lacittadinanzaeuropea online
Rivista di studi e documentazione sull'integrazione europea
ISSN 2785-4183
lceonline 2/2023 (www.lceonline.eu) - numero speciale

Minori e nuove tecnologie: una sfida improrogabile per il costituzionalismo digitale(*)

Luis Fernando MARTÍNEZ QUEVEDO*

Sommario: 1. Introduzione **2.** L'uso di Internet e delle ICT tra i minori **3.** Alcune questioni giuridico-costituzionali del rapporto tra minori e ICT *3.1.* Il minore e i diritti fondamentali *3.2.* Rischi per i minori nell'uso delle ICT *3.2.1.* Problemi relativi al consenso *3.2.2.* L'anonimato *3.2.3.* La commissione di reati *3.2.4.* Il cyberbullismo scolastico **4.** Possibili soluzioni **5.** Conclusioni

1. Introduzione

Negli ultimi due decenni abbiamo assistito a una crescita esponenziale dell'uso delle nuove Tecnologie dell'Informazione e della Comunicazione (Information and Communication Technologies: ICT) che stanno indubbiamente segnando un prima e un dopo nella storia dell'umanità, così come è accaduto nell'antichità con il fuoco, la stampa o la penicillina. Al giorno d'oggi, l'universalizzazione di Internet è sinonimo di progresso in qualsiasi ambito della nostra esistenza, in particolare nei settori della comunicazione e della scienza. Oggi è difficile non solo capire la vita delle persone senza accesso alla rete, ma anche capire quale potrebbe essere il limite di questo tipo di tecnologia. In questo senso, le ICT sono uno strumento indispensabile per lo sviluppo, l'internazionalizzazione, la pubblicità e la diffusione della ricerca scientifica in qualsiasi disciplina, oltre che per un migliore profitto nel mondo del lavoro, dell'università e della scuola.

Tuttavia, questa crescita esponenziale porta con sé, oltre agli indubbi vantaggi appena citati, una serie di rischi la cui importanza non deve essere ignorata. Dobbiamo quindi tenere conto, tra l'altro, dell'esposizione pubblica degli individui, del trattamento dei dati personali (come nome, indirizzo, indirizzo e-mail, situazione lavorativa o immagine, per citare alcuni dei più comuni) e del fatto che la rete costituisce di per sé un contesto appropriato per la commissione di atti criminali, con la comparsa sia di nuove forme di reati già esistenti in precedenza nel mondo 'analogico' (ad esempio, la frode), sia la criminalizzazione di forme nuove che possono essere realizzate esclusivamente tramite Internet (come lo stalking o il grooming).

Tra questi rischi, che assumiamo quasi in modo naturale (o, forse, sarebbe più corretto parlare ~~di~~ in modo in alcuni casi inconsapevole), è opportuno tenere presente i minori, con particolare attenzione a quelli che non hanno ancora compiuto 14 anni, perché costituiscono un gruppo eterogeneo in termini di maturità e capacità e, inoltre, perché sono utenti abituali di Internet, delle ICT e dei social network; molto spesso inconsapevoli di tutti i pericoli connessi a questo settore.

In sintesi, partendo da questo contesto, il presente lavoro si propone di affrontare: in primo luogo e da una prospettiva generale, quelli che dal nostro punto di vista sono i rischi più rilevanti che i minori possono incontrare nell'uso delle nuove tecnologie, concentrandosi in particolare su quel fenomeno che riteniamo essere il più dannoso (non strettamente per le conseguenze, ma per la frequenza di accadimento e la difficoltà di individuazione), ovvero il cyberbullismo nelle scuole; in secondo luogo,

(*) Traduzione dallo spagnolo di Rosa Iannaccone.
* Dottorando in Scienze giuridiche, Dipartimento di Diritto Costituzionale, Università di Granada.

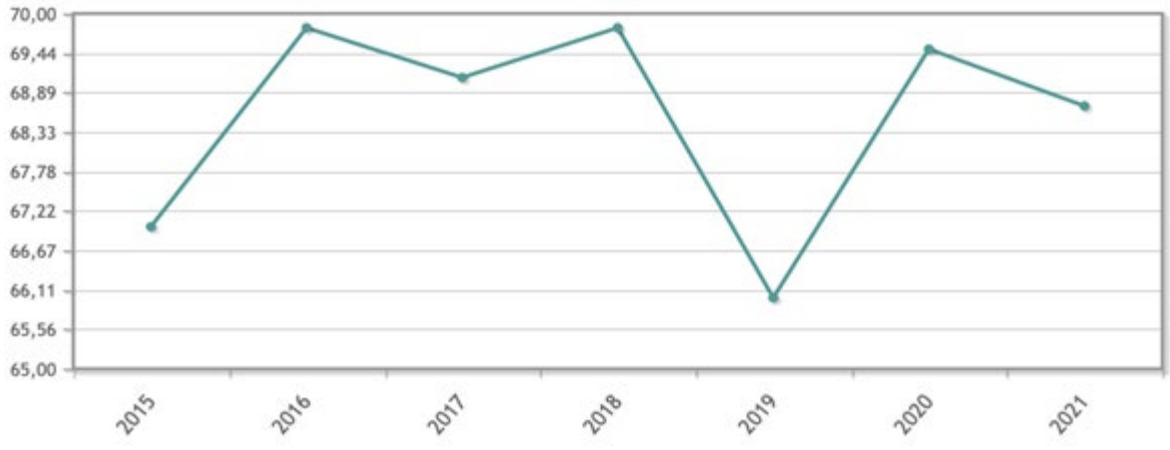
indurre il lettore a porsi alcune domande e indicare alcune possibili soluzioni che hanno come nesso la necessità che il diritto costituzionale sia coinvolto in modo decisivo nell'affrontare questi problemi, integrando così altre branche del diritto (principalmente il diritto penale e civile) e altre discipline (come la psicologia e la pedagogia) che ne hanno fanno oggetto di studio a partire dallo scorso decennio.

