I minori sulla rete: un problema di natura costituzionale

Bianca Pileggi*

CHILDREN ON THE INTERNET: A CONSTITUTIONAL PROBLEM

ABSTRACT: The article addresses the complex issue of protecting minors in the digital age, highlighting its constitutional implications. It examines how the Digital Services Act (DSA) has revitalized the issue of safeguarding children's rights online and how proceedings have been initiated against some digital giants for allegedly being harmful to minors. The discussion includes the historical context of digital maturity laws, comparing the Children's Online Privacy Protection Act (COPPA) with the European General Data Protection Regulation (GDPR). It concludes by invoking the doctrine of "constitutional precaution", which argues that the protection of minors' fundamental rights should be guaranteed in the design of new technologies, emphasizing the need to balance protection measures with the safeguarding of young users' rights.

KEYWORDS: Children protection; vulnerability; Digital Services Act; age verification systems; Constitutional Law.

ABSTRACT: L'articolo affronta la complessa questione della protezione dei minori nell'era digitale, sottolineandone le implicazioni costituzionali. Esamina come il Digital Services Act (DSA) abbia dato nuova linfa al tema della salvaguardia dei diritti dei bambini *online* e come siano stati avviati procedimenti contro i alcuni colossi del digitale proprio con l'accusa di essere dannosi per i minori. Viene inoltre delineato il contesto storico delle leggi sulla maturità digitale, confrontando il *Children's Online Privacy Protection Act* (*COPPA*) con il Regolamento Generale sulla Protezione dei Dati (*GDPR*) europeo. Si conclude facendo appello alla dottrina della "precauzione costituzionale", affinché la protezione dei diritti fondamentali dei minori possa essere garantita nella progettazione di nuove tecnologie, sottolineando la necessità di operare un bilanciamento tra istanze di tutela e garanzia dei diritti dei giovani utenti.

PAROLE CHIAVE: Protezione dei minori; vulnerabilità; Digital Services Act; sistemi di verifica dell'età; diritto costituzionale.

SOMMARIO: 1. Il caso: la Commissione europea apre i primi procedimenti ai sensi del DSA contro TikTok e Meta per violazione delle norme a tutela dei minori – 2. L'accesso a Internet dei minori: ovvero come i tredici anni sono diventati l'età della "maturità digitale" – 2.1. Il *Children's Online Privacy Protection Ac*t del 1998 – 2.2. Dal COPPA al GDPR – 3. Uno sguardo comparato: il contenzioso negli Stati Uniti – 4. Oltre la *privacy*: gli "*age verification*

* *Dottoranda di Diritto costituzionale, Università di Firenze. Mail: bianca.pileggi@unifi.it.* *Contributo sottoposto a doppio referaggio anonimo.*

system" – 5. I minori sulla rete: un problema di "precauzione" costituzionale.

1. Il caso: la Commissione europea apre i primi procedimenti ai sensi del DSA contro TikTok e Meta per violazione delle norme a tutela dei minori

A partire da agosto 2023 il *Digital Services Act*[1], il regolamento europeo sui servizi digitali, si applica alle piattaforme designate con oltre 45 milioni di utenti nell'UE[2] (il 10% della popolazione europea), vale a dire le piattaforme (VLOP) o i motori di ricerca *online* (VLOSE) di dimensioni molto grandi[3].

Con il nuovo regolamento sui servizi digitali il legislatore europeo ha dimostrato sensibilità al tema della tutela dei minori[4] nel contesto digitale prevedendo espressamente obblighi di protezione nei confronti degli utenti più giovani da parte dei fornitori di servizi digitali[5], nonché imponendo alle piattaforme e ai motori di ricerca *online* di dimensioni molto grandi obblighi più stringenti in relazione alla valutazione dei rischi[6] derivanti dall'utilizzo delle piattaforme tenendo in considerazione «qualsiasi

[1] Il Digital Services Act (DSA) è il 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). L'applicazione generalizzata dal DSA a tutte le piattaforme è avvenuta a partire dal 17 febbraio 2024.
Il DSA, insieme al Digital Markets Act (DMA), il Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), fa parte di un pacchetto di norme che l'Unione europea ha inteso adottare al fine di raggiungere due obiettivi principali: creare uno spazio digitale più sicuro in cui siano tutelati i diritti fondamentali di tutti gli utenti dei servizi digitali; stabilire condizioni di parità per promuovere l'innovazione, la crescita e la competitività, sia nel mercato unico europeo che a livello globale. Vd. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (ultima consultazione 22/07/2024).

[2] Articolo 33 del DSA.

[3] Per quanto riguarda il DSA, infatti, vengono distinte le regole applicabili alle cosiddette VLOP (Very Large Online Platforms) o VLOSE (Very Large Online Search Engines), ovverosia piattaforme che abbiamo più di quarantacinque milioni di utenti, da quelle applicabili a tutti gli altri prestatori di servizi intermediari. Sulla distinzione tra VLOP e VLOSE e le altre piattaforme s.v. J. VAN HOBOKEN ET AL, *Putting the Digital Services Act Into Practice: Enforcement, Access to Justice, and Global Implications*, in *Amsterdam Law School Research Paper*, 13, 2023, disponibile in: https://verfassungsblog.de/books/; E. LONGO, *Libertà di informazione e lotta alla disinformazione nel Digital Services Act*, in *Giornale di diritto amministrativo*, 6, 2024, 737-745.

[4] Il DSA fa parte della nuova strategia europea per un *Internet migliore per i ragazzi* adottata a maggio 2022 dalla Commissione europea, la c.d. "BIK+" perché si inserisce in linea di continuità con la precedente BIK (*Better Internet for Kids*) introdotta nel 2012. Vd. Considerando 71 del DSA.

[5] L'articolo 28, paragrafo 1, del DSA recita: «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 servizi».

