in quanto, alla luce degli effetti lesivi della dignità e pregiudizievoli del benessere fisico e mentale dei minori, sono considerati idonei a costituire un problema di salute pubblica.

La norma si pone nel solco del monito lanciato dalla Commissione europea in ordine all'attuazione di norme mirate alla tutela dei minori online e di quanto previsto dall'articolo 28 del DSA (Digital Services Act), che richiede che tutti i fornitori di piattaforme online adottino misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di

[3] P. HOLLAND, *The rise of the mobile – born*, in TechCrunch, 2013.
[4] M.ZINNO, *Educazione digitale e responsabilità genitoriale*, in Diritto Famiglia e Persone, 2025.
[5] Regolamento 2016/679/UE (GDPR)
[6] Regolamento 2022/2065 del (DSA)
[7] Regolamento 2024/1689
[8] Decreto Legge 23.09.2025, n. 132 coordinato con la legge di conversione 13 novembre 2023, n. 159.

protezione dei minori.

L'articolo 13-*bis* del decreto-legge vieta "l'accesso dei minori a contenuti a carattere pornografico, in quanto individuati come lesivi del rispetto della dignità del minore e idonei a comprometterne il benessere fisico e mentale, pertanto, impone ai gestori di siti web ed ai fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto*"*.

È assegnata all'Autorità per le garanzie nelle comunicazioni il compito di individuare con proprio provvedimento le modalità tecniche e di processo che 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 ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e al rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo.

L'Autorità, che peraltro è competente anche ai sensi del Testo Unico sui Servizi Media Audiovisivi (T.U.S.M.A.) a tutela dei minori rispetto a contenuti che possano nuocere al loro sviluppo fisico, mentale o morale [9], vigila sull'adempimento del prescritto obbligo e in caso di inadempimento ne contesta, anche d'ufficio, la violazione, diffidando i gestori ad adeguarsi entro venti giorni e, nel caso l'inottemperanza persista, adottando il provvedimento utile ai fini del blocco del sito o della piattaforma.

Ai fini dell'attuazione dei prescritti obblighi l'Autorità ha adottato un approccio tecnologicamente neutrale, lasciando agli operatori ampi margini di scelta in ordine alle modalità attraverso cui conseguire il risultato prescritto. Ad ogni modo l'Autorità ha previsto che la prova della maggiore età per accedere a determinati siti o piattaforme web possa essere fornita da soggetti terzi indipendenti certificati, attraverso un processo di verifica che prevede due passaggi logicamente separati: identificazione e autenticazione della persona, per ciascuna sessione di utilizzo del servizio regolamentato.

Nel caso di sistemi di verifica dell'età non basati su applicativi installati nel terminale utente, il provvedimento dell'Autorità [10] specifica che il processo deve essere diviso in tre fasi distinte: identificazione e verifica dell'età da parte di soggetti terzi, fornitura della prova dell'età all'utente e autenticazione. In particolare le fasi previste nello schema di provvedimento dell'Autorità si declinano come segue: dopo l'identificazione avviene l'emissione di una "prova dell'età" rilasciata da soggetti indipendenti dal fornitore di contenuti certificati, in modo da avere garanzie sul sistema di identificazione usato. Tali soggetti possono essere fornitori di servizi specializzati nella fornitura di identità digitale, ovvero un'organizzazione o un soggetto che abbiano identificato l'utente di Internet in un altro contesto. Il soggetto che fornisce la prova dell'età non è a conoscenza dell'utilizzo che della stessa ne farà l'utente. L'esito della prova dell'età è comunicato all'utente sul sito o sulla piattaforma

[9] L'articolo 42, comma 7, del D.lgs 8 novembre 2021, n. 208 (T.U.S.M.A.) recita "I fornitori di piattaforma per la condivisione di video sono in ogni caso tenuti a predisporre sistemi per verificare, nel rispetto della normativa in materia di protezione dei dati personali, l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori".

[10] AGCOM, *Comunicato stampa*, 7.10.2024, Consultabile al sito: *Comunicato stampa del 07.10.2024*

che desidera visitare. I titolari del sito o della piattaforma analizzano la prova e forniscono o negano l'accesso al contenuto richiesto.

Nel caso di sistemi di verifica dell'età basati su applicativi installati sul dispositivo, il soggetto terzo che fornisce la prova dell'età mette a disposizione dell'utente una App per la certificazione e la generazione della prova dell'età. La disponibilità dell'app sul dispositivo dell'utente consente di effettuare l'autenticazione e di fornire la prova dell'età al sito web o alla piattaforma visitata senza passaggi intermedi e limitando la circolazione dei dati personali.

Per aiutare i gestori dei siti e delle piattaforme online ad implementare un metodo di verifica dell'età conforme alla normativa in materia di dati personali, in attuazione delle disposizioni a tutela dei minori online previste dall'articolo 28, par.1, del Digital Services Act il 14 luglio 2025[11] , la Commissione europea ha pubblicato la prima versione di un progetto di verifica dell'età white-label dell'UE.

Il progetto mira a consentire agli utenti, che desiderino accedere a contenuti per adulti per i quali siano previste restrizioni, di dimostrare di avere più di 18 anni senza rivelare altre informazioni personali. La soluzione europea si basa su una tecnologia open source, che quindi potrà essere ulteriormente sviluppata dagli operatori del mercato (fermo restando le funzionalità a tutela della privacy che rimangono immodificabili), e pienamente interoperabile con i futuri portafogli di identità digitale europea (EUDIW).

L'Italia, unitamente alla Spagna, alla Danimarca, alla Francia ed alla Grecia, sarà tra i primi Stati membri a mettere in pratica tale soluzione nella versione pilota.

Dal punto di vista della protezione dei dati personali preme evidenziare che, attraverso l'utilizzo di questa soluzione, i servizi online a cui l'utente desidera accedere ricevono solo la prova della maggiore età senza che vengano trasmessi altri dati personali e che, al contempo, il fornitore della prova non è informato in ordine ai servizi per i quali la stessa viene utilizzata. È infatti adottato il cosiddetto metodo in doppio cieco. Inoltre ogni prova può essere utilizzata una sola volta, per impedire il tracciamento incrociato tra servizi e, tramite esso, dedurre dati inferenziali.