2. L'uso di Internet e delle ICT tra i minori

Quando discutiamo dei rischi connessi alle nuove tecnologie per i minori, è frequente trovare alcune voci dissenzienti che pur riconoscendo l'esistenza di un rischio, lo minimizzano. Pur non volendo fare allarmismo, la verità è chei pericoli posti dalle ICT, da Internet e dai social network sono rilevanti, non solo per quanto concerne la violazione di diritti, ma anche perché l'uso di questi dispositivi e applicazioni è diffuso praticamente tra tutti i minori a partire dai 10 anni. Ciò significa che, in astratto, quasi ogni minore è esposto a un problema di queste caratteristiche.

Per fare un esempio concreto, relativo alla Spagna, è sufficiente collegarsi al sito ufficiale dell'Istituto Nazionale di Statistica spagnolo (INE). Una semplice consultazione del sito conferma che l'uso di Internet tra i minori è effettivamente molto diffuso[1]. In particolare, secondo dati recenti, relativi all'utilizzo di computer e Internet, tra i minori di età compresa tra 10 e 15 anni, si riscontra che la percentuale di giovani che utilizzano Internet è del 97,5%, ovvero quasi l'intero gruppo. Tuttavia, anche i dati analizzati nel dettaglio sono piuttosto interessanti, soprattutto se si guarda alla specifica fascia d'età. La percentuale di minori che hanno usato Internet negli ultimi 3 mesi del 2020 aumenta con l'aumentare dell'età, dal 93,1% per i minori di 10 anni al 99,5% per quelli di 15 anni. Nei dati consultati, ci è sembrato interessante includere specificamente quello relativo al luogo di connessione, compresa l'abitazione come luogo privilegiato, circostanza che, come vedremo più avanti, è di importanza capitale per capire dove si trovano sia la radice del problema che la ricerca di soluzioni.

D'altra parte, consideriamo interessanti per il nostro studio i dati dell'Istituto Nazionale di Statistica spagnolo relativi ai minori che hanno un proprio cellulare[2] e la loro evoluzione negli ultimi anni, nel diagramma qui riprodotto, frutto di una indagine sulle apparecchiature e sull'uso delle tecnologie dell'informazione e della comunicazione nelle case, da parte di minori (10-15 anni) che dispongono di un telefono cellulare.



Come possiamo vedere, nel 2021 è stato registrato un leggero calo rispetto all'anno precedente,

[1] INE (https://www.ine.es/jaxi/Tabla.htm?tpx=50168&L=0).
[2] *Ibid.*

anche se dobbiamo tenere presente che, dal 2015, la percentuale di ragazzi tra i 10 e i 15 anni che possiedono un cellulare ad uso esclusivo è sempre stata superiore al 65%. Questo dato è sorprendente anche se si considerano i segmenti di età più giovani, perché è noto che i bambini di 10, 11 o 12 anni non hanno sufficiente responsabilità o maturità per capire a quali problemi possono essere esposti o, almeno, come affrontarli nel caso in cui si confrontino con alcuni di essi[3].

In breve, questa prima sezione serve a collocare il lettore nella reale portata del problema, sulla base di dati che illustrano come la quasi totalità dei bambini e degli adolescenti spagnoli abbia un accesso continuo a Internet (e non solo a Internet, ma anche ai social network e alle applicazioni di messaggistica istantanea) e la maggior parte di loro abbia un proprio telefono cellulare, con tutte le conseguenze che questo comporta (rispetto alla loro intimità, impossibilità di sorveglianza permanente, accesso a siti non adatti alla loro età, ecc.)

3. Alcune questioni giuridico-costituzionali del rapporto tra minori e ICT

3.1. Il minore e i diritti fondamentali

La titolarità e l'esercizio dei diritti fondamentali da parte dei minori è stata una questione molto dibattuta dalla dottrina negli ultimi anni del XX secolo. L'evoluzione dello status giuridico dei minori è iniziata, per quanto interessa in questa sede, nei primi decenni del XX secolo, quando i minori hanno cominciato a essere considerati un soggetto degno di protezione, come si evince dalla "Dichiarazione di Ginevra dei Diritti del Fanciullo" del 1924. Dal canto suo, la Dichiarazione ONU dei Diritti del Fanciullo, approvata il 20 novembre 1959, pone il minore in una situazione di particolare protezione, pur considerandolo, a differenza della precedente, come un soggetto incipiente titolare di alcuni diritti[4]. Tuttavia, sarà la consacrazione del suo superiore interesse a costituire il maggiore progresso di questo documento, il germe della posizione giuridica che inizierà ad occupare negli ultimi decenni[5], già considerato come soggetto titolare di diritti e come persona autonoma che deve progressivamente maturare per configurare i profili della propria dignità. Il punto culminante è rappresentato dalla, "Convenzione sui diritti dell'infanzia e dell'adolescenza" (*Convention on the Rights of the Child*, CRC) adottata e aperta alla firma e alla ratifica dall'Assemblea Generale delle Nazioni Unite con la risoluzione 44/25 del 20 novembre 1989, entrata in vigore il 2 settembre 1990. Si tratta di un trattato internazionale, vincolante per gli Stati che lo ratificano, che rappresenta una vera e propria conquista a favore del regime giuridico e della protezione dei minori.

In questo senso, l'analisi della posizione giuridica dei minori e della loro titolarità ed esercizio dei diritti non è una questione accessoria. Al contrario, dobbiamo partire dal fatto che i minori, anche se non ne sono consapevoli, esercitano quotidianamente diversi diritti, alcuni dei quali fondamentali,

[3] F. Ramón Fernández, *Menores y redes sociales: cuestiones legales*, in *Revista sobre la infancia y la adolescencia*, 8/2015, pp. 33-44, p. 35: "En cuanto a si los menores son conscientes y ejecutan las acciones sabiendo las consecuencias de sus actos ha sido objeto de un informe del proyecto europeo EU Kids Online en el que participa la Universidad del País Vasco (UPV/EHU), como ha precisado el Diario Información. El informe concluye con que sí que conocen los menores los riesgos, pero no hacen nada por evitarlo".