[6] L'approccio del legislatore europeo, seppur diversamente declinato rispetto ad altre normative (Cfr. Regulation EU n. 679/2016 (*General Data Protection Regulation*) e Regulation EU n. 1689/2024 (*Artificial Intelligence Act*)) adottate nell'ambito della *Digital Strategy* (Commissione europea, Comunicazione: Shaping Europe's digital future, 19 febbraio 2020, disponibile al seguente link: https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future_it ultima consultazione 22/07/2024), si è dimostrato ancora una volta di tipo *risk based* in relazione a quelli che sono i provvedimenti che i fornitori di servizi digitali devono adottare al fine di prevenire o arginare gli effetti dannosi derivanti dal verificarsi di rischi prevedibili a priori. Anziché limitarsi a stabilire nuovi diritti e garanzie, l'Unione ha cercato di regolamentare i pericoli aumentando la responsabilità

ISSN 2284-4503

effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica *e dei minori* e alle gravi conseguenze negative per il benessere fisico e mentale della persona»[7]. Ai fornitori di servizi digitali di grandi dimensioni spetta poi anche di provvedere alla attenuazione dei rischi così individuati, in particolare attraverso «l'adozione di misure mirate per *tutelare i diritti dei minori*, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi»[8].

Il legislatore europeo con la nuova normativa ha ritenuto di operare una distinzione tra piattaforme e motori di ricerca molto grandi e piattaforme più piccole in ragione dei diversi rischi che le prime possono comportare per la società in termini di portata ed effetti[9]. Data l'importanza che le VLOP e i VLOSE hanno in ragione del loro raggio d'azione, visto l'alto numero di destinatari dei servizi, il legislatore europeo ha ritenuto necessario di imporre ai fornitori di tali piattaforme obblighi specifici, in aggiunta agli obblighi previsti dal DSA e applicabili a tutte le piattaforme *online*. Tali obblighi supplementari per i fornitori di piattaforme *online* di dimensioni molto grandi e di motori di ricerca *online* di dimensioni molto grandi sono necessari per affrontare e prevenire il verificarsi di quelli che il legislatore ha definito "rischi sistemici"[10], rimettendo alle VLOP e ai VLOSE la responsabilità di individuare, analizzare e valutare con diligenza tali rischi[11] entro quattro mesi dalla notifica della designazione come piattaforme o motori di ricerca di dimensioni molto grandi ai sensi dell'articolo 33 del DSA.

Ad aprile 2023 la Commissione europea ha individuato un primo elenco di VLOP e VLOSE[12], designando (tra le altre) come piattaforme di dimensioni molto grandi *TikTok*, *Facebook* ed *Instagram*. Pertanto, ad agosto 2023 i colossi *social* hanno dovuto fornire ai sensi dell'articolo 34 del DSA una prima valutazione dei rischi sistemici derivanti dall'utilizzo dei loro servizi. Le informazioni così fornite da *TikTok* e da *Meta* non sono state ritenute del tutto esaustive da parte della Commissione europea che ha sollecitato le *big tech* a più riprese affinché fornissero ulteriori informazioni ai sensi dell'articolo 67 del DSA. In particolare, nei mesi successivi all'applicazione del DSA, la Commissione europea aveva chiesto a

degli attori pubblici e privati rispetto ai rischi e ai potenziali effetti collaterali derivanti dalle loro attività. Vd. G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law* Review, 59, 2, 2022, 473-500.

[7] Articolo 34 del DSA. Nostro il corsivo.

[8] Articolo 35 del DSA. Nostro il corsivo.

[9] Vd. Considerando 76 del DSA.

[10] I c.d. "rischi sistemici" sono suddivisi in quattro categorie, così individuate dall'articolo 34 del DSA: «a) la diffusione di contenuti illegali tramite i loro servizi; b) eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al *rispetto dei diritti del minore sancito nell'articolo 24 della Carta*, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta; c) eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica; d) qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla *protezione della salute pubblica e dei minori* e *alle gravi conseguenze negative per il benessere fisico e mentale della persona*». Nostro il corsivo.

[11] Vd. Articolo 34 del DSA.

[12] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413 (ultima consultazione 22/07/2024).

Meta e a *TikTok* di fornire maggiori informazioni[13] in merito alle misure adottate per ottemperare agli obblighi di protezione dei minori ai sensi del DSA, compresi quelli relativi alla valutazione e alle misure di attenuazione dei rischi per proteggere i minori *online*, specificatamente per quanto atteneva ai rischi per la salute mentale e fisica derivanti dall'utilizzo dei servizi da parte dei più giovani.

Nonostante le plurime richieste di informazioni e i solleciti della Commissione europea affinché *TikTok*, *Instagram* e *Facebook* provvedessero ad adeguarsi alle previsioni del DSA, in particolare con riferimento agli obblighi imposti in relazione al tema della protezione dei minori e alle conseguenze dannose che l'utilizzo di tali servizi potrebbe comportare per il loro benessere fisico e mentale, la Commissione ha considerato le risposte fornite da *TikTok* e *Meta* non soddisfacenti e a seguito di un'analisi preliminare delle informazioni ottenute ha ritenuto che non si fossero correttamente adeguate al DSA[14].

Pertanto, il 19 febbraio 2024 Commissione europea ha annunciato l'apertura di un procedimento ai sensi dell'articolo 66 del DSA contro il *social network* cinese *TikTok*[15], assumendo che tra gli articoli violati dalla piattaforma vi fossero quelli posti a tutela dei minori[16]. In seguito, il 16 maggio 2024 la Commissione europea ha annunciato di aver aperto un ulteriore procedimento contro *Meta*[17] per ragioni analoghe[18] a quelle contestate alla piattaforma *TikTok*.

