

Focus tematici

Accesso sicuro a internet. Tutele contro abusi, sfruttamento e violenza online nei confronti delle persone di minore età: un quadro normativo

Le tecnologie digitali sono parte integrante della vita dei bambini, delle bambine, degli e delle adolescenti in quanto strumenti di comunicazione e relazione, di informazione, studio, creatività e partecipazione. Nell'ultimo periodo, complice anche l'emergenza sanitaria derivante dalla diffusione della pandemia da Covid-19, internet e le altre tecnologie digitali di comunicazione e informazione hanno avuto un ruolo ancora più preponderante nella vita dei più giovani. Basti pensare alla didattica a distanza che ha dominato l'ultimo anno scolastico e continua in parte a caratterizzare anche quello in corso. Si stima che attualmente sei adolescenti su dieci passino, in media, più di cinque ore al giorno connessi (in particolare fra le cinque e le dieci ore). È quanto emerge dall'indagine promossa da "Generazioni Connesse", il Centro italiano per la sicurezza in rete guidato dal Ministero dell'istruzione, e presentata in occasione del *Safer Internet Day 2021*, la Giornata mondiale dedicata all'uso positivo di internet. Negli ultimi anni è inoltre cambiata anche la qualità dell'uso di internet da parte delle persone di minore età con un aumento considerevole del ricorso ai social network quali principali strumenti di comunicazione e relazione tra amici, di partecipazione alla vita sociale, di informazione e di espressione della propria identità. L'uso massiccio delle tecnologie digitali e l'accesso sempre più facile a internet e ai suoi contenuti sottopongono bambini, bambine e adolescenti a una maggior esposizione ai rischi della rete: nel contesto online proliferano episodi di *cyberbullismo*, aumentano i fenomeni di abusi e violenze sessuali a danno di bambini, bambine e adolescenti, si diffondono fonti contenenti materiali di tipo pedopornografico. Le recenti misure di confinamento che hanno portato a un aumento del tempo trascorso su internet da parte delle persone di minore età, spesso senza supervisione, hanno esposto ancor di più queste ultime alle pratiche di abuso e sfruttamento, nonché al rischio di violazione dei dati personali.

L'utilizzo delle nuove tecnologie è alla portata di tutti e ingenera fenomeni di portata globale. Altrettanto a livello globale deve dunque essere affrontato il tema della difesa delle persone di minore età dai rischi che provengono da un uso scorretto e non consapevole di internet e delle altre tecnologie digitali. Anzitutto, la [Convenzione sui diritti dell'infanzia e dell'adolescenza](#), adottata dall'Assemblea Generale delle Nazioni Unite con risoluzione del 20 novembre 1989, n. 44/25, all'art. 34 prescrive agli Stati di proteggere le persone di minore età da ogni forma di sfruttamento e abuso sessuale, mediante l'adozione di ogni adeguata misura a livello nazionale, bilaterale e multilaterale per impedire che esse: siano incitate o costrette a dedicarsi a un'attività sessuale illegale; siano sfruttate a fini di prostituzione o di altre pratiche sessuali illegali;

siano sfruttate ai fini della produzione di spettacoli o di materiale a carattere pornografico. Soprattutto a partire dalla fine degli anni Novanta in poi si sono susseguiti numerosi interventi normativi volti a incentivare i singoli Stati a sviluppare e rafforzare gli strumenti giuridici per prevenire e contrastare fenomeni quali la detenzione, la produzione, il commercio, la distribuzione di materiale pedopornografico in rete, la violenza e l'abuso delle persone di minore età su internet, l'adescamento e lo sfruttamento sessuale online e via dicendo. Il tema dell'accesso sicuro a internet, ai contenuti digitali e alle piattaforme di social networking è divenuto sempre più centrale nella riflessione giuridica internazionale, europea e nazionale. Si pensi, per esempio, alla tutela dei dati personali che vengono più o meno consapevolmente diffusi ogni volta che si accede a social network o siti internet; ai rischi di una scorretta navigazione in rete che può condurre a contenuti pericolosi o esporre il giovane utente a pratiche di abuso sessuale online; o, ancora, all'impatto delle *fake news* sulla corretta informazione e sull'oggettività necessaria alla creazione di una propria coscienza critica, soprattutto negli adolescenti, nel pieno della loro formazione psicologica, culturale e sociale.