1.2 Il controllo parentale

Al fine di limitare l'accesso dei minori a contenuti ritenuti inadeguati e potenzialmente lesivi allo sviluppo psicofisico del minore, il decreto Caivano ha altresì introdotto nuove disposizioni in materia di controllo parentale. In particolare l'articolo 13 del decreto, dopo aver spiegato che per "controllo parentale" si intende "la possibilità di limitare e controllare, da parte dei genitori o di coloro che esercitano la responsabilità genitoriale, l'accesso ai contenuti e/o alla rete da parte dei minori, mediante la scelta degli spazi digitali e dei tempi di utilizzo", prevede che, per garantire un ambiente digitale sicuro, i produttori debbano assicurare che i sistemi operativi installati nei dispositivi consentano l'utilizzo e includano la disponibilità di applicazioni di

[11] COMMISSIONE EUROPEA, *Plasmare il futuro digitale dell'Europa*, 10.10.2025, Consultabile al sito: *https://digital-strategy.ec.europa.eu*

controllo parentale. Il comma 6 del medesimo articolo specifica altresì che "I dati personali raccolti o generati durante l'attivazione delle applicazioni di controllo parentale non possano essere utilizzati per scopi commerciali e di profilazione". Tale previsione si pone in linea con quanto già previsto in attuazione dell'articolo 7 *bis* del decreto-legge n. 28/2020 e delle linee guida Agcom [12] indirizzate agli operatori che forniscono servizi di comunicazione elettronica, le quali hanno previsto l'obbligo per gli Internet Service Provider (ISP) di rendere disponibile agli utenti, a partire dal 21 novembre 2023, sistemi di controllo parentale volti a garantire a coloro che esercitano la potestà genitoriale la tutela del minore, limitando o bloccando l'accesso alla rete ovvero a contenuti digitali, vietati o valutati inappropriati per i minorenni, che rientrano in specifiche categorie tra cui i contenuti per adulti, le scommesse, le armi ed il gioco d'accordo. A tale scopo i destinatari dell'obbligo possono operare attraverso due soluzioni tecniche: un filtro di rete mediante DNS (c.d. Domain Name System, sistema di rete che traduce gli indirizzi IP in nomi di dominio) e l'installazione di un'apposita applicazione sul dispositivo utilizzato per la navigazione.

2. Orientamenti relativi alle misure per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online

La Commissione europea ha pubblicato, a norma dell'articolo 28, par.4, del DSA, specifici orientamenti relativi agli strumenti online di protezione dei minori[13] in cui si afferma espressamente che "le misure che limitano l'accesso in base all'età sono un mezzo efficace per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione per i minori sulle piattaforme online."

Dal punto di vista del trattamento dei dati personali la Commissione sottolinea come la verifica dell'età costituisca un trattamento di dati separato e distinto rispetto alle altre attività di raccolta svolte dalle piattaforme online e dai gestori dei siti e che questi ultimi non possano conservare ed impiegare le informazioni sulla fascia di età dell'utente per scopi ulteriori rispetto alla suddetta finalità di trattamento.

Tra i metodi di verifica dell'età consigliati dalla Commissione si evidenziano quelli basati su token anonimizzati, la cui emissione deve essere preceduta da una verifica affidabile dell'età della persona da parte di un terzo indipendente rispetto al fornitore del sito o della piattaforma.

La Commissione individua nei protocolli crittografici, come la rotazione delle chiavi e le dimostrazioni a conoscenza zero, le basi adeguate per accertare l'età senza trasmettere dati personali. I token anonimizzati unitamente alla rotazione regolare delle chiavi permettono di far sì che il prestatore del servizio a cui l'utente desidera accedere venga a conoscenza esclusivamente della circostanza per cui l'età del richiedente sia al di sotto o al di sopra di una

[12] AGCOM, *Delibera n. 9/23/CONS*, Consultabile al sito *www.agcom.it* .
[13] COMMISSIONE EUROPEA, *Orientamenti su misure per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online, a norma dell'articolo 28, paragrafo 4, del regolamento (UE) 2022/2065*, 10.10.2025.

determinata soglia, mentre il fornitore terzo fornisce il token che l'utente mostra al primo prestatore, senza conoscere il servizio per il quale esso sarà utilizzato. Al contempo il sistema di rotazione consente di sostituire periodicamente le chiavi di cifratura attive con nuove chiavi per ridurre il rischio di attacchi che compromettano la singola chiave. Con l'espressione "dimostrazione a conoscenza zero", invece, si fa riferimento a quel metodo attraverso cui una parte dimostra all'altra che una determinata affermazione sia vera, senza trasmettere a quest'ultima nessuna informazione se non la conferma circa la veridicità dell'affermazione stessa.

Nel valutare l'adeguatezza e la proporzionalità del metodo di accertamento i fornitori *ex ante* e le autorità di vigilanza *ex post*, devono tener conto del livello di accuratezza con cui il metodo stabilisce l'età dell'utente, l'affidabilità del funzionamento di tale metodo in circostanze reali, la non invasività rispetto ai diritti degli utenti, l'assenza di effetti discriminatori, la sua solidità, la facilità con cui è possibile aggirarlo. Con specifico riferimento a quest'ultimo aspetto si evidenzia come i fornitori dei servizi impieghino molto spesso meccanismi di verifica dell'età basati sull'autodichiarazione dell'utente e come tale prassi sia apertamente sconsigliata sia dalla Commissione che "non considera l'autodichiarazione un metodo di accertamento adeguato per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori conformemente all'articolo 28, paragrafo 1, del regolamento (UE) 2022/2065", che dal Comitato europeo dei garanti che individua nella solidità un requisito in grado di far fronte a situazioni impreviste e di resistere ai tentativi di ingannare o aggirare il sistema[14].

3. Il decalogo dei principi dell'Autorità di protezione dei dati personali spagnola in materia di verifica dell'età e protezione delle persone minori da contenuti inadeguati

A livello europeo si segnalano, ai fini del presente scritto i documenti[15], adottati dall'Autorità di protezione dei dati personali spagnola (Agencia española de protección de datos, di seguito indicata anche come AEPD), che dal 2023 si è espressa a più riprese sul tema della verifica dell'età nel tentativo di illustrare ai titolari ed ai responsabili del trattamento come sia astrattamente possibile garantire una maggior tutela dei minori attraverso sistemi di verifica dell'età degli utenti, nel pieno rispetto del diritto alla riservatezza della generalità dei consociati. Alla luce di tali documenti l'Autorità, da un lato, ha sostenuto di poter esigere la predisposizione di specifiche forme di tutela dei minori da parte dei titolari del trattamento e, dall'altro, ha ribadito che "las pruebas de concepto" (PoC) indicate sono meri prototipi, non rientrando tra i compiti dell'Autorità quello di individuare in modo specifico le soluzioni più idonee.

[14] CEPD, *Dichiarazione 1/2025 sulla garanzia dell'età*, 11.02.2025.
[15] AEPD, *Decálogo de principios Verificación de edad y protección de personas menores de edad ante contenidos inadecuados, 12.02.2023; AEPD, Preguntas frecuentes. Menores y educación*. Consultabile al sito: https://www.aepd.es .

