Cittadinanza digitale e minori

Digital Citizenship and Minors

Giovanni Pascuzzi [1]

Sommario

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

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

Abstract

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

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

1. La cittadinanza digitale

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Lo spazio digitale e i minori

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

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

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

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

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

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

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

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

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

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

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

La Dichiarazione dedica delle indicazioni precise relativamente ai minori.

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

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

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

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

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

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

4. La formazione dei minori sulle competenze digitali

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. I minori e l'identità digitale

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

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

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

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

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

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

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

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

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

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

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

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

6. I diritti di cittadinanza digitale dei minori

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

6.1.1 (segue) La verifica dell'età

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

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

Alcune disposizioni normative prescrivono precisi oneri, sotto questo profilo.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.2.2 La lotta al cyberbullismo

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

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

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

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

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

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

6.2.3 La tutela tecnologica: il parental control

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

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

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

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

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

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

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

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

6.2.4 La tutela del minore come "consumatore digitale"

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

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

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

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

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

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

7. I doveri dei minori per la cittadinanza digitale

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

8. Conclusioni

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

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

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

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

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

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

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

Bibliografia

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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