[4] I. Otaegui Aizpurua, *La relevancia del Tribunal Europeo de Derechos Humanos en la protección de los derechos del menor*, Pamplona, 2017, p. 34: "Aunque esta última Declaración tuviera carácter programático y sin eficacia jurídica alguna, el texto supuso un avance en el tratamiento del/ de la niño/a con respecto a la Declaración de Ginebra de 1924. En primer lugar, porque se recogieron explícitamente más derechos y ámbitos concretos de protección que no aparecían en el texto de 1924; y, en segundo lugar, – y lo más importante, en nuestra opinión –, porque el/la niño/a aparecía por primera vez como sujeto activo de derechos, a diferencia de lo que sucedía en la Declaración de Ginebra".

[5] Sul regime giuridico dell'interesse del minore nel nostro Stato, si veda, tra tutti, A. Pérez Miras, *La regulación constitucional y estatutaria de la infancia*, in M. C. Pérez Villalobos (dir.), *Los conflictos armados y la protección de la infancia. Un estudio multidisciplinar desde la perspectiva de los Derechos Humanos*, Pamplona, 2020.

nelle loro relazioni orizzontali, un aspetto necessario per lo sviluppo della loro personalità e dignità[6]. Questo aspetto deve essere collegato anche al ruolo di primo piano svolto dal mondo virtuale nella loro realtà. I cosiddetti "nativi digitali"[7] costruiscono il loro mondo intorno a Internet e ai social network, un fatto che ha conseguenze molto positive, ma che allo stesso tempo comporta grandi rischi personali. In relazione alla dignità umana, uno dei suoi pilastri fondamentali è la libera configurazione della personalità, per la quale Internet è attualmente un fattore determinante: su Internet i minori stabiliscono relazioni con i loro coetanei, plasmano i loro gusti, si arricchiscono, stabiliscono legami e, in breve, costruiscono un'immagine virtuale di se stessi che, a volte, può persino essere più importante di quella analogica.

In sintesi, per avere un'idea reale dell'entità dei rischi che comporta per i minori l'uso irresponsabile delle TIC, dobbiamo mettere in relazione aspetti quantitativi (la percentuale di utenti minorenni che usano Internet e i dispositivi mobili, che abbiamo visto sopra) e aspetti qualitativi. Tra questi ultimi, è essenziale valutare i beni giuridici che possono essere lesi, sia i diritti fondamentali detenuti ed esercitati dai minori, come il diritto all'onore, alla privacy e all'immagine di sé, la libertà di espressione o il diritto all'istruzione, sia altri beni costituzionalmente protetti, principalmente attraverso il sistema penale.

3.2. Rischi per i minori nell'uso delle ICT

Come abbiamo detto, l'uso delle ICT comporta molti rischi, non solo per i minori, ma in particolare per loro, nella misura in cui consideriamo che la loro capacità di valutarli è inferiore e il modo di affrontarli può non essere il più efficace. Poniamo, di seguito, quelli che ci sembrano più rilevanti (per la loro natura quotidiana o per il loro grado di dannosità).

3.2.1. Problemi relativi al consenso

Affrontiamo, innanzitutto, la problematica che deriva dal prestare consenso perché è un prerequisito per la comparsa del resto dei rischi. In altre parole, consideriamo che molti dei problemi che sorgono nel rapporto tra minori e nuove tecnologie hanno il loro contesto ideale nei social network, ma è chiaro che per avere accesso a un social network è necessario creare un profilo, per il quale l'utente deve fornire il consenso al trattamento dei dati. Da un punto di vista puramente cronologico, questa è la prima situazione conflittuale che si presenta; ma, inoltre, da un punto di vista legale, il controllo della veridicità del consenso può essere, come vedremo in seguito, una soluzione per una parte non trascurabile del resto dei rischi assunti.

A questo proposito, il punto essenziale è la validità del consenso dato dai minori e, più specificamente, i meccanismi di controllo della veridicità del consenso. Il Regolamento (UE) 2016/679 stabilisce all'articolo 8.1 che il trattamento dei dati è lecito se il consenso è stato dato da un minore di almeno 16 anni; tuttavia, nel paragrafo finale, offre agli Stati membri la possibilità di abbassare questo limite a 13 anni. Avvalendosi di questa disposizione, lo Stato spagnolo prevede all'art. 7.1 della "Ley Orgánica de Protección de Datos de Carácter Personal" (LOPD)[8] che: "El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años", aggiungendo al comma 2 che, per quanto riguarda i minori di 14 anni, il trattamento

[6] B. Aláez Corral, *Minoría de edad y derechos fundamentales*, Madrid, 2003, p. 57: essi [i diritti fondamentali] sono strumenti attraverso i quali l'individuo può sviluppare la propria personalità e, con ciò, occupare diversi ruoli nel processo di comunicazione sociale [...]. Ed è proprio questa funzione strumentale che permette loro di configurare la dignità della persona come loro risultato, cioè come vie per l'identificazione e il libero sviluppo dell'individuo nella sua interrelazione con gli altri.

[7] Il termine "nativo digitale" è stato utilizzato per la prima volta in M. Prensky, *Digital Natives, Digital Immigrants*, in *On the Horizon*, 5/2001.

[8] *Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales*, 5/12/2018.

"solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad".

Ci troviamo, di conseguenza, di fronte a una situazione complessa, se prendiamo in considerazione i dati illustrati nelle sezioni precedenti. Come abbiamo visto, oltre il 65% dei bambini tra i 10 e i 15 anni possiede un telefono cellulare e il 97,5% ha utilizzato regolarmente Internet negli ultimi tre mesi. Le statistiche includono quindi dati relativi ai minori di 14 anni, il cui consenso è illegittimo in assenza del consenso del titolare della potestà genitoriale e, inoltre, nei termini previsti dalla legge.