La AEPD ha altresì chiarito che la verifica dell'età e la protezione dell'interesse superiore del minore non costituiscono una base giuridica idonea a legittimare un trattamento ulteriore di dati della persona minore e, al contempo, che la protezione di quest'ultimo non obbliga i fornitori dei servizi a trattare dati personali ulteriori al fine di valutare se il destinatario del servizio abbia una determinata età.

Considerazioni analoghe sono state elaborate da parte della dottrina nazionale italiana che ha più volte sottolineato l'esigenza di bilanciare gli interessi in gioco, onde evitare che l'adozione di un regime di massima tutela a favore dei minori si riveli eccessivamente "sacrificante" per altri soggetti dell'ordinamento[16].

Ad avviso dell'Autorità iberica i sistemi di verifica dell'età sono da ritenersi rispettosi dell'interesse superiore del minore e dei diritti fondamentali della generalità dei consociati, laddove conformi ai principi di seguito indicati:

- Il sistema di protezione del minore da contenuti inadeguati garantisce l'anonimato, vale a dire l'impossibilità di identificare, rintracciare e localizzare i minori, con la conseguenza che l'informazione per cui una persona non sia "autorizzata all'accesso" debba essere trattata in modo da non consentire di dedurre che ci si trovi dinanzi ad un minore sia nel processo di accreditamento dell'autorizzazione che in quello di filtraggio dei contenuti e di analisi della navigazione. A tal fine una possibile soluzione è rappresentata dal trattamento delle informazioni relative alla "persona autorizzata ad accedere" esclusivamente nell'ambito del dispositivo dell'utente e dall'attuazione delle politiche di limitazione dell'accesso, senza ricorrere ai server dei fornitori di servizi o a terzi intermediari e nel pieno rispetto del principio di minimizzazione dei dati personali di cui all'articolo 25, par.2, del RGPD.
- La verifica dell'età è finalizzata a consentire alle persone che abbiano l'età per accedere al servizio di dimostrare il proprio status di "persona autorizzata" e non, viceversa, ad ottenere la dimostrazione dello status di minore.
- L'accreditamento per l'accesso a contenuti inadeguati è anonimo sia per i fornitori di servizi Internet che per le terze parti che lo gestiscono ed il trattamento dei relativi dati è indipendente da quello posto in essere per altri scopi legittimi. Si può supporre che l'anonimato venga a mancare quando vengono utilizzati certificati o attributi riconducibili in modo univoco ad una persona. Permane in ogni caso il compito del fornitore del servizio di utilizzare strategie e misure che non consentano l'identificazione, il tracciamento online e la profilazione della persona.
- L'obbligo di verifica dell'età dell'utente è limitato ai contenuti considerati inadeguati e non interpretato in maniera estensiva, pertanto

[16] S. VACCARI e G. BAROZZI REGGIANI, *Gli strumenti di c.d. age verification per la protezione dei minori nell'ecosistema digitale,* in Wolters Klumer, 1.05.2025; A. SPANGARO*, Tutela dei minori e delle fasce deboli,* in Diritto privato dell'informatica, 2014; M. OROFINO, *Minori e diritto alla protezione dei dati personali*, in Privacy, minori, cyberbullismo, 2018.

la regola generale è la navigazione libera e anonima e l'assenza di forme di accreditamento generalizzate. In caso contrario il trattamento dei dati personali sottostante al processo di verifica dell'età è da considerarsi sproporzionato ed in violazione del principio generale di minimizzazione di cui all'articolo 5 del RGPD.

- La verifica dell'età restituisce esiti certi classificando il richiedente come "persona autorizzata ad accedere"; ciò implica che i meccanismi di verifica dell'età restituiscano valori affidabili e non permettano ai fornitori dei servizi o a terze parti di ricevere dati relativi all'età effettiva di una persona, ovvero dati da cui quest'ultima possa essere identificata.
- Il sistema garantisce che le persone non vengano profilate in funzione delle attività di navigazione. Tale rischio è possibile che si concretizzi attraverso l'etichettatura, sia essa demandata a revisori umani che automatici, in quanto etichettando i contenuti a cui l'utente ha avuto accesso è spesso possibile costruire un profilo dettagliato. L'Autorità spagnola consiglia l'utilizzo di restrizioni di accesso ai siti web a livello locale sui dispositivi degli utenti di Internet al fine di eliminare i rischi di profilazione o monitoraggio. La protezione locale tramite la verifica dell'attributo "persona autorizzata ad accedere", avverrebbe sugli stessi dispositivi, nei sistemi operativi o tramite l'adattamento delle app dei servizi Internet.
- Il sistema garantisce l'esercizio dei poteri attribuiti al titolare della responsabilità genitoriale. È inoltre previsto che le famiglie, le istituzioni scolastiche, le associazioni di protezione dei minori e lo Stato partecipino attivamente nello stabilire i criteri attraverso cui definire ciò che si debba considerare "inadeguato".
- Il sistema di protezione dei minori da contenuti inadeguati garantisce il rispetto dei diritti fondamentali di tutte le persone che accedono ad Internet. Invero qualsiasi limitazione o controllo sullo sviluppo digitale, se non applicato correttamente, può comportare una limitazione dei diritti fondamentali, sia degli adulti che dei minori.
- Il sistema di protezione dei minori da contenuti inadeguati prevede un quadro di governance ben definito che preservi la privacy e garantisca un livello minimo di efficacia, pur considerando che nessun sistema tecnologico sia perfetto. L'efficacia del sistema di governance è valutata in modo obiettivo e critico, includendo nell'analisi gli effetti collaterali che possano ripercuotersi sulle persone e sulla società ed il suo funzionamento è trasparente e verificabile da parte degli utenti, delle autorità e di terzi indipendenti.

4. Il consenso del minore in Europa

In Europa il Digital service act ha introdotto disposizioni specificamente mirate alla protezione dei minori, tra cui la previsione rivolta ai fornitori di piattaforme online, che li obbliga ad adottare misure che garantiscano un elevato livello di riservatezza, sicurezza e protezione dei minori, e ad impiegare strumenti di verifica dell'età e controllo parentale. Il DSA non stabilisce un'età minima uniforme per l'accesso a servizi come i social network, pertanto ogni Paese sta procedendo in modo autonomo nella definizione dei vincoli ai quali i fornitori dovranno attenersi.

L'atto dell'Unione pone la tutela dei minori al centro della strategia europea, la loro esposizione è infatti elencata tra i rischi sistemici di cui i gestori di piattaforme ed i motori di ricerca online di dimensioni molto grandi contemplati dall'art. 35, par. 1, lett. j) del DSA devono tener conto in sede di valutazione d'impatto degli effetti negativi dei loro servizi ed ai fini dell'adozione di soluzioni ragionevoli, proporzionate ed efficaci.