In entrambi i casi la Commissione ha evidenziato il rischio che i sistemi di *TikTok*, *Facebook* e *Instagram*, compresi i loro algoritmi, potessero stimolare dipendenze comportamentali nei bambini e nei ragazzi e creare il cosiddetto effetto "*rabbit hole*"[19], cioè un fenomeno che avviene quando gli utenti vengono trascinati in una serie continua di contenuti correlati, portandoli ad esplorare argomenti sempre più lontani dalla loro ricerca iniziale. La Commissione ha inoltre rilevato una possibile illegittimità dei metodi di verifica dell'età predisposti sia da parte della società cinese che da parte di *Meta* in relazione

[13] Tra le richieste di informazioni *ex* art. 67 del DSA si veda https://ec.europa.eu/commission/presscorner/detail/en/mex_23_5145; https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-TikTok-and-youtube-under-digital-services-act; https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-Meta-and-snap-under-digital-services-act); https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-Meta-under-digital-services-act; https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-Meta-under-digital-services-act-1; https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-generative-ai-risks-6-very-large-online-platforms-and-2-very; https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-TikTok-regarding-launch-TikTok-lite-france-and-spain (ultima consultazione dei link presenti in nota 22/07/2024).

[14] Per un commento sul tema si vd. M. FABBRI, *Moderating online platforms after the DSA: from designing rules to enabling enforcement*, https://digi-con.org/moderating-online-platforms-after-the-dsa-from-designing-rules-to-enabling-enforcement/ (ultima consultazione 22/07/2024).

[15] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926 (ultima consultazione 22/07/2024).

[16] Gli articoli che, se accertata la violazione, si assumono violati sono: artt. 34(1), 34(2), 35(1), 28(1), 39(1), e 40(12) del DSA. Vd. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926 (ultima consultazione 22/07/2024).

[17] https://digital-strategy.ec.europa.eu/it/news/commission-opens-formal-proceedings-against-Meta-under-digital-services-act-related-protection (7/07/2024).

[18] Gli articoli che, se accertata la violazione, si assumono violati sono: artt. 28, 34 e 35 del DSA.

[19] K. WOOLLEY, M.A. SHARIF, *Down a Rabbit Hole: How Prior Media Consumption Shapes Subsequent Media Consumption*, in *Journal of Marketing Research*, 3, 2022, 453-471. Così come Alice cadendo nella tana del coniglio si ritrova catapultata suo malgrado nel Paese delle Meraviglie, il giovane utente dei social media si trova risucchiato all'interno di un algoritmo che gli propone contenuti disturbanti e potenzialmente pericolosi da cui difficilmente riuscirà autonomamente ad uscire.

all'accesso ai servizi forniti da parte di colossi del digitale, nonché la mancata adozione di misure adeguate e proporzionate per garantire un elevato livello di *privacy*, sicurezza e protezione dei minori.
Entrambi i procedimenti sono attualmente ancora in corso[20]. Laddove le violazioni contestate dovessero essere accertate in tema di protezione dei minori, le società saranno chiamate a rispondere ai sensi degli articoli 28 (*Protezione online dei minori*), 34 (*Valutazione del rischio*) e 35 (*Attenuazione dei rischi*) del DSA. L'eventuale accertamento da parte della Commissione delle violazioni contestate comporterà l'applicazione delle sanzioni pecuniarie previste dall'articolo 74 del DSA.
Con queste azioni di *enforcement* del DSA sembra chiaro che la protezione dei minori sia uno dei punti nevralgici dell'attuazione del regolamento europeo. La Commissione ha sin da subito invitato le piattaforme e i motori di ricerca di grandi dimensioni a presentare le informazioni relative ai possibili rischi derivanti all'utilizzo di tali servizi, mostrando una crescente preoccupazione per la salute e la tutela dei minori.
Quello però che appare necessario è di trovare risposta ad alcuni interrogativi: cosa intende il legislatore quando si riferisce alla tutela dei *minori*? Da cosa scaturiscono le odierne preoccupazioni per bambini e preadolescenti? Quali sono i prossimi passi per rafforzare i propositi del legislatore europeo?

2. L'accesso a Internet dei minori: ovvero come i tredici anni sono diventati l'età della "maturità digitale"

2.1. Il Children's Online Privacy Protection Act del 1998

Per comprendere l'ambito di tutela del DSA e delle norme previste a protezione del minore occorre innanzitutto interrogarsi su chi sia considerato *minore* nel contesto digitale.
Per molto tempo l'età minima per accedere ai servizi della società dell'informazione è stata fissata a tredici anni in virtù di una normativa statunitense del 1998 posta a tutela della *privacy* dei minori, il *Children's Online Privacy Protection Act* (COPPA)[21].
Il testo del COPPA è stato ampiamente discusso prima di essere stato approvato. L'idea iniziale del deputato Edward Markey, proponente della Carta dei diritti sulla *privacy* dei bambini, era quella di definire bambino, ai fini del COPPA, il minore di sedici anni. Questo limite trovò l'opposizione sia delle grandi società di *e-commerce* portatrici di interessi privati, sia dei gruppi per le libertà civili. I primi non volevano rinunciare ad una redditizia fetta di mercato che non avrebbe potuto beneficiare di beni e servizi della società dell'informazione, i secondi invece non volevano che molti ragazzi venissero esclusi dall'accesso ad Internet e dunque a una serie di informazioni come quelle legate all'utilizzo di contraccettivi, all'aborto o all'aiuto in situazioni di abuso[22].

[20] Il contributo è consegnato a luglio 2024.
[21] Il *Children's Online Privacy Protection Act* del 1998 (COPPA) è una legge federale degli Stati Uniti, situata al 15 USC §§ 6501 – 6506 (Pub. L.Tooltip Diritto pubblico (Stati Uniti) 105–277, 112 Stat. 2681-728, emanato il 21 ottobre 1998). 16 CFR Part 312.
[22] J. JARGON, *How 13 Became the Internet's Age of Adulthood*, in *The Wall Street Journal*, 18 giugno 2019, in https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201 (ultima consultazione 7/07/2024).