Tuttavia, senza perdere di vista quanto appena detto, basta guardare i termini e le condizioni di servizio dei social network più rilevanti per capire che la normativa, anche da un punto di vista aprioristico, non viene rispettata. Facebook, Instagram, Whatsapp o Snapchat stabiliscono un'età minima di 14 anni per essere membri (o altre età, ma avvertono che se nello Stato in cui si trova il potenziale utente la normativa è diversa, si applicheranno le disposizioni della stessa). Twitter, dal canto suo, pone il requisito in modo un po' ambiguo[9], al punto che si può dire che non sembra rispettare le disposizioni della LOPD per quanto riguarda il limite di età, fissando il minimo a 13 anni. TikTok, invece, afferma che "Los Servicios y la Plataforma están destinados únicamente a personas de al menos 13 años de edad", innalzando questo minimo a 18 nel caso del Messico.

Tuttavia, tralasciando la maggiore o minore conformità alla normativa spagnola contenuta nei diversi termini di servizio dei social network consultati, ciò che è davvero preoccupante è la mancanza di interesse da parte delle piattaforme nel verificare la veridicità del requisito dell'età. Infatti, per accedere a Facebook, Twitter o Instagram è sufficiente inserire un indirizzo e-mail valido e una data di nascita che soddisfi il requisito minimo di età, senza alcun tipo di accreditamento che lo confermi. Inoltre, nel caso in cui si inserisca una data di nascita sbagliata, cioè che non superi il limite di età richiesto, è possibile ripetere la stessa operazione semplicemente ricaricando il sito. TikTok, nel suo caso, utilizza lo stesso metodo di registrazione in prima istanza, ma rende un po' più complicato il caso in cui si inserisca una data di nascita sbagliata (anche se è sufficiente registrarsi da un altro browser).

Dal nostro punto di vista, ciò rappresenta una fonte di problemi, nella misura in cui i social network sono un mezzo favorevole per mettere in atto comportamenti lesivi dei diritti di altri minori e/o subirli da parte di altre persone. Non c'è dubbio che, allo stato attuale e per come è strutturata l'adolescenza, ogni minore che fa parte di un gruppo di amici trova nei social network nuove forme di comunicazione che prolungano e rafforzano le relazioni al di là dell'ambiente scolastico; e, viceversa, i minori che non partecipano a questo tipo di relazioni possono trovarsi allontanati dal gruppo, motivo per cui è logico comprendere perché gli adolescenti mostrino un elevato interesse a registrarsi su questo tipo di siti. Ma è anche chiaro che, quando lo fanno, non sono realmente consapevoli di ciò che stanno esponendo, di ciò che stanno regalando e di ciò che potrebbero affrontare[10]. È in questo contesto che i vari fornitori di servizi non hanno, come abbiamo appena visto, implementato metodi di registrazione che verifichino in modo affidabile la veridicità dei dati[11].

---

[9] "Puede hacer uso de los Servicios solo si accede a firmar un contrato vinculante con Twitter y no es usted una persona vetada para hacer uso de los servicios de conformidad con la legislación de su jurisdicción aplicable. En cualquier caso, usted deberá tener al menos 13 años, o 16 años en el caso de Periscope, para hacer uso de los Servicios". A nostro avviso la formulazione è quantomeno ambigua, anche se l'interpretazione più letterale della condizione "de conformidad con la legislación de su jurisdicción aplicable" sembra riferirsi a "no es usted una persona vetada para hacer uso de los servicios". In altre parole, tale circostanza si riferisce all'ipotetica situazione di divieto di accesso ai social network, piuttosto che a un generale assoggettamento normativo.

[10] F. Ramón Fernádez, *Menores y redes sociales: cuestiones legales,* cit., p. 37: "El menor no es consciente (…) de la información que facilita, ya que en la mayoría de las ocasiones infringe las normas básicas de privacidad (…) y suele aportar datos en las redes que conforman su vida familiar, económica y social, sin caer en las consecuencias de quién puede ver dicha información".

[11] R. Pérez Díaz, *Los menores de edad en la nueva Ley de Protección de Datos Personales*, in L. A. Fernández Villazón (coord.), *Derecho y nuevas tecnologías*, Navarra, 2020, p. 172: "En este marco, son significativas las denuncias presentadas ante la Agencia de Protección de Datos en la LOPD, como por ejemplo la correspondiente a un portal de Internet orientado a favorecer el contacto personal entre usuarios, fundamentalmente adolescentes o jóvenes, tratamiento de datos de menores sin consentimiento paterno, entre ellos su dirección electrónica, asociada a una imagen fotográfica y, en algunos

In definitiva, è evidente la preoccupazione per la necessità di verificare il requisito del consenso da parte dei social network. Il Regolamento (UE) 2016/679[12] lo dimostra nel suo Considerando 38, nonché nei numerosi riferimenti ai requisiti che l'espressione del consenso deve soddisfare per essere considerata valida. Pertanto, l'articolo 4, paragrafo 11, stabilisce che il consenso della persona interessata è "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". A nostro avviso, questi fornitori di servizi non rispettano le disposizioni del diritto dell'Unione europea e nazionale, in quanto non viene rispettata l'età minima per il rilascio del consenso o, quantomeno, non sono stati inclusi i metodi per verificare l'età (o il consenso del titolare della potestà genitoriale, per i minori di 14 anni), come previsto dall'articolo 8.2 del Regolamento (UE) 2016/679[13].

3.2.2. L'anonimato

Un altro aspetto che può portare a vari problemi è quello dell'anonimato[14]. La creazione di profili sui social network non è controllata, non solo per quanto riguarda l'età dell'utente, ma anche per quanto riguarda la sua identità. Per registrarsi è necessario disporre di un account di posta elettronica valido (per la cui creazione non è richiesta nemmeno la verifica dell'identità) e inserire una data di nascita. Dopodiché, il social network di solito favorisce l'inserimento del maggior numero possibile di dati (nome, cognome, fotografie, gusti personali, link ad altri social network, ecc). Questo porta alla creazione di profili falsi (cioè profili che includono dati credibili ma che non appartengono realmente all'utente) o di profili anonimizzati, cioè con informazioni che non permettono di identificare l'utente perché non seguono la logica dei dati. Esempi famosi di questi ultimi sono i personaggi di Twitter come "La vecina rubia", "Maestra de Pueblo" o "Jurista Enloquecido".