In linea generale il DSA impone limiti ed obblighi afferenti a vari servizi digitali, con regole che variano a seconda del ruolo, delle dimensioni e dell'impatto della piattaforma online. Tra gli scopi perseguiti c'è quello di facilitare la segnalazione e la rimozione di contenuti illegali dalle piattaforme online, con sistemi di reclamo facilmente accessibili e di facile utilizzo, nonché la promozione della trasparenza relativamente ai sistemi di moderazione dei contenuti ed agli algoritmi di raccomandazione.

Sulla base del DSA, nel 2024, la Commissione ha avviato un procedimento formale per valutare se Meta abbia violato le norme a tutela dei minori nell'ambito dei suoi social network, con particolare riferimento allo sfruttamento delle loro debolezze e della loro inesperienza per generare forme di dipendenza[17].

Come anticipato, un aspetto fondamentale della protezione dei minori online è l'età a partire dalla quale i minori possono fornire il proprio consenso al trattamento dei dati personali per accedere alle piattaforme digitali.

In Europa il Regolamento generale in materia di protezione dei dati personali fissa a 16 anni l'età del consenso digitale, laddove il trattamento riguardi l'offerta diretta di servizi della società dell'informazione ai minori e si basi sul presupposto di liceità di cui all'articolo 6, paragrafo 1, lett. a) del RGPD.

Per il trattamento dei dati personali dei minori di età inferiore ai 16 anni da parte delle piattaforme della società dell'informazione è invece richiesta la prestazione del consenso del titolare della responsabilità genitoriale.

L'articolo 8 del RGPD prevede altresì che gli Stati membri possano abbassare l'età del consenso digitale fino a 13 anni, possibilità che, ad oggi, è stata adottata da più della metà degli Stati membri dell'UE[18], compresa l'Italia dove il rinvio è stato recepito nell'articolo 2 *quinquies* del Codice in materia di

[17] F.DEL VECCHIO, *L'Unione europea avvia un'indagine su Meta per la dipendenza social nei bambini,* 16.05.2024, Consultabile al sito: https://www.wired.it. A tale riguardo si segnala la recente sentenza dello Stato del New Mexico emessa contro Meta per la violazione della legge statale sulle pratiche commerciali sleali, segnatamente per aver ingannato i consumatori sulla reale sicurezza dei propri servizi a danno dei minorenni. Notizia consultabile al sito: https://www.repubblica.it , 25.03.2026.

[18] M. NIESTADT, *Protecting children online Selected EU, national and regional laws and initiatives*, in European Parlamentary y Research Services, 04.2025

protezione dei dati personali[19], che fissa a 14 anni il limite per esprimere il consenso al trattamento dei propri dati personali. Si tratta di una capacità giuridica *sui generis* che rappresenta una regola di validità per accordi atipici di somministrazione di servizi digitali, il cui corrispettivo spesso è rappresentato dalla cessione dei dati. La c.d. maggiore età digitale è stata sin da subito frutto di critiche da parte della dottrina, che ritiene che l'articolo 2 *quinquies* del Codice risponda più alle esigenze dell'economia digitale che alla esaltazione della reale autodeterminazione del minore[20].

4.1.1. Il consenso digitale del minore in Italia

Attualmente in Italia è in corso di esame in Commissione la proposta di legge presentata nel 2024[21], che prevede la riforma della disciplina della tutela dei minori online, *in primis* attraverso l'abrogazione dell'articolo 2 *quinquies* del Codice.

La proposta parte dalla premessa per cui il modello di business più diffuso nella dimensione digitale sia rappresentato dallo scambio di dati personali contro servizi; viene infatti citato il provvedimento dell'Autorità garante della concorrenza e del mercato n. 27432 del 29 novembre 2018[22] con il quale è stato intimato alla società Facebook (oggi Meta) di non promuovere i propri servizi come gratuiti, dal momento che la loro fornitura ha come corrispettivo lo sfruttamento commerciale dei dati personali degli utenti[23]. Nel provvedimento i parlamentari proponenti invitano a prendere atto della circostanza per cui nella dimensione digitale dovrebbe essere naturale prevedere un'età minima per la fruizione di determinati contenuti e servizi, al pari di quanto accade per una serie di attività che si svolgono nel mondo analogico, come la somministrazione di alcool e tabacco.

L'obiettivo della legge proposta è imporre un obbligo di verifica dell'età degli utenti ed incaricare l'Autorità per le garanzie nelle comunicazioni (AGCOM) di stabilire, sentito il Garante per la protezione dei dati personali, le modalità tecniche da adottare per l'accertamento dell'età di coloro che

---

[19] A.ASTONE, *L'accesso dei minori di età ai servizi della c.d. Società dell'informazione: l'art.8 del Reg. (UE)2016/679 e i suoi riflessi sul Codice per la protezione dei dati personali,* in Contratto e Impresa, 2019; I.A.CAGGIANO, *Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law.,* in European Journal of Privacy Law & Technologies, 2022/1; G. RESTA, V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in Riv. trim. dir. proc. civ., 2018; A. ANNONI, A. THIENE, *Minori e* privacy. *La tutela dei dati personali dei bambini e degli adolescenti alla luce del regolamento (UE) 2016/679*, Jovene Editore, 2019.

[20] M.ZINNO, *Educazione digitale e responsabilità genitoriale*, in Diritto di Famiglia e delle Persone, 2025; D. POLETTI, *Soggetti deboli*, in Enc. dir., Annali, VII, 2014; F. RUGGERI, *Minori e privacy*, in Diritto Privato delle Persone Minori di età, 2021.

[21] CAMERA DEI DEPUTATI PROPOSTA DI LEGGE N. 1863, *Disposizioni per la tutela dei bambini e degli adolescenti nell'utilizzo degli strumenti digitali,* 13.05.24

[22] Si precisa che il provvedimento de quo è stato confermato, seppur parzialmente, dalle sentenze del tribunale amministrativo regionale del Lazio n. 260 del 10 gennaio 2020 e dal Consiglio di Stato n. 2360 del 29 marzo 2021.

[23] Sul punto si vedano C.IRTI, *Consenso negoziato e circolazione dei dati personali*, Giappichelli, 2021; R. SENEGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali,* in Contratto e Impresa, 2020; V. RICCIUTO, *Consenso al trattamento e Contratto*, in Persona mercato, 2024.

vogliano fruire di determinati servizi, nel rispetto del principio di minimizzazione dei dati personali di cui all'articolo 5, paragrafo 1, lettera c), del RGPD. Tale obbligo troverebbe applicazione nei riguardi di tutti i fornitori di servizi della società dell'informazione che operano in Italia, a prescindere dal luogo di stabilimento, e che registrino un numero di accessi mensili superiore a quello stabilito dall'AGCOM.