La soglia di legittimità del trattamento dei dati è stata quindi individua\ta nella regola pratica "sotto i dodici anni", utilizzata negli anni Settanta dai regolatori negli Stati Uniti e in altri Paesi per elaborare leggi sul *marketing* rivolto ai bambini. Ciò era stato supportato da una ricerca[23] che aveva dimostrato che i bambini dagli otto ai dodici anni erano in grado di distinguere la pubblicità da altri contenuti.
È stata dunque valutata adeguata la soglia di tredici anni perché il minore potesse esprimere liberamente il consenso al trattamento dei propri dati personali. L'età della maturità digitale trae dunque la propria origine da studi che hanno a che vedere con la capacità dei bambini di distinguere l'*advertising* dal programma televisivo che stanno guardando, anziché partire da studi sullo sviluppo cognitivo vero e proprio, sulla capacità di esprimere il consenso informato, sulla capacità di navigare sul *web* o di comprendere ed elaborare i contenuti cui hanno accesso.
Pertanto, il COPPA ha dato una definizione generale di "bambino"[24] dichiarando che ai fini dello stesso regolamento dovesse essere considerato tale il minore di tredici anni di età[25], determinando quelli che sono i limiti e le condizioni del trattamento dei suoi dati personali.
La legge aveva previsto poi il divieto di raccolta, conservazione e divulgazione dei dati personali dei bambini da parte di siti *web* o servizi *online* in violazione di quanto previsto dal COPPA[26]. Il trattamento dei dati personali dei minori di tredici anni poteva avvenire qualora fosse stato espresso il consenso del genitore[27] o di chi esercitasse la responsabilità genitoriale nei confronti del bambino, nei modi e nei termini[28] previsti dall'*Act* stesso.
Non vige dunque ad oggi un divieto assoluto di trattamento dei dati personali dei bambini negli Stati Uniti, ma un divieto eventualmente superabile nel caso in cui venga espresso il consenso di chi esercita la responsabilità genitoriale e qualora il consenso sia informato e carpito in maniera certa da parte del titolare del trattamento.
La ragione per cui la maggior parte delle piattaforme prevede un divieto di utilizzo da parte dei minori di tredici anni non è dovuto al fatto che i bambini e i preadolescenti debbano essere tutelati con maggiore forza rispetto alle eventuali conseguenze di un'esposizione prematura ai *social* e in generale ai prodotti della società dell'informazione, o al fatto che l'accesso a determinati contenuti presenti sulle piattaforme sia inappropriato se non addirittura rischioso, bensì è una scelta "commerciale" delle *big tech*. Come poc'anzi evidenziato, sarebbe infatti astrattamente possibile l'accesso e il ricorso ai servizi

[23] R.P. ADLER ET AL., *Research on the Effects of Television Advertising on Children; A Review of the Literature and Recommendations for Future Research*, Washington DC, 1975, in https://files.eric.ed.gov/fulltext/ED145499.pdf (ultima consultazione 07/07/2024).
[24] 16 CFR 312.2 «*"Child" means an individual under the age of 13*».
[25] J. JARGON, *op. cit.*, in https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201 (ultima consultazione 07/07/2024).
[26] 16 CFR 312.3 «*General requirements. It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part*».
[27] 16 CFR 312.5(a)(1).
[28] 16 CFR 312.4(a) «*General principles of notice. It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials*».

della società dell'informazione da parte dei bambini, qualora il consenso al trattamento dei loro dati venisse legittimamente espresso dagli esercenti la responsabilità genitoriale. Ad oggi però le società che forniscono questo genere di servizi anziché creare laboriosi sistemi di verifica del consenso dei genitori e di verifica dei dati, di per sé molto complessi e dispendiosi, preferiscono prevedere che possano registrarsi alle piattaforme solo coloro che abbiano compiuto tredici anni.
Peraltro, il COPPA prevede che le società siano soggette a sanzioni se raccolgono o divulgano dati di bambini in violazione delle previsioni della legge, ma solo laddove ne siano effettivamente a conoscenza[29]. Ciò significa che, laddove il minore di tredici anni acceda ad un sito o si registri a una piattaforma mentendo sulla propria età, il fornitore di servizi che a quel punto tratterà i suoi dati non sarà soggetto a sanzioni.

2.2. Dal COPPA al GDPR

In Europa la disciplina relativa alla protezione dei dati personali è contenuta nel *General Data Protection Regulation* UE/2016/679 (GDPR), entrato in vigore nel 2018, che all'articolo 8 rubricato «Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione»[30] prevede una disciplina apposita per il trattamento dei dati dei minori. L'atto europeo, a differenza del corrispettivo americano, prevede come regola generale che l'età del consenso digitale al trattamento dei dati, da parte di coloro che offrono servizi, sia stabilita a sedici anni, con la facoltà però per i singoli Stati membri di abbassare tale soglia, purché non al di sotto dei tredici anni. Quest'ultimo è probabilmente un richiamo al contenuto del COPPA e alla definizione che esso fornisce di "bambino" ai fini dell'applicabilità della disciplina sulla protezione della *privacy* del minore. In Italia, il legislatore ha esercitato tale facoltà portando la soglia della "maturità digitale" a quattordici anni[31].
L'articolo 8 del GDPR prevede anche che «ove il minore abbia un'età inferiore ai sedici anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare

[29] 16 CFR 312.3 "*General requirements*".
[30] L'articolo 8 del GDPR recita «1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni. 2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili. 3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore».
[31] Decreto legislativo 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", Art. 2-*quinquies* (Consenso del minore in relazione ai servizi della società dell'informazione): «1. In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale. 2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi».

della responsabilità genitoriale» e che «il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili». Pertanto, il limite al trattamento dei dati dei minori infrasedicenni può essere teoricamente superato, in Europa come negli Stati Uniti, per mezzo del consenso informato espresso da colui che esercita la responsabilità genitoriale sul bambino. Come evidenziato in precedenza[32] buona parte dei fornitori di servizi della società dell'informazione hanno preferito porre un divieto assoluto di utilizzo per gli utenti di età inferiore ai tredici anni, così da risparmiare costi e rischi legati allo sviluppo e utilizzo di sistemi di verifica del consenso legittimamente rilasciato dagli esercenti la responsabilità genitoriale in vece degli infratredicenni.