Partendo da questa idea, non sembra necessario approfondire le conseguenze di questa scelta. Non si tratta più solo del fatto che i metodi per verificare il requisito dell'età sono praticamente inesistenti; ora bisogna aggiungere che è molto facile creare un profilo falso o anonimo, il che comporta un senso di impunità (in un certo senso incerta, perché sappiamo che su Internet quasi ogni azione lascia una traccia indelebile) e un'ulteriore difficoltà nel caso in cui si voglia monitorare o porre fine a certi comportamenti dannosi. Comunque sia, questo tipo di profilo facilita la comparsa di altri rischi più

---

casos, al nombre de usuario. Las medidas adoptadas para verificar que los usuarios eran mayores de 14 años no se demostraron eficaces".

[12] A. Lambea Rueda, *Entorno digital, robótica y menores de edad*, in *Revista de Derecho Civil*, 4/2018, p. 196: "El RGPD se ocupa de los menores y su consentimiento como punto clave para el acceso a sus datos y actuación en el entorno digital […]. El consentimiento es considerado por el Reglamento no sólo como un requisito de legitimación y garantía del tratamiento de datos personales, sino que se constituye como derecho del interesado, generando un deber por parte del responsable del tratamiento de datos a obtenerlo en las condiciones legalmente previstas".

[13] "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". [txt corretto del documento].

[14] Per quanto riguarda l'anonimato e il suo rapporto con la libertà di espressione, si tratta di una questione già dibattuta dalla dottrina e persino dallo stesso *Tribunal Constitucional* (TC). I fornitori di servizi basano il loro rifiuto di fornire i dati degli utenti con profili anonimizzati su un presunto effetto deterrente sull'esercizio della libertà di espressione. Il TC afferma che non c'è libertà di espressione (almeno non quella che dovrebbe essere costituzionalmente protetta) nei casi in cui non c'è un autore conosciuto (SSTC 200/1998, 153/2000 e 204/2001). Tuttavia, per quanto riguarda il rapporto tra l'anonimato nel cyberspazio e la libertà di espressione, si veda, per tutti, I. Villaverde Menéndez, *Libertad de expresión, anonimato y ciberespacio*, in L. A. Fernández Villazón (coord.), *Derecho y nuevas tecnologías*, cit. L'autore sostiene che la pretesa di anonimato e, soprattutto, di non divulgazione da parte dei fornitori di servizi non è realmente finalizzata a tutelare la libertà di espressione evitando un effetto scoraggiante, ma piuttosto la volontà di proteggere i dati degli utenti, anche se questo può comportare il mantenimento di contenuti offensivi o, se necessario, ostacolare lo sviluppo di un'azione legale: "El TEDH […] argumenta que, sin dudar de los beneficios que el anonimato ofrece para un discurso público robusto en el ciberespacio, no debe obviarse que ese mismo anonimato fomenta la propagación de expresiones injuriosas y denigrantes, y llevado al extremo puede frustrar cualquier remedio judicial efectivo frente a la difamación de la vida privada de terceros" (p. 310).

dannosi, come quelli che vedremo di seguito.

3.2.3. La commissione di reati

È innegabile che le ICT abbiano portato una rivoluzione nella comunicazione. Gli utenti sono permanentemente connessi alla rete e inviano informazioni, che possono essere pubbliche o parzialmente private, esponendo la loro immagine, i loro gusti, le loro abitudini, ecc.[15] Ciò rappresenta una fonte di informazioni rilevanti per facilitare la commissione di reati come frodi o furti. Tuttavia, ci concentreremo sui reati che possono essere commessi esclusivamente attraverso le nuove tecnologie[16] e, nello specifico, su quelli in cui i minori possono essere vittime o autori.

Tralasciando i reati tradizionalmente definiti che possono essere commessi anche nel mondo virtuale (ingiurie, calunnie, minacce, ecc.), accenniamo brevemente a quelli che sono stati recentemente criminalizzati a seguito dell'espansione dell'uso delle nuove tecnologie. Così, in primo luogo, troviamo l'adescamento (art. 183 ter CP), che è: "el acoso ejercido por un adulto y que se refiere a las acciones realizadas deliberadamente para establecer una relación y un control emocional sobre el menor con el fin de preparar el terreno para el abuso sexual del mismo"[17]. Si tratta, quindi, di un adulto che, generalmente attraverso un falso profilo sui social network, riesce a entrare in contatto con un minore, dal quale intende ottenere una qualche prestazione sessuale[18].

Un altro nuovo reato è la "vessazione" (stalking e cyberstalking), che è incluso nell'art. 172 ter CP che implica "comportamientos que pueden incluir, aunque no están limitados solo a éstos, la transmisión de amenazas y acusaciones falsas, daños a los datos o equipos, robo de identidad, robo de datos, 'monitoreo' informático, la solicitud de sexo y cualquier otra forma de agresión"[19], ma con una nota di continuità, richiesta dal legislatore nel reato attraverso le caratteristiche di "insistente e reiterato"[20].

Infine, possiamo evidenziare il sexting, incluso nell'art. 197.7 CP, che "consiste en la difusión o publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil o cualquier otro dispositivo tecnológico"[21].

3.2.4. Il cyberbullismo scolastico

Infine, ci troviamo di fronte a questo fenomeno, replica ed estensione del bullismo. Ci sono diverse

---

[15] Esistono campagne periodiche da parte di diverse istituzioni e organizzazioni, tra cui il Corpo e le Forze di Sicurezza dello Stato che avvertono che questo tipo di comportamento facilita la commissione di reati (ad esempio, in estate è comune postare sui social network l'imminente partenza di un viaggio o foto da luoghi diversi dall'abitazione abituale, cosa che le Forze dell'Ordine hanno più volte sconsigliato.