Ciò è evidenziato anche nel *General Comment no. 25*, adottato il 2 marzo 2021 dal Comitato sui diritti dell'infanzia e dell'adolescenza, [CRC/C/GC/25](#), che, nell'affrontare il tema del mondo digitale come potenziale strumento di realizzazione dell'intera gamma dei diritti civili, politici, culturali, economici e sociali delle persone di minore età, ne richiama anche i rischi per un accesso sicuro e consapevole alle tecnologie digitali.

Quella dell'utilizzo sicuro di internet e degli strumenti digitali, specialmente nell'era dei social media, è una priorità che si è manifestata anche a livello europeo. In particolare, nella recente comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'UE sui diritti dei minori*, del 24 marzo 2021, [COM/2021/142 final](#), uno degli obiettivi programmatici di intervento riguarda proprio la lotta alla disinformazione e la tutela dei diritti delle persone di minore età nella società digitale. Si tratta di rendere lo spazio europeo un contesto nel quale le persone di minore età possano utilizzare in modo sicuro le risorse digitali e sfruttarne le opportunità per una piena e corretta informazione e per un esercizio consapevole dei propri diritti. Finalità simili sono perseguite anche mediante altri strumenti normativi come la direttiva del 13 dicembre 2011, [2011/93/UE](#), relativa alla "lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile"; la direttiva del 14 novembre 2018, [2018/1808/UE](#), sui "servizi di media audiovisivi";

la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Contrastare la disinformazione online: un approccio europeo*, del 26 aprile 2018, [COM\(2018\)236](#). Sempre nell'ambito della Strategia sui diritti delle persone di minore età si è inoltre previsto che l'Unione europea continuerà a contribuire a potenziare le norme internazionali per la protezione delle persone di minore età dagli abusi sessuali promuovendo la cooperazione multipartecipativa anche attraverso il finanziamento a iniziative di cooperazione multilaterale come *WeProtect Global Alliance to End Child Sexual Exploitation Online*, che attualmente comprende 97 governi, 32 imprese tecnologiche a livello mondiale, 33 organizzazioni della società civile e istituzioni internazionali e 5 organizzazioni regionali e che intende migliorare la protezione delle vittime, individuare e perseguire i colpevoli, sensibilizzare l'opinione pubblica e ridurre la disponibilità di materiale pedopornografico online.

Più recentemente, il Parlamento europeo e il Consiglio Ue hanno approvato ulteriori norme per permettere ai fornitori di servizi online di individuare, segnalare e rimuovere materiale contenente abusi sessuali sulle persone di minore età. Infatti, secondo il [rapporto annuale della Internet Watch Foundation \(IWF\)](#), le tecnologie digitali da un lato hanno facilitato il compito ai criminali, permettendogli di raggiungere più facilmente le persone di minore età tramite l'uso di webcam, dispositivi connessi e *chat room* sui social media e nei videogiochi, dall'altro ne hanno garantito l'anonimato grazie all'uso di tecnologie come il *cloud computing* e il *dark web*. L'utilizzo delle suddette tecnologie da parte dei trasgressori ha complicato notevolmente il lavoro di indagine delle autorità preposte all'applicazione della legge e al perseguimento degli abusi sessuali su persone di minore età. Con il [regolamento del 14 luglio 2021, n. 1232](#), relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE, sono state perciò introdotte alcune norme temporanee allo scopo di consentire ai fornitori di alcuni servizi di comunicazione interpersonale di utilizzare tecnologie specifiche per il trattamento di dati personali e di altro tipo nella misura strettamente necessaria a individuare gli abusi sessuali online sulle persone di minore età sui propri servizi e segnalarli e a rimuovere il materiale pedopornografico online dai loro servizi.

Per maggior completezza, è utile infine richiamare anche il regolamento adottato dal Parlamento e dal Consiglio Ue del 27 aprile 2016, [2016/679/UE](#), entrato in vigore il 25 maggio 2018, relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" che, nell'occuparsi specificamente della capacità del minore di prestare

il consenso in relazione ai servizi della società dell'informazione (art. 8, § 1), ha previsto che «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».