Secondo il Considerando (38) del GDPR, «i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati […]». I bambini godono di una protezione speciale ai sensi del Regolamento generale sulla protezione dei dati in quanto considerati vulnerabili[33]. Non hanno ancora raggiunto la maturità fisica e psicologica, quindi potrebbero essere meno consapevoli degli adulti dei rischi e delle conseguenze della condivisione dei loro dati personali quando si registrano a servizi *online* o utilizzano piattaforme connesse.

Recentemente il Garante per la protezione dei dati personali italiano ha dato applicazione al GDPR richiamando le norme poste a tutela dei minori al fine di oscurare due piattaforme: *TikTok*[34] e *ChatGPT*[35]. In entrambi i casi le *policy* delle società prevedevano un divieto di utilizzo delle piattaforme ai minori di tredici anni, senza però aver predisposto dei sistemi di verifica dell'età adeguati a impedire l'accesso a soggetti minori. Il Garante della *privacy* italiano, invocando le norme del GDPR poste a tutela del minore e il principio del *best interest of the child* di cui all'articolo 24, par. 2, della Carta dei diritti fondamentali dell'Unione europea[36], ha deciso di oscurare le piattaforme su tutto il territorio italiano, sottolineando in entrambi i casi come l'esposizione dei bambini a contenuti inidonei al loro grado di sviluppo, esponesse gli stessi a rischi intollerabili e pertanto fosse necessario vietare l'accesso a tali piattaforme su tutto il territorio italiano, a tutela dei minori.

[32] Cfr. par. 2.1.

[33] EUROPEAN DATA PROTECTION BOARD (EDPB), *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, Versione 1.1, adottate il 4 maggio 2020, p. 28. «Rispetto alla direttiva attuale, il regolamento generale sulla protezione dei dati crea un ulteriore livello di protezione per il trattamento dei dati personali delle persone fisiche *vulnerabili*, in particolare i minori». Nostro il corsivo.

[34] Garante per la protezione dei dati personali, provvedimento del 22 gennaio 2021, in https://www.garanteprivacy.it/*web*/guest/home/doc*web*/-/doc*web*-display/doc*web*/9524194 (ultima consultazione 29/07/2024). Per un commento si vd. D. MARCELLO, *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo*, Napoli, 2023, 62 ss.

[35] Garante per la protezione dei dati personali, Provvedimento del 30 marzo 2023, in https://www.garanteprivacy.it/home/doc*web*/-/doc*web*-display/doc*web*/9870832 (ultima consultazione 29/07/2024). Per un commento al provvedimento si vd. G. PISTORIO, *Chat GPT e la sfida della regolamentazione normativa*, in *Associazione italiana costituzionalisti – La Lettera,*5, 2023, in https://www.associazionedeicostituzionalisti.it/it/la-lettera/05-2023-costituzione-e-intelligenza-artificiale/chat-gpt-e-la-sfida-della-regolamentazione-normativa (ultima consultazione 29/07/2024).

[36] Carta dei diritti fondamentali dell'unione europea (2000/C 364/01).

3. Uno sguardo comparato: il contenzioso negli Stati Uniti

Per anni il fulcro della tutela dei minori nell'ambiente digitale è stata dunque la *privacy* dei bambini e la tutela dei loro dati personali, ma alcune inchieste e ricerche recenti sembrano aver dato nuova linfa al tema.

A settembre 2021 sono stati pubblicati i c.d. *Facebook files*[37] da parte del Wall Street Journal, un'inchiesta nata dalla collaborazione tra il famoso quotidiano americano e una ex dipendente di Meta, Frances Haugen, volta a dimostrare, tra le altre cose, come il colosso di Menlo Park fosse perfettamente a conoscenza degli effetti dannosi di *Instagram* sulla salute mentale di bambini e adolescenti[38].

A seguito della pubblicazione dei *Facebook files*, il *Surgeon General*[39] degli Stati Uniti, il Dr. Vivek Murthy, ha iniziato a pubblicare una serie di *advisory*[40] che hanno richiamato l'attenzione sulla crisi nazionale della salute mentale, del benessere dei giovani[41] e sulle profonde conseguenze sulla salute derivanti dalla c.d. "*social disconnection*" [42]. Infine, a maggio 2023 è stato pubblicato un parere dal titolo "*Social media and Youth Mental Health"*[43] che descrive l'impatto che i *social media* hanno sulla salute mentale di bambini e adolescenti sulla base dei dati ad oggi disponibili.

Quello che emerge chiaramente da quest'ultimo *advisory* è che, seppur gli studi non siano ancora del tutto conclusivi e vi sia necessità di approfondire ulteriormente l'impatto dei *social* sulla salute psicofisica dei minori, non è oggi possibile affermare con certezza che l'utilizzo delle piattaforme sia sufficientemente sicuro per il loro sviluppo ed il loro benessere[44]. Dai numerosi studi citati[45] emerge come

[37] Si vd. https://www.wsj.com/articles/the-Facebook-files-11631713039 (ultima consultazione 07/07/2024).

[38] G. WELLS, J. HORWITZ, D. SEETHARAMAN, Facebook *Knows* Instagram *Is Toxic for Teen Girls, Company Documents Show*, in *The Wall Street Journal*, 14 settembre 2021, in https://www.wsj.com/articles/Facebook-knows-Instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 (ultima consultazione 07/07/2024).

[39] Il *Surgeon General* degli Stati Uniti (*Surgeon General of the United States*) è il capo esecutivo dello *United States Public Health Service Commissioned Corps* e il portavoce delle questioni di salute pubblica all'interno del governo federale. È il soggetto più autorevole e titolato in materia di sanità pubblica negli Stati Uniti e in quanto tale costituisce il principale consigliere della Casa Bianca sul tema.