Alla luce dell'articolo 3 della proposta di legge i contratti conclusi tra i fornitori di servizi della società dell'informazione ed i minori di anni quindici sarebbero nulli ed inidonei a costituire una idonea base giuridica per il trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b) del RGPD, salvo che sia stato validamente prestato il consenso, per conto dei minori medesimi, da chi esercita la responsabilità genitoriale o dal tutore.

L'onere di provare che i contratti siano stati conclusi da minori con più di quindici anni ovvero, nel caso di minori di anni quindici, da chi esercita la responsabilità genitoriale o dal tutore, ricadrebbe sul fornitore del servizio.

4.1.2 Il consenso ai sensi dell'articolo 4, comma 4, della legge italiana in materia di intelligenza artificiale

Il legislatore della legge n.132/2025 individua il consenso del minore di almeno quattordici anni ovvero del titolare della responsabilità genitoriale come misura minima per garantire un accesso sicuro ai servizi di intelligenza artificiale, rinviando a quanto previsto dal Regolamento generale 2016/679 e dal Codice in materia di protezione dei dati personali la definizione dei requisiti dell'atto autorizzativo[24].

Si osserva come un filone della dottrina italiana stia di fatto mettendo in dubbio la possibile operatività di tale previsione normativa, in quanto ritenuta in contrasto con la norma del diritto italiano dei contratti, che riconosce la capacità di agire al compimento del diciottesimo anno di età (articolo 2 del Codice civile). La tesi si fonda sulla considerazione per cui il consenso negoziale debba essere tenuto distinto da quello ai sensi dell'articolo 8 del RGPD e che il contratto di utenza stipulato tra il minore ed un fornitore di servizi di IA non possa essere annoverato tra gli atti minuti della vita quotidiana e considerarsi funzionale all'esercizio delle libertà fondamentali[25].

Alla luce dell'articolo 4, comma 4, della recente normativa il consenso assume centralità assoluta, essendo individuato *ex lege* come la base giuridica per eccellenza per l'accesso alle tecnologie di intelligenza artificiale da parte dei minori di anni quattordici e per il conseguente trattamento dei dati personali.

Il considerando 75 del RGPD, nel rappresentare i rischi di cui il titolare del trattamento deve tener conto al fine di adottare misure di protezione idonee, identifica i minori come soggetti vulnerabili incapaci di riconoscere i pericoli e

---

[24] Sul punto si vedano l'articolo 7 Regolamento generale 2016/679 del EDPB e le Linee guida N.5/2020 sul consenso ai sensi del regolamento (UE) 2016/679. Versione 1.1 adottate il 4.05.2020. Consultabili al sito: www.edpb.com

[25] C.ARMONE, *L'uso dei servizi di intelligenza artificiale da parte dei minori: solo una questione di "age verification?"*, in Diritto di Internet, 2024.

le conseguenze derivanti dall'elaborazione delle informazioni che li riguardano. Il minore è ritenuto vulnerabile in quanto "persona in formazione", sensibile ai meccanismi di gratificazione, condizionato dal giudizio altrui e, per questo, privo di un giudizio ponderato e critico.

Il RGPD, pertanto, prevede una tutela rafforzata, *in primis* attraverso il rispetto degli obblighi informativi, di cui il titolare deve tenere debitamente conto fornendo all'interessato minore informazioni chiare e precise, calibrate in un linguaggio tale da porre rimedio all'asimmetria cognitiva di quest'ultimo rispetto ai fornitori dei servizi. Si tratta dei medesimi obblighi informativi contemplati dalla legge nazionale in materia di intelligenza artificiale che, tuttavia, sembra limitarne l'operatività solo laddove il minore presti il proprio consenso e non anche nel caso in cui il trattamento dei suoi dati personali si basi sull'atto autorizzativo del titolare della responsabilità genitoriale. L'articolo 4 della legge n.132/2025 infatti prevede che "il minore di anni diciotto, che abbia compiuto quattordici anni, possa 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." Viceversa si osserva come la normativa privacy preveda il rispetto di quest'ultima condizione, quindi l'adempimento degli obblighi informativi di cui agli articoli 12, 13 e 14 del RGPD, anche laddove il trattamento non si basi sul consenso del minore. L'obiettivo è permettere al minore di avere il pieno controllo dei suoi dati, anche quando l'atto autorizzativo non provenga da lui, tenuto conto del fatto che al momento del raggiungimento dell'età del consenso digitale potrà confermare, modificare o revocare il consenso prestato e che in assenza di una qualsiasi di queste azioni il consenso rimarrà un valido presupposto ai fini del trattamento.

In tal senso appare significativo l'intervento del 2021 del Garante per la protezione dei dati personali, che ha contestato alla società tecnologica cinese ByteDance, titolare del social network TikTok, tra le altre, la violazione degli obblighi informativi previsti dalla normativa a causa dell'utilizzo di un linguaggio standardizzato, poco chiaro e di difficile lettura per i minori.

In tale occasione l'Autorità ha ricordato che quando un servizio è rivolto ai minori è indispensabile fornire le informazioni relative al trattamento dei dati in un linguaggio tale da poter essere facilmente compreso dal minore.

Si osserva inoltre come il provvedimento adottato dal Garante[26], nei confronti della società cinese Tik Tok, si soffermi anche sulle modalità per l'accertamento dell'età anagrafica degli iscritti alla piattaforma, considerate lacunose *ex* articolo 25, paragrafo 1, del RGPD e tali da giustificare un intervento in via d'urgenza dell'Autorità, ai sensi del combinato disposto dagli articoli 58, par. 2, lett. f) e 66, par. 1 del Regolamento, volto a limitare provvisoriamente il trattamento ed a vietare l'ulteriore trattamento dei dati degli utenti presenti sul territorio italiano per i quali non vi fosse assoluta certezza dell'età.

Dal punto di vista procedurale si evidenzia come l'attivazione della procedura d'urgenza prevista dall'articolo 66 del Regolamento abbia consentito all'autorità nazionale di adottare, in luogo della autorità capofila

[26] GPDP, *Provvedimento 22 gennaio 2021, n.20, [doc. web n. 9524194*], Consultabile al sito www.gpdp.it

irlandese, misure provvisorie intese a produrre effetti giuridici nel proprio territorio, con un periodo di validità determinato non superiore a tre mesi.

4.2. Il consenso digitale del minore in Francia

Nell'aprile 2024 il Presidente Emmanuel Macron ha tenuto un discorso[27] presso l'Università Sorbona di Parigi dove ha dichiarato che avrebbe sostenuto la fissazione dell'età minima per l'accesso al digitale a quindici anni a livello europeo, trovando appoggio anche da parte di altri leader europei come il ministro danese, Mette Frederiksen[28], che ha espresso il desiderio che l'Unione europea preveda il limite di età a quindici anni per l'accesso ai social media.