A tal riguardo, è da sottolineare, con specifico riferimento all'ordinamento italiano, come il [D.Lgs. del 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento \(UE\) 2016/679](#), abbia ritenuto di ridurre a 14 anni l'età minima per esprimere il consenso al trattamento dei propri dati in relazione all'accesso ai servizi della società dell'informazione. Ciò dunque richiede un impegno da parte delle istituzioni, parallelamente a quello della famiglia e della scuola, a incentivare la diffusione di una cultura digitale finalizzata a educare bambini, bambine e adolescenti, ciascuno in relazione al grado di maturità e al livello di accessibilità ai contenuti presenti in rete, a un utilizzo corretto dei servizi di informazione digitale, così come a una fruizione consapevole dei mass media e dei social media. In quest'ottica, si può segnalare, per esempio, la [legge del 20 agosto 2019, n. 92, Introduzione dell'insegnamento scolastico dell'educazione civica](#), che, all'art. 5 in tema di educazione alla cittadinanza digitale, evidenzia la necessità di formare gli/le studenti/studentesse a essere in grado di evitare, usando tecnologie digitali, rischi per la salute e minacce al proprio benessere fisico e psicologico; essere in grado di proteggere sé e gli altri da eventuali pericoli in ambiente digitale; essere consapevoli di come le tecnologie digitali possono influire sul benessere psicofisico e sull'inclusione sociale, con particolare attenzione ai comportamenti riconducibili alla disinformazione, al *cyberbullismo*, all'adescamento online, alla diffusione di immagini inappropriate e di dati personali sensibili e così via.

Più segnatamente, con riferimento al *cyberbullismo*, l'ordinamento italiano si è dotato di una specifica disciplina con la [legge del 29 maggio 2017, n. 71, Disposizioni a tutela delle persone di minore età per la prevenzione ed il contrasto del fenomeno del cyberbullismo](#), che intende tutelare il diritto delle nuove generazioni a una navigazione sicura, positiva e libera. Un provvedimento legislativo che, fin dall'inizio, è stato pensato non solo per le vittime, ma anche per il riscatto di quei ragazzi che, spesso inconsapevolmente, danneggiano i propri coetanei attraverso le piattaforme digitali.

Oltre a prevedere la possibilità per ciascun minore con più di 14 anni, genitore o chi esercita la responsabilità genitoriale, di poter inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi dato del minore vittima di *cyberbullismo*, l'attenzione è focalizzata sulla prevenzione e sull'educazione all'uso corretto di internet con la previsione, tra le altre cose, dell'obbligo per ogni scuola di individuare un responsabile per questi temi e di realizzare specifici interventi di formazione e sensibilizzazione.

Con riferimento alla lotta contro l'abuso e la violenza sessuale anche online, l'Italia ha mosso notevoli passi in avanti, già a partire dalla ratifica della [Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica](#), sottoscritta a Istanbul l'11 maggio 2011, avvenuta con [L. 27 giugno 2013, n. 77](#), e in vigore dal 1° agosto 2014, contenente norme in materia di abusi sessuali su persone di minore età in ambito domestico; più recentemente, con la [legge del 25 luglio 2019, n. 69](#), contenente nuove misure relative alla tutela delle vittime di violenza domestica e di genere, anche denominata "Codice rosso". Tra i punti più significativi - in una società che deve impegnarsi sempre di più per tutelare questa tipologia di vittime - vi è certamente l'introduzione dei reati di *revenge porn*, sfregi e nozze forzate. Il nuovo testo impone, inoltre, una maggiore durezza in relazione ai maltrattamenti in famiglia e aumenta le pene per violenza sessuale e *stalking*. Più in particolare, con il reato di *revenge porn* si intende punire la diffusione illecita di immagini o video sessualmente espliciti in assenza del consenso delle persone in essi presenti. L'art. 10 stabilisce, infatti, che venga inserito, dopo il 612-bis, l'art. 612-ter, il quale prevede la pena della reclusione da uno a sei anni e la multa da 5mila a 15mila euro per chiunque, dopo aver realizzato o sottratto, immagini o video a contenuto sessualmente esplicito che erano destinati a rimanere privati, li invii, li consegni, li ceda, li pubblichi o li diffonda senza il consenso delle persone rappresentate, con la volontà di causar loro un danno. È previsto un aumento della pena qualora i fatti siano commessi dal coniuge, anche separato o divorziato, o da una persona che sia o sia stata legata da una relazione affettiva alla vittima o qualora i fatti siano commessi con l'utilizzo di strumenti informatici o telematici. Inoltre, al quarto comma, è stabilito un aumento della pena che va da un terzo alla metà, quando la vittima è una persona in condizione di inferiorità fisica o psichica o una donna in stato di gravidanza.