[40] Per una definizione di "*advisory*" si vd. THE U.S. SURGEON GENERAL'S ADVISORY, *Social media and Youth Mental Health*, 2023, 3, in https://www.hhs.gov/surgeongeneral/priorities/youth-mental-health/social-media/index.html (ultima consultazione 07/07/2024): «*A Surgeon General's Advisory is a public statement that calls the American people's attention to an urgent public health issue and provides recommendations for how it should be addressed. Advisories are reserved for significant public health challenges that require the nation's immediate awareness and action*».

[41] THE U.S. SURGEON GENERAL'S ADVISORY, *Protecting Youth Mental Health*, 2021, in https://www.hhs.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf (ultima consultazione 07/07/2024).

[42] THE U.S. SURGEON GENERAL'S ADVISORY, *Our Epidemic of Lonliness and Isolation*, 2023, in https://www.hhs.gov/sites/default/files/surgeon-general-social-connection-advisory.pdf (ultima consultazione 07/07/2024).

[43] THE U.S. SURGEON GENERAL'S ADVISORY, *op. cit.*, in https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf (ultima consultazione 7/07/2024).

[44] Per un commento si vd. S. CALZOLAIO, *Social media e minori. Il Safety-first approach. Nota a: U.S. Surgeon General, Social media and Youth Mental Health. The U.S. Surgeon General's Advisory, 2023*, in *Rivista di informatica e diritto*, 2, 2023, 292 ss.

[45] Fra i tanti cfr. G. FIORAVANTI, S. CASALE, S.B. BENUCCI, A. PROSTAMO, A. FALONE, V. RICCA, F. ROTELLA, *Fear of missing out and social networking sites use and abuse: A* Meta-*analysis*, in *Computers in Human Behavior*, 122, 2021, 1-12.

vi sia una correlazione allarmante tra utilizzo dei *social* da parte di bambini e adolescenti e l'aumento delle malattie legate alla salute mentale come depressione, ansia, disturbi alimentari, disturbi dell'attenzione e della qualità del sonno.
A seguito della pubblicazione dell'*advisory* del *U.S. Surgeon General* e prima che la Commissione europea aprisse il procedimento contro *Meta* ai sensi del DSA, ad ottobre 2023 già oltre quaranta Stati americani e il Distretto di Columbia avevano citato il colosso dei *social media* in giudizio con l'accusa di aver intenzionalmente progettato dei prodotti che creano dipendenza e che sono dannosi per i giovani utenti di *Instagram* e *Facebook*[46]. I ricorrenti in questione hanno accusato *Meta* di aver ingannato i consumatori in merito agli effetti dannosi sui più giovani. Inoltre, la *big tech* è stata accusata di aver commercializzato dei prodotti a utenti di età inferiore ai tredici anni, contravvenendo alla legge federale sulla protezione della *privacy* in rete dei minori[47] e alla sua stessa *policy*[48]. Quello che emerge chiaramente dalle casistiche riportate è come il tema della *privacy* e della protezione dei dati personali finisca per diventare secondario, la maggiore preoccupazione non è più e non è solo la riservatezza del bambino, ma la tutela della sua persona.

4. Oltre la privacy: gli "age verification system"

Da quanto finora emerso, è possibile ravvisare una crescente preoccupazione da parte degli attori pubblici per quanto attiene alla tutela dei minori all'interno dello spazio digitale. Una tutela non più limitata al trattamento dei dati personali e al diritto alla *privacy* del minore, ma che si estende alla protezione del bambino.
Dal quadro delineato, infatti, il minore risulta un soggetto vulnerabile, che agisce nella società dell'informazione in maniera autonoma al pari di un adulto, seppur egli non sia dotato degli strumenti e della maturità di un adulto. La condizione di vulnerabilità del minore è da intendersi in maniera specifica in relazione alle sue caratteristiche intrinseche[49], poiché egli si trova in una fase della vita in cui necessita di una protezione rafforzata, proprio in virtù della sua incapacità di difendersi autonomamente dai danni che l'esposizione ai rischi del *web* potrebbe provocare[50].
Recentemente la Commissione europea, come evidenziato in apertura, si è adoperata sul tema, sostenendo e promuovendo l'attuazione di norme mirate alla tutela dei minori *online*: in particolare, l'articolo 28 del DSA richiede che tutti i fornitori di piattaforme *online* accessibili ai minori adottino misure

[46] https://www.washingtonpost.com/technology/2023/10/24/Meta-lawsuit-Facebook-Instagram-children-mental-health/ (ultima consultazione 7/07/2024).
[47] Cfr. *Children's Online Privacy Protection Act*, 1998, (COPPA).
[48] Nelle condizioni d'uso di Facebook si legge che «Il nostro obiettivo è rendere Facebook disponibile a tutti, ma il suo uso è proibito nei casi seguenti: per gli utenti che hanno meno di 13 anni [...]». Così come le Condizioni d'uso di Instagram prevedono «Chi può usare Instagram: desideriamo che il nostro Servizio sia quanto più aperto e inclusivo possibile, ma vogliamo che sia anche sicuro, protetto e conforme alla legge. Pertanto, l'utente è tenuto a rispettare alcune limitazioni legali per poter far parte della community di Instagram. L'utente deve avere almeno 13 anni [...]».
[49] In relazione alle dimensioni ontologica e specifica del concetto di vulnerabilità vds. L. BUSATTA, C. CASONATO, S. PENASA, M. TOMASI, *Le "maschere" della vulnerabilità nella cura della persona*, AA. VV. (a cura di), *Liber amicorum per Paolo Zatti*, Napoli, 2023, 651-652.
[50] Sulla nozione di vulnerabilità vds. *Ibidem*, 651.

ISSN 2284-4503

adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori, anzitutto mediante l'attivazione dei meccanismi di verifica dell'età. Inoltre, l'articolo 35, paragrafo 1, lettera j), del DSA, prevede che i fornitori di piattaforme *online* e di motori di ricerca *online* di dimensioni molto grandi adottino misure di attenuazione dei rischi sistemici, tra cui quelle «mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi».