A distanza di pochi anni in Francia è stato approvato il disegno di legge n.2107 volto a proteggere i minori dai rischi a cui sono esposti tramite l'uso dei social network, che inibisce l'accesso alle piattaforme social ai minori di quindici anni ("Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux") [29]. La legge sarà prossimamente discussa in Senato per il voto finale. Rimangono escluse dalla previsione normativa le enciclopedie online ed i repertori educativi e scientifici. L' Autorità di regolamentazione della comunicazione audiovisiva e digitale è incaricata di vigilare sul rispetto della norma, alle condizioni previste dal capitolo IV del DSA.

4.3. Il consenso digitale del minore in Spagna

In occasione del World Governments Summit il Presidente spagnolo Pedro Sanchez ha recentemente annunciato un piano per limitare l'accesso dei minori ai social network[30]. Il governo spagnolo intende adottare un pacchetto di cinque misure legislative per fronteggiare gli abusi delle grandi piattaforme e garantire un contesto digitale sicuro, democratico e rispettoso dei diritti fondamentali. Tali misure pongono particolare attenzione alla protezione dei più piccoli ed al miglioramento del controllo delle reti social a partire dal divieto di accesso alle medesime da parte dei minori di sedici anni, obbligando i titolari delle piattaforme ad adottare efficaci sistemi di verifica dell'età.

La previsione di una maggiore età per l'accesso alle piattaforme, che passerebbe dagli attuali quattordici ai sedici anni, è in linea con quanto suggerito nel 2024 dal Comitato di esperti per lo sviluppo di un ambiente digitale sicuro per i giovani e i bambini istituito in Spagna il 1° febbraio 2024 con i compiti di redigere una relazione che analizzi le buone pratiche in materia, indicare i principali rischi e pericoli che i minori possano incontrare nell'ambiente digitale e formulare raccomandazioni. Nel documento prodotto

[27] E. MACRON, *Bilancio dell'azione europea da parte del Presidente della Repubblica francese,* in Eliseo 24.04.24, Consultabile al sito: https://www.elysee.fr
[28] M.POLLET, *Danish PM calls for 15+ age limit for social media in EU*, in Politico, 27.05.24, Consultabile al sito: https://www.politico.eu
[29] A.ALU', *Francia, divieto di social agli under 15: cosa prevede la nuova legge,* 2.02.26, Consultabile al sito: https://www.agendadigitale.eu/
[30] MINISTERIO PARA LA TRANSFORMACION DIGITAL Y LA FUNZION PUBLICA, *España planea prohibir el acceso a redes sociales a menores de 16 años,* 13.02.26. Consultabile al sito: https://espanadigital.gob.es

dal Comitato[31] nel 2024 si legge che l'articolo 7 della Legge Organica 3/2018 sulla protezione dei dati personali individua i quattordici anni come età minima per il consenso al trattamento dei dati personali da parte dei minori, ma che è opportuno elevare tale soglia a sedici anni. Il cambiamento, secondo quanto espresso dal Comitato, si fonderebbe sulla considerazione per cui l'evoluzione della tecnologia digitale richiede una maturità sempre maggiore nell'uso dei servizi, delle piattaforme e dei sistemi e sul fatto che l'utilizzo precoce di tali strumenti possa dar luogo a gravi pregiudizi di natura fisica, mentale, psicosociale e sessuale.

Tra i rapporti che riflettono l'impatto dell'uso inappropriato dei servizi della tecnologia digitale da parte dei minori, il Comitato fa menzione della relazione nazionale "Uso di internet e malattie nei bambini e negli adolescenti in Spagna dal 1997 al 2021" [32] , della relazione dell'UNICEF titolata "L'esposizione dei bambini e degli adolescenti a messaggi di odio e immagini violente online"[33], del documento prodotto dall'osservatorio nazionale della tecnologia (ONTSI) sull'impatto dell'aumento dell'uso di internet e delle reti sociali sulla salute mentale dei giovani e degli adolescenti[34] e delle risultanze del gruppo di lavoro istituito presso l'Autorità spagnola di protezione dei dati personali denominato "minori, salute digitale e riservatezza", nell'ambito del quale è stata manifestato un *favor* rispetto all'aumento della maggiore età del consenso da quattordici a sedici anni.

Risulta particolarmente interessante ai fini del presente scritto l'elenco dei rischi menzionati dal Comitato al fine di giustificare la necessità di un intervento normativo multiplo, che comprenda quello finalizzato all'aumento dell'età digitale. In particolare sono indicati: i danni psicologici ed emotivi causati dalla mancanza di maturità ed autostima del minore in fase di sviluppo, carenze che rendono il minore incapace di assimilare e di reagire adeguatamente dinanzi a contenuti pornografici o violenti; la disinformazione, la manipolazione e la creazione di false credenze, segnatamente i contenuti falsi relativi alla salute ed alla sicurezza che possono confondere i minori e rivelarsi particolarmente dannosi; l'adozione di comportamenti pericolosi o socialmente inappropriati causati dall'influenza di contenuti sessisti, omofobi e razzisti, che rischiano essere considerati dal minore come modelli positivi; i danni alla salute fisica generati dai contenuti che promuovono abitudini alimentari malsane o veri e propri disturbi, come anoressia, bulimia e comportamenti autolesionistici; l'inclusione in gruppi estremisti, violenti o razzisti, nonché in sette di carattere ideologico o religioso; l'accesso a contenuti

---

[31] MNISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES CON LAS CORTES, MINISTERIO DE JUVENTUD Y INFANCIA, MINISTERIO PARA LA TRANSFORMACION DIGITAL Y DE LA FUNZION PUBLICA, MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030, *Anteproyecto de ley orgánica para la protección de las personas menores de edad en los entornos digitales - Memoria del análisis de impacto normativo,* 2024. Consultabile al sito: www.mpr.gob.es

[32] OBSERVATORIO DE LA INFANCIA Y DE LA ADOLECENCIA, *Uso de Internet y enfermedad mental en niños y adolescentes en España 1997-2021,* in SiiS Servicio de Información e Investigación Social, 2024. Consultabile al sito: https://www.observatoriodelainfancia.es

[33] D.KARDEFELT WINTHERA, M.STOILOVAB, M.BÜCHIA, R.TWESIGYEA, D.SMAHELC, M.BEDROSOVÁC, S.LIVINGSTONEB, *L'esposizione dei bambini e degli adolescenti a messaggi di odio e immagini violente online,* 2024. Consultabile al sito: https://www.unicef.it

[34] ONTSI, *Impacto del aumento del uso de Internet y las redes sociales en la salud mental de jóvenes y adolescentes*, 2023, Consultabile al sito: https://www.ontsi.es

inappropriati relativi a droghe, sesso e giochi d'azzardo idonei a favorire disturbi e dipendenze, a causa dell'assenza di una capacità critica tale da consentire al minore di gestire le sollecitazioni derivanti da tali attività; le frodi o i tentativi di inganno volti a truffare i minori per ottenere denaro o dati ed a generare il bisogno di acquisti compulsivi.