[16] N. García Guilabert, *El ciberacoso. Análisis de la victimización de menres en el ciberespacio desde la Teoría de las actividades cotidianas*, Madrid, 2017. L'autore propone diverse classificazioni dei crimini che possono essere commessi nel cyberspazio, di cui ne evidenziamo due: la prima ritiene che esistano tre tipi, i cyber-attacchi puri, i cyber-attacchi di replica e i cyber-attacchi di contenuto; la seconda include anch'essa tre categorie, i cyber-crimini economici, i cyber-crimini sociali e i cyber-crimini politici. All'interno di questa sistematizzazione, tra i crimini informatici sociali rientrano quelli di cui i minori possono essere più facilmente vittime o autori: "En efecto, la gran mayoría de los cibercrímenes sociales o personales que se perpetran no son más que […] ciberataques réplica, esto es, copias en el ciberespacio de delitos que ya existían anteriormente, pero que sólo se ejecutaban en el espacio físico. Las injurias, las calumnias, las amenazas, el acoso sexual y todo un conjunto de conductas que se pueden realizar sin que sea necesaria una cercanía física entre agresor y víctima, también se pueden realizar cuando ésta existe" (p. 17).

[17] S. Mendoza Calderón, *El Derecho Penal frente a las formas de acoso a menos. Bullying, ciberbullying, grooming y sexting*, Valencia, 2013, p. 99.

[18] La SAP Jaén, sezione 2, 113/2015 dell'11 maggio (JUR20151561) definisce esattamente in cosa consiste l'adescamento di minori.

[19] N. García Guilabert, *El ciberacoso,* cit., p. 24.

[20] STS, Sala de lo Penal, Sección 1ª, 324/2017, dell'8 maggio (in particolare FFJJ 3 e 4).

[21] INTECO, *Guía sobre adolescencia y sexting, qué es y cómo prevenirlo*, 2011 (versione online), p. 4. Interessanti i contributi sul reato di sexting di S. Mendoza Calderón, *Derecho Penal frente a las formas de acoso a menos,* cit., p. 170; e di E. Pérez Conchillo, *Intimidad y difusión de sexting no consentido*, Valencia, 2018.

ragioni che ci inducono a pensare che meriti uno studio dettagliato, separato dalle categorie discusse nella sezione precedente. In primo luogo, il cyberbullismo costituisce il punto di incontro tra diversi aspetti che sono oggetto di studio del diritto costituzionale: 1) la titolarità e l'esercizio dei diritti fondamentali (diritto all'istruzione, libertà di espressione, diritto all'onore, alla privacy e all'immagine di sé, tra gli altri); 2) un gruppo che necessita di particolare protezione come protagonista (i minori); 3) possibili cause con particolare rilevanza costituzionale (questioni di genere, appartenenza a diversi livelli socio-economici, discriminazione per orientamento e/o identità sessuale, xenofobia o disabilità); 4) e, infine, la necessità di misure preventive, responsabilità e riparazione che possono coinvolgere istituzioni pubbliche e private. Inoltre, non può essere affrontato direttamente dal diritto penale, a causa della varietà di condotte che possono essere implicate, come vedremo di seguito. In secondo luogo, si tratta di un problema più comune rispetto alla condotta criminale descritta nella sezione precedente. Infine, l'analisi del bullismo e del cyberbullismo scolastico è stata tradizionalmente affrontata dalla psicologia e dalla pedagogia; ad entrambe le discipline si è aggiunto negli ultimi tempi il diritto, ma attraverso approcci prevalentemente civili e penali, anche se il costituzionalismo ha molto da apportare per le ragioni che abbiamo appena visto.

Come punto di partenza, va sottolineato che concettualizzare ciò che dovremmo intendere per bullismo[22] e cyberbullismo è un compito complesso[23]. Ovviamente sono state proposte diverse definizioni teoriche per entrambi i termini, ma individuare quando ci si trova di fronte a una situazione di bullismo, incrociando variabili come l'età, la frequenza e la nocività, è difficile, ancor più se si tiene conto delle conseguenze che possono derivare non solo per la vittima e l'autore, ma anche per i coetanei che assistono.

Merino González afferma che il primo ad affrontare il problema del bullismo è stato Olweus, nel 1993, definendolo come "una conducta de persecución física o psicológica que realiza el alumno o alumna contra otro, al que elige como víctima de repetidos ataques. Esta acción, negativa e intencionada, sitúa a las víctimas en posiciones de las que difícilmente pueden salir por sus propios medios"[24]. Per essere considerate tali, le molestie devono essere prolungate nel tempo, attraverso aggressioni fisiche, umiliazioni, insulti, minacce, coercizione o isolamento della vittima, anche se è comune che diversi di questi comportamenti si verifichino contemporaneamente (questa varietà di comportamenti complica, come già detto, il suo trattamento dal punto di vista legale). Le conseguenze per la vittima[25] e per l'autore[26] sono di diversa natura e si manifestano in varia misura, anche se, per quanto minime, riteniamo che siano sufficientemente importanti per cercare di trovare soluzioni efficaci in modo risolutivo, come dimostrano i seguenti dati: il 94% delle persone colpite soffre di qualche problema psicologico derivato dalla situazione di molestia; tra le conseguenze gravi, il 2,4% soffre di autolesionismo, il 4,6% ha idee suicide e l'1,2% ha tentato il suicidio[27].

Il cyberbullismo, invece, ha elementi di definizione molto simili a quelli del bullismo, in quanto

---

[22] La Procura Generale dello Stato ha studiato questo fenomeno nell'Istruttoria 10/2005, sul trattamento del bullismo nel sistema giudiziario minorile.

[23] A. Pérez Vallejo, F. Pérez Ferrer, *Bullying, ciberbullying y acoso con elementos sexuales: desde la prevención a la reparación del daño*, Madrid, 2016, p. 18: "Aunque hoy en día no existe una definición jurídica unánime, las aportaciones doctrinales y jurisprudenciales mayoritarias vienen a concretar que estamos ante un comportamiento intencionado, –prolongado o repetitivo en el tiempo – de agresión física y/o insultos verbales, situaciones de rechazo o aislamiento social, intimidación psicológica, etc., realizado por uno o varios menores para dañar a la víctima, y poder doblegar de esta forma su voluntad".