I sistemi di *age verification* risultano pertanto essere il punto di partenza per poter rispondere efficacemente alla presenza illecita dei minori su Internet. In tal senso in Italia, a seguito della conversione del c.d. "Decreto Caivano"[51] recante specifiche disposizioni per la sicurezza dei minori in ambito digitale, è stata data attuazione all'articolo 49, comma 2, del DSA: l'Autorità per le garanzie nelle comunicazioni (AGCOM) è stata designata Coordinatore dei servizi digitali per l'Italia, ossia l'autorità preposta a garantire l'effettività dei diritti e l'efficacia degli obblighi stabiliti dal Regolamento, «nonché la relativa vigilanza e il conseguimento degli obiettivi previsti, anche con riguardo alla protezione dei minori in relazione ai contenuti pornografici disponibili *online*, nonché agli altri contenuti illegali o comunque vietati, veicolati da piattaforme *online* o altri gestori di servizi intermediari, e contribuire alla definizione di un ambiente digitale sicuro»[52].

L'AGCOM è stata incaricata di stabilire, previa consultazione del Garante per la protezione dei dati personali, le modalità tecniche e di processo che gestori e fornitori di servizi della società digitale devono adottare per l'accertamento della maggiore età degli utenti che accedano a siti a carattere pornografico, con un livello di sicurezza adeguato e il rispetto della minimizzazione dei dati raccolti[53]. Il 6 marzo 2024 l'AGCOM ha pertanto avviato una consultazione pubblica[54] per l'approvazione di un provvedimento che disciplini le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti[55]. L'allegato B di tale provvedimento riporta quella che è un'analisi dei principali sistemi di verifica dell'età ad oggi esistenti, mettendone in luce pregi e difetti[56] e sottolineando poi quali devono essere i requisiti generali che un sistema di verifica dell'età deve rispettare.

[51] Decreto-legge 15 settembre 2023, n. 123, coordinato con la legge di conversione 13 novembre 2023, n., recante: «Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale».

[52] Art. 15, comma 1, d.l. n. 123/2023 (c.d. Decreto Caivano).

[53] Art. 13-bis, d.l. n. 123/2023 (c.d. Decreto Caivano).

[54] L'Autorità Garante per le Comunicazioni con Delibera del 6 marzo 2024, n. 61/24/CONS. ha dato «Avvio della consultazione pubblica di cui all'art. 1, comma 4, della delibera n. 9/24/CONS volta all'adozione di un provvedimento sulle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della dalla legge 13 novembre 2023, n. 159».

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

[56] Secondo il report dell'European Parliamentary Research Service del febbraio 2023 i metodi più diffusi di age verification sono: autodichiarazione; inserimento della carta di credito; utilizzo della biometria; analisi dei comportamenti su internet; verifiche online e offline dei documenti di identità; consenso dei genitori; vouching; identificazione digitale (es. SPID); portafoglio per l'identità digitale; utilizzo di app specifiche; verifica tramite sms o e-mail; open banking.

Dal report dell'AGCOM è possibile individuare principalmente tre diverse macrocategorie di sistemi di verifica dell'età: l'autodichiarazione, cioè la dichiarazione semplice dell'utente in merito al possesso del requisito dell'età o meno, evidentemente il metodo meno attendibile in quanto facile da aggirare; i sistemi di certificazione da parte di terzi, che costituiscono il sistema più attendibile però più invasivo; i sistemi di riconoscimento, che fanno ricorso all'intelligenza artificiale per verificare l'età del soggetto e che utilizzano un vasto numero di dati e presentano il più alto grado di insidie in quanto maggiormente a rischio di commettere errori[57].

I sistemi di verifica dell'età assumono un ruolo particolarmente rilevante poiché sono gli strumenti che consentono o vietano l'accesso ai servizi della società dell'informazione per la cui fruizione è richiesta un'età minima. Di fatto, la predisposizione di tali sistemi e la loro effettività sono in grado di incidere sulla libertà dell'utente di accedervi o meno e di svolgervi la propria personalità. Non sembra un caso il fatto che l'individuazione di *age verification system* sia stata demandata proprio all'AGCOM, cioè l'autorità posta a garanzia, tra le altre cose, della libertà di comunicazione, di informazione e di espressione, anziché al Garante delle protezione dei dati personali, deputato, per l'appunto, alla tutela della *privacy*. Risulta evidente uno spostamento del problema dell'accesso dei minori alle piattaforme *online* da una logica *privacy*, incentrata sul consenso, a una logica costituzionale di bilanciamento delle libertà costituzionali e delle istanze di tutela del soggetto minore che potrebbe essere realizzato tramite il ricorso ai sistemi di *age verification*.

5. I minori sulla rete: un problema di "precauzione" costituzionale

Quello che sembra emergere dallo scenario finora delineato è una progressiva espansione dell'ambito di tutela del minore nell'ambiente digitale. Per anni gli attori pubblici hanno operato una tutela secondo la logica della *privacy*, dando preminente importanza al consenso quale strumento per la liceità del trattamento dei dati personali: da un lato, infatti, il COPPA e il GDPR stabiliscono un'età della maturità digitale diversa e non coincidente con l'età della capacità di agire, che consente all'infradiciottenne di disporre dei propri dati prestando il proprio consenso; dall'altro lato sia la normativa statunitense che quella europea consentono astrattamente la liceità del trattamento dei dati personali del minore anche qualora il consenso sia espresso da colui che esercenti la responsabilità genitoriale.