4.4. Il consenso dei minori in Australia e in Nuova Zelanda

Il 10 dicembre in Australia è entrata in vigore la prima legge al mondo che obbliga le piattaforme social ad impedire l'accesso degli adolescenti ai propri servizi. La Online Safety Amendment approvata dal Parlamento di Canberra obbliga i fornitori dei servizi social, come Facebook, Instagram, TikTok, YouTube, X, Snapchat e Reddit, ad adottare misure ragionevoli per impedire ai minori di sedici anni di creare o mantenere account social. [35] La normativa australiana non prescrive misure specifiche e in un'ottica di minimizzazione del trattamento prevede di evitare controlli laddove dall'analisi dei dati già in possesso delle Società che forniscono il servizio si possa desumere la maggiore età dell'utente, come nel caso in cui l'anzianità del profilo dimostri indirettamente che quest'ultimo sia stato creato più di sedici anni prima. Inoltre è previsto che le piattaforme predispongano sistemi per contestare eventuali errori di determinazione dell'età e consentire agli utenti la scelta tra più metodi di verifica. La ministra delle comunicazioni australiana ha apertamente ammesso che nessuna soluzione potrà essere efficace al 100%, soprattutto all'inizio, ma che è importante fare un primo passo verso la regolamentazione per evitare che le piattaforme prendano il sopravvento[36].

Negli ultimi mesi anche altri Paesi hanno introdotto, o stanno valutando di introdurre, misure volte a limitare l'accesso dei minori alle piattaforme di social network. L'obiettivo è mitigare i rischi associati all'esposizione precoce ai social media, come il cyberbullismo, il loro utilizzo potenzialmente compulsivo e l'elevata vulnerabilità dei più fragili nei confronti di soggetti malintenzionati[37].

Sulla scia dell'Australia anche la Nuova Zelanda sta lavorando per vietare l'accesso ai social media da parte dei minori. La proposta di legge prevede il divieto di creare nuovi account per i minori di sedici anni e sanzioni fino a 2 milioni di dollari in caso di mancato rispetto dell'obbligo[38].

5. Considerazioni conclusive

L'analisi delle restrizioni imposte dai diversi Stati volte a limitare l'accesso dei minori a determinati servizi del mondo digitale mette in luce rilevanti criticità sotto il profilo sia dell'implementazione pratica sia

[35] R.PICCOLO, *Social network vietati ai minori di 16 anni, in Australia entra in vigore la prima legge al mondo (con molti dubbi)*, 9.12.2025, Consultabile al sito: https://www.wired.it
[36] C.ANDERSON, *ESafety commissioner hits back at US politician's 'zealot for global takedowns' claim*, 3.12.2025, Consultabile al sito: www.sbs.com.
[37] A.FRAU, *Divieti social ai minori, quali Paesi li hanno e quali stanno per introdurli*, 18.02.26, Consultabile al sito: https://www.agi.it
[38] S. GRIERSON, *Access Denied: New Zealand's proposed social media ban for under-16s*, 6.05.2025, Consultabile al sito: www.simpsongrierson.com

dell'efficacia di tali limiti. Tali misure, spesso fondate su divieti generalizzati o su meccanismi di controllo dell'età facilmente eludibili[39], rischiano infatti di rivelarsi inadeguate rispetto alla complessità dell'ecosistema digitale contemporaneo.

Risulta dunque necessario affiancare agli strumenti proibitivi interventi di natura regolatoria, pubblici e privati, articolati e sistemici, capaci di incidere sulle responsabilità dei fornitori di servizi digitali e sulla progettazione degli ambienti online, nonché un coinvolgimento attivo delle famiglie e delle istituzioni educative, chiamate a svolgere un ruolo centrale nella promozione di un uso consapevole e responsabile delle tecnologie digitali. Solo un approccio integrato, che combini regolazione pubblica e privata, responsabilizzazione degli operatori ed educazione digitale, può garantire una tutela effettiva dei minori senza sacrificare in modo eccessivo le opportunità a loro offerte dal mondo digitale.

Ciò posto, oltre a dover considerare che, di fatto, risulta irrealistica e poco praticabile la totale astinenza digitale dei minori[40], appare utile sia interrogarsi sull'opportunità di tali divieti, non essendoci ad oggi prove scientifiche che dimostrino che l'inibizione di servizi come i social network porti le nuove generazioni ad interagire in modo più diretto e sano con i loro coetanei e le attragga verso i mondi della lettura e dello sport, sia considerare che spesso per alcuni ragazzi in difficoltà i servizi digitali si rivelano salvifici. Bisognerebbe poi chiedersi quali possano essere le possibili conseguenze di una conoscenza improvvisa di taluni spazi del web da parte di un adolescente che sino ad una certa età non abbia maturato alcuna esperienza che gli consenta di gestire in modo corretto determinati contenuti, ovvero di distinguere video o immagini reali da quelle create tramite strumenti di intelligenza artificiale.

La nota rivista liberale The Economist[41] si è recentemente espressa sul tema sostenendo che le restrizioni legali siano deboli e le loro conseguenze negative: proibire l'accesso non eliminerebbe il problema, ma, al contrario, spingerebbe gli adolescenti verso un uso meno controllato di alcuni servizi dal contenuto inadeguato.

Tali considerazioni suggeriscono l'instaurazione di un sistema complesso che comprenda interventi pubblici - non meramente repressivi[42] – e privati,

---

[39] J. WARMUND, *Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act,* in Fordham Intellectual Property Media & Entertainment Law Journal*,* 01.11, 2001.

[40] F.SCIA, *Diritti dei minori e responsabilità dei genitori nell'era digitale,* in Edizioni Scientifiche Italiane, 06.2020.