[24] J. Merino González, *El acoso escolar-bullying. Una proposta di studio dall'analisi delle reti sociali (ARS)*, in *Revista d'Estudis de la violencia*, 4/2008.

[25] Id.*:* "La continuidad de estas relaciones provoca en las víctimas efectos claramente negativos: disminución de su autoestima, estados de ansiedad e incluso cuadros depresivos, lo que hace difícil su integración en el medio escolar y el desarrollo normal de los aprendizajes".

[26] Nell'Istruttoria 10/2005, la Procura ritiene che se non vengono corretti tempestivamente e con fermezza, oltre a essere rafforzati dall'acquisizione di un certo rilievo tra i coetanei, i loro "comportamiento agresivo puede convertirse en una forma habitual de actuar haciendo de la dominación un estilo normalizado en sus relaciones interpersonales".

[27] Uno studio più concreto e molto interessante si trova in Fundación Anar, *III Estudio sobre acoso escolar y cyberbullying según los afectados*, 2018.

richiede anch'esso un certo tipo di comportamento dannoso (molesto, intimidatorio, umiliante, ecc.) con una certa frequenza. Tuttavia, occorre tenere presente che il cyberbullismo può costituire un'estensione del bullismo "analogico", nel caso in cui la vittima e il bullo condividano la stessa scuola. Oltre a ciò, vanno notate tre differenze fondamentali: 1) il cyberbullo può facilmente rimanere anonimo, come abbiamo visto sopra; 2) i potenziali testimoni sono molti di più, trascendendo l'ambiente puramente scolastico a un contesto sociale più ampio; 3) e gli atti di umiliazione (sotto forma di commenti, isolamento, immagini, ecc.) possono essere ancorati nei social network, il che, insieme al numero di testimoni, può comportare un danno maggiore per la vittima (soprattutto se la procedura per richiederne la rimozione è complessa, anche se è vero che negli ultimi tempi i meccanismi di segnalazione delle pubblicazioni da parte dei fornitori di servizi sembrano essersi snelliti).

Infine, non possiamo non sottolineare un altro dato che, dal nostro punto di vista, è molto significativo. Infatti, l'età media delle vittime di bullismo è di 10,9 anni (e l'età media all'inizio del bullismo è di 9,8 anni, la situazione generalmente si prolunga per un anno) e quella degli autori è di 11,3 anni; mentre l'età media della vittima di cyberbullismo è di 13,5 anni, l'età media all'inizio è di 12,2 anni e l'età media dell'autore è di 13,9 anni[28]. Al di là dell'interpretazione penale di questi dati (la responsabilità penale dei minori è perseguibile in Spagna a partire dai 14 anni), dobbiamo collegarli alle norme sulla validità del consenso. Comunque sia, ciò che appare chiaro è che esiste una notevole discrepanza tra il requisito dell'età stabilito dalla LOPD e la realtà, come abbiamo visto nei dati forniti dall'INE sull'uso dei dispositivi e di Internet e quelli raccolti dalla Fondazione ANAR nei suoi studi.

4. Possibili soluzioni

Non c'è dubbio che ci troviamo di fronte a una sfida di notevole portata, poiché sono in gioco beni giuridici di enorme importanza. Allo stesso modo, tutti quelli menzionati costituiscono problemi la cui soluzione è urgente, poiché le conseguenze per le vittime, a prescindere dal tipo di comportamento, sono preoccupanti: problemi psicologici, sociali e/o accademici difficili da gestire per gli adulti, e ancor più se subiti da minori.

Per questo motivo riteniamo necessario cercare una risposta in maniera decisa. È ovvio che queste soluzioni devono coinvolgere la società nel suo complesso con una visione a lungo termine, dando a questi problemi l'importanza che meritano. Tuttavia, dal nostro punto di vista, è possibile implementare alcune soluzioni che affronteranno alcuni di questi fenomeni nel breve termine e, allo stesso tempo, ostacoleranno l'emergere di altri.

Pertanto, riteniamo che l'implementazione di meccanismi efficaci per verificare chi dà il consenso nei registri degli utenti dei social network è un'azione relativamente semplice per i fornitori di servizi e aiuterebbe non solo a controllare meglio alcune situazioni, ma anche a ottenere un effetto deterrente preventivo utile quanto il controllo stesso. Non si tratta di impedire l'accesso ai social network ai minori di 14 anni, ma di coinvolgere i titolari della potestà genitoriale nella sorveglianza e nel controllo dell'attività che i minori svolgono su queste applicazioni (ribadiamo il fatto che la quasi totalità degli utenti minorenni di Internet si connette da casa propria, quindi è fondamentale che i genitori o i tutori siano coinvolti attivamente in questo compito di controllo). Brito Izquierdo[29] e Bartolomé Tutor[30] suggeriscono diversi meccanismi ragionevoli per effettuare questa verifica; anche

[28] *Ibid*.

[29] N. Brito Izquierdo, *Tratamiento de los datos personales de menores de edad: supuestos, límites, retos y desafíos*, in *La Ley Derecho de Familia: Revista jurídica sobre familia y menores*, 14/2017. L'autore propone diverse alternative per verificare il consenso a priori e a posteriori.

[30] A. Bartolomé Tutor, *Los derechos de la personalidad del menor de edad*, Pamplona, 2015, p. 293: "Para la comprobación de la edad de los menores proponemos que se haga a través de la fórmula E-ID (E-Identity Document), que es un carné electrónico oficial, que permite el acceso a determinadas páginas web, cuyo código de acceso identifica inmediatamente al menor, y que además contiene los nombres de los padres o a través de los nuevos DNI y sus certificados de firma electrónica, que permiten la identificación electrónica de los menores".

altri autori, come Lambea Rueda, avanzano proposte simili, sebbene suggeriscano che il costo debba essere condiviso tra il fornitore del servizio e l'utente[31]. Non dimentichiamo che le società di gioco d'azzardo che operano online hanno dovuto istituire un sistema di verifica dell'identità affidabile per confermare che l'utente sia maggiorenne. Non si può fare a meno di chiedersi, con una certa sorpresa, perché non si possa chiedere lo stesso alle imprese di social media.