La tutela apprestata alla *privacy* è pertanto una tutela relativamente debole in quanto superabile attraverso l'esercizio dello strumento negoziale per eccellenza, ovverosia il consenso di colui che sia legittimato dalla legge a disporre dei dati personali di un soggetto minore o da parte del minorenne stesso. Ne deriva che fino ad oggi è stata solo la mancanza di consenso dell'esercente la responsabilità genitoriale a frapporsi tra il minore e la sua presenza *online*. Il divieto di accesso ad alcuni servizi della società dell'informazione è dovuto esclusivamente a una scelta di *policy* delle *big tech*, che hanno preferito vietare l'accesso ai minori anziché predisporre complicati sistemi di verifica del consenso

[57] Con il paradosso per cui lo stesso sistema di *age verification* integra un trattamento automatizzato di dati personali. Di conseguenza, laddove un minore di 14 anni tenti di accedere ad una piattaforma, non vi può essere un consenso validamente espresso neppure allo stesso trattamento di *age verification*.

dell'esercente la responsabilità genitoriale [58]. L'unico fondamento della tutela, dunque, è solo l'autoregolamentazione delle piattaforme[59].

Non vi è dubbio che l'accesso alle piattaforme *online* costituisca oggi uno dei mezzi attraverso il quale un soggetto può svolgere la sua personalità, esercitare diritti e libertà costituzionalmente garantiti quali la libertà di comunicazione[60], di informazione e di espressione[61]. Nel caso del minore però si pone una questione ulteriore, legata al fatto che l'esposizione prematura dello stesso all'ambiente digitale potrebbe comportare dei danni per la sua salute psico-fisica e comprometterne persino lo sviluppo, come emerge dai più recenti risvolti scientifici[62].

La Costituzione italiana nel riconoscere i diritti fondamentali non opera alcuna distinzione basata sull'età, ciò significa che il minore può godere degli stessi a prescindere dalla sua condizione personale. Tuttavia, la complessità della posizione del minore, quale persona in divenire, pone non pochi problemi nel godimento dei diritti che attengono alla sua sfera personale. Sono due le finalità di tutela assunte come prioritarie per il minore: da una parte, le istanze di autodeterminazione; dall'altra, le esigenze di cura[63].

Se da un lato la presenza del minore *online* consente allo stesso di esercitare diritti e libertà costituzionalmente garantiti, dall'altro lato si pone la necessità di operare un bilanciamento con le istanze di tutela che nascono dai rischi che possono insorgere a seguito di questa esposizione prematura. Il minore, infatti, nella Costituzione riemerge come destinatario di una tutela più ampia e distinta rispetto a quella dell'adulto in quanto persona in formazione[64], pertanto si pone l'esigenza di predisporre strumenti adeguati a tale scopo.

Senza voler scadere in conclusioni paternalistiche e anacronistiche, alla luce delle incertezze e delle conseguenze negative che la presenza prematura del minore *online* può avere sullo stesso, sembrerebbe opportuno ricorrere al *principio di precauzione*[65], elaborato nell'area del diritto dell'ambiente,

[58] Questo è ciò che accade ogni volta che un genitore fornisce il proprio consenso alla creazione di un *account* del proprio bambino per registrarsi ad un'applicazione riservata ai minori, per esempio *YouTube Kids* richiede al genitore il consenso al trattamento dei dati del bambino che poi potrà utilizzare autonomamente la piattaforma. Vd. la *privacy policy* di *YouTube Kids* https://kids.youtube.com/t/privacynotice (ultima consultazione 30/07/2024).

[59] Sul tema si vd. E. CREMONA, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023, 46 ss.

[60] Art. 15, Cost.

[61] Art. 21, Cost.

[62] Vd. par. 3.

[63] G. MATUCCI, *Lo statuto costituzionale del minore d'età*, Padova, 2015.

[64] C. DI COSTANZO, *La tutela del minore: identità, salute e relazion*i, Torino, 2023, 18. Cfr. anche G. MATUCCI, *op. cit*.; G. DE MINICO, *Il favor constitutionis e il minore: realtà o fantasia?* in A. CIANCIO, G. DE MINICO, G. DEMURO, F. DONATI, M. VILLONE (a cura di), *Nuovi mezzi di comunicazione e identità. Omologazione o diversità?* Roma, 2012, 162; F. MODUGNO, *Breve discorso intorno all'uguaglianza. Studio di una casistica: i minori e i nuovi media*, in *Osservatorio costituzionale*, 1, 2014, 1-14.

[65] Seppur desumibile implicitamente anche da convenzioni precedenti, il principio di precauzione trova il suo esplicito riconoscimento internazionale nel 1992 nella Dichiarazione di Rio su ambiente e sviluppo. Il principio ha fatto il suo ingresso a livello comunitario con il Trattato di Maastricht ed è attualmente richiamato dall'art. 191 TFUE senza che ne venga fornita una sua definizione. S.GRASSI, A.GRAGNANI, *Il principio di precauzione nella giurisprudenza costituzionale*, in L.CHIEFFI (a cura di), *Biotecnologie e tutela del valore ambientale*, Torino, 2003, 149-169; G. GALASSO, *Il principio di precauzione nella disciplina degli OGM,* Torino, 2006; F. DE LEONARDIS, *Il principio di*

per riconsiderare le misure volte a limitare l'accesso ai servizi della società dell'informazione da parte dei minori. In base a tale principio, la condizione di incertezza a riguardo dei possibili effetti negativi dell'impiego di una tecnologia non può essere utilizzata come una ragione legittima per non regolare e limitare tale sviluppo[66].

Trasponendo tale principio nell'ambiente digitale, sembrerebbe opportuno ricorrere a un progressivo rafforzamento delle tutele disposte dall'ordinamento nei confronti del minore. Il ricorso a sistemi di *age verification* effettivi potrebbe essere un punto di partenza per operare il bilanciamento sopra auspicato. Occorrerà seguire con attenzione la concreta definizione di questi sistemi perché rappresenta un tema dall'indiscusso tono costituzionale.

precauzione nell'amministrazione del rischio, Milano, 2005; a livello internazionale non mancano autorevoli posizioni critiche nell'applicazione forte del principio di precauzione cfr. C.R. SUNSTEIN, *Laws of fear: beyond the precautionary principle*, Cambridge, 2005 (trad. it. *Il diritto della paura: oltre il principio di precauzione*, Bologna, 2010).

[66] A. SIMONCINI, *L'algoritmo incostituzionale: l'intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 86 ss.

ISSN 2284-4503