[41] THE ECONOMIST, *Don't ban teenagers from social media Restrictions would do more harm than good*, 12.02.26, in The Economist; *Should teenagers be banned from social media? - Readers responded in droves to our argument that young people's internet access should not be restricted*, 23.02.26, in The Economist;

[42] A tale riguardo si segnala il Joint Statement on AI – Generated Imagery and Protection of Privacy, sottoscritto da 61 Autorità per la protezione dei dati di tutto il mondo e pubblicato il 23 febbraio 2026. Nella dichiarazione i co-firmatari hanno ricordato a tutte le organizzazioni che sviluppano e utilizzano sistemi di generazione di contenuti basati sull'IA come gli stessi debbano essere sviluppati e utilizzati in conformità con i quadri giuridici applicabili, comprese le norme sulla protezione dei dati e sulla privacy. Segnatamente sono stati ribaditi i seguenti obblighi: 1) l'implementazione di solide misure di sicurezza per prevenire l'uso improprio di informazioni personali e la generazione di immagini intime non consensuali e altri materiali dannosi, in particolare quando sono raffigurati bambini; 2) la garanzia di trasparenza; 3) l'adozione di meccanismi efficaci e accessibili, che consentano agli individui di richiedere la rimozione di contenuti dannosi che coinvolgono informazioni personali e rispondere rapidamente a tali richieste. In sintesi, i partecipanti hanno invitato le organizzazioni che sviluppano ed utilizzano sistemi di

oltre che la riscoperta del ruolo delle famiglie[43] e delle scuole. In alternativa alla censura, come suggerito anche dalla rivista inglese, i regolatori potrebbero obbligare le Big tech a condividere dati su come i giovani usino i loro prodotti, a riprogettare le funzionalità che creino dipendenza [44] ed a rafforzare i meccanismi di moderazione dei contenuti e quelli di verifica dell'età. Per conformare la tecnica al rispetto della persona del minore il modello legislativo, formale e settoriale, caratterizzato da regole e soluzioni rigide, dovrebbe quindi essere affiancato da strumenti regolatori privati [45] , come la co-regolamentazione[46] mediante i codici di condotta[47]. Secondo alcuni giuristi[48], infatti, il diritto privato regolativo costituisce un necessario presupposto di effettività[49], tenuto conto che, in virtù del principio di vicinanza al rischio, i soggetti privati siano i più adatti a garantire la compatibilità dei loro servizi all'identità ed alla dignità della persona.

In sintesi, si ritiene che siano inefficaci, quindi da escludere, divieti drastici. Di contro la tutela dei minori nello spazio digitale non può prescindere da un approccio basato sulla regolamentazione diffusa ed intelligente, ossia da un sistema regolativo complesso, condotto da attori pubblici e privati e dalla riscoperta del ruolo delle istituzioni scolastiche e delle famiglie, a cui è demandato il compito di fissare i riferimenti valoriali della coscienza dei più piccoli anche nella dimensione digitale[50] e di gestire i loro primi contatti con le reti social in modo sicuro e graduale.

Invero anche laddove si raggiunga una maggiore sicurezza nell'ambiente

---

IA a collaborare in modo proattivo con gli enti regolatori, ad attuare solide misure di salvaguardia fin dall'inizio delle attività di trattamento dei dati ed a garantire che il progresso tecnologico non vada a scapito della privacy, della dignità, della sicurezza e di altri diritti fondamentali.

[43] G. CASSANO, *La responsabilità genitoriale nell'uso dell'odierna tecnologia telematica*, in Famiglia e diritto, 2020.

[44] D.PUENTE, *WhatsApp Under 13: Guida agli account gestiti dai genitori*, in Open, 11.03.2026. Consultabile al sito: https://www.open.online. A tale riguardo si segnala che la Società ha annunciato che la nuova funzione di parental control implementata su Whatsapp consentirà ai genitori un maggior controllo dei loro bambini: attraverso la configurazione del telefono acquistato per il minore, il titolare della responsabilità genitoriale potrà decidere chi può contattare l'account e in quali gruppi lo stesso può entrare a far parte. Inoltre, attraverso tale configurazione, sarà possibile controllare le richieste di messaggi da parte di contatti sconosciuti e gestire le impostazioni sulla privacy dell'account, personalizzando l'esperienza di utilizzo del minore.

[45]R. SENEGAGLIA, *Il dovere di educare i figli nell'era digitale,* in Persone e Mercato, 2021.

[46] Nel parere 2015/C 291/05 del Comitato economico e sociale europeo (CESE) sul tema "Autoregolamentazione co-regolamentazione nel quadro legislativo dell'UE) definisce la co-regolamentazione come una forma di regolamentazione delle parti interessate che è promossa, orientata, guidata, o controllata da una terza parte (sia essa un organismo ufficiale o una autorità indipendente) di norma dotata di poteri di esame, di controllo, e in alcuni casi, sanzionatori, 4.09.2015

[47]A tale riguardo si segnala il Children's Code entrato in vigore nel Regno Unito il 2 settembre 2021: un codice di condotta elaborato dall'autorità amministrativa a tutela dei dati personali - Information Commissioner's Office, ICO, con funzione interpretativa ed applicativa delle norme in materia ed un effetto indiretto vincolante.

[48] P. PERLINGIERI, *La libertà di educazione,* Edizioni Scientifiche Italiane, 1987.

[49] R. SENIGAGLIA, *Il dovere di educare i figli nell'era digitale*, in Persona e Mercato, 2021.

[50] C.DE DOMENICO, *Diritti e tutele del minore nella realtà digitale*, in Jus Civile, 2025. Con riferimento al ruolo delle famiglie ed all'ausilio che le stesse devono ricevere da parte dello Stato ai fini dello svolgimento dei compiti di cui sono incaricate si ricorda il preambolo della Convenzione di New York sui diritti del fanciullo del 20 novembre 1989, che afferma "che la famiglia, unità fondamentale della società e ambiente naturale per la crescita e il benessere di tutti i suoi membri e in particolare dei fanciulli, deve ricevere la protezione e l'assistenza di cui necessita per poter svolgere integralmente il suo ruolo nella collettività, riconoscendo che il fanciullo, ai fini dello sviluppo armonioso e completo della sua personalità deve crescere in un ambiente familiare in un clima di felicità, di amore e di comprensione".

digitale che ospita i minori, l'inferenza parentale e l'esercizio del compito fondamentale di sorveglianza appaiono insormontabili per garantire il best interest [51] del minore che non abbia maturato sufficienti capacità di discernimento e di comprensione rispetto ai rischi del web. Acquisita tale capacità, conformemente a quanto stabilito dai principi di matrice internazionale, *in primis* dall'articolo 12 della Convenzione di New York, le opinioni espresse dal minore su questioni che lo interessano, invece, dovranno essere prese in considerazione in linea con il suo effettivo grado di maturità.

[51] L'interesse superiore del minore, criterio guida per il legislatore e per l'interprete in tutte le questioni che riguardano i minori di età, è stato proclamato: nell'art. 3, par. 1, della Convenzione sui diritti del fanciullo di New York del 20 novembre 1989, ratificata in Italia con la legge 27 maggio 1991, n. 176.