Inoltre, riteniamo opportuno che i profili siano ancorati alle identità reali, il che può essere fatto attraverso la stessa operazione di verifica del consenso. Verificando che l'utente abbia più di 14 anni (o che sia autorizzato da chi esercita la patria potestà), gli viene consentito di creare un profilo collegato a dati reali, per cui il fatto che tale profilo abbia dati anonimizzati diventa irrilevante, in quanto la ricerca del vero "titolare" del profilo viene effettuata in modo molto più semplice. Non dimentichiamo che i social network sono un ambiente ideale per mettere in atto le condotte dannose sopra descritte (grooming, stalking o cyberbullismo), soprattutto quando l'utente si rifugia in un profilo falso o anonimo. Se potessimo verificare l'identità reale e collegarla al profilo, questo avrebbe, dal nostro punto di vista, un effetto preventivo rispetto a queste situazioni, poiché la sensazione di impunità sarebbe notevolmente ridotta.

In breve, riteniamo che un controllo rigoroso sulla creazione di profili utente possa essere un buon rimedio a breve termine, sia in termini di età che di identità dell'utente. Oltre all'effetto deterrente, faciliterebbe anche l'assunzione di responsabilità per eventuali danni. E, non da ultimo, sarebbe effettivamente conforme alla legislazione europea in materia. È vero che le risposte a lungo termine a tutti questi problemi devono basarsi sull'educazione, sul coinvolgimento dei genitori, delle famiglie, dei centri educativi e della società in generale nell'educazione globale dei minori, nel renderli consapevoli dei rischi connessi alle nuove tecnologie e della necessità di rispettare gli altri come parte dei valori democratici incarnati dal nostro Stato di diritto. Allo stesso tempo, però, non è meno vero che questo tipo di azione richiede tempo e una spinta decisa a impegnarsi in un dibattito che coinvolga l'opinione pubblica nel suo complesso, un compito piuttosto complesso. D'altra parte, il controllo proposto non sembra eccessivamente difficile da attuare e può portare benefici in breve tempo.

5. Conclusioni

Abbiamo visto che, riprendendo l'espressione degli stessi adolescenti, il rapporto che si è instaurato tra i minori e le nuove tecnologie è in qualche modo tossico. I bambini e gli adolescenti costruiscono una parte importante della loro esistenza nel mondo virtuale; non vivono "con" Internet, ma "su" Internet. Le ICT, in generale, ci hanno fornito un insieme di strumenti il cui valore in termini di lavoro, scienza e comunicazione è praticamente incalcolabile, tanto che oggi non possiamo capire la nostra vita quotidiana senza di esse. Questo progresso ha comportato anche l'assunzione di alcuni rischi, molti dei quali riguardano la messa in pericolo di beni giuridici costituzionalmente protetti, soprattutto quando gli utenti sono minori, un gruppo particolarmente vulnerabile.

Rispetto ai problemi sopra esposti, si possono stabilire due categorie specificamente differenziate: la prima, costituita da quelli relativi al consenso e all'anonimato, in quanto costituiscono di per sé la condizione per la configurazione di un contesto favorevole all'emersione di quelli del secondo gruppo, in modo da poterli affrontare in modo aprioristico; la seconda, costituita da alcuni reati di tradizionale criminalizzazione (come insulti, minacce, ecc.), altri di recente criminalizzazione (come grooming, stalking o sexting) e il cyberbullismo scolastio (fenomeno che può manifestarsi in modi diversi).

Partendo dall'idea che la soluzione di questi problemi richiede un coinvolgimento sociale, a partire

[31] A. Lambea Rueda, *Entorno digital, robótica y menores de edad,* cit., p. 193: "Para el control de acceso a redes de los menores, debería implementarse por ley la obligación de los proveedores de facilitar mecanismos de control, sujetos a un conste compartido con el usuario. Se trataría de incluir funcionalidades ofrecidas por las compañías de acceso a redes y servicios, obligatorias en caso de menores. Ya hay sistemas de control parental de pago para controlar el acceso, o a través de la publicidad".

da un dibattito approfondito sui limiti che vogliamo porre ai nostri minori, fino all'adozione di misure educative la cui efficacia dovrà essere valutata in un futuro un po' più lontano, è necessario cercare alternative a breve termine che possano contribuire a rendere più sicuro l'ambiente virtuale in cui tutti noi operiamo, soprattutto i minori. A questo proposito, riteniamo che la verifica dell'età degli utenti dei social network e, nel caso di minori di 14 anni, del consenso da parte del titolare della potestà genitoriale, insieme all'ancoraggio dell'identità dei profili a un'identità reale, siano due misure che assolverebbero perfettamente a questo compito in tempi relativamente prudenti e, inoltre, non sembrano di difficile attuazione, come dimostrano alcuni precedenti (centri scommesse online, ad esempio).

_____

Abstract

Negli ultimi due decenni si è avuta una crescita esponenziale dell'uso delle nuove Tecnologie dell'Informazione e della Comunicazione che stanno indubbiamente segnando un prima e un dopo nella storia dell'umanità. Questo fenomeno porta con sé, oltre a indubbi vantaggi, una serie di rischi. contributo si propone di affrontare il tema dei rischi più rilevanti che i minori possono incontrare nell'uso delle nuove tecnologie, concentrandosi in particolare sul cyberbullismo nelle scuole; e, in secondo luogo, per sollevare alcune domande e indicare alcune possibili soluzioni accomunate dalla necessità che il diritto costituzionale sia coinvolto in modo decisivo nell'affrontare questi problemi, integrando così altre branche del diritto (principalmente il diritto penale e civile) e altre discipline (come la psicologia e la pedagogia).

Parole chiave: ICT, minori, cyberbullismo

*****

The last two decades have seen an exponential growth in the use of new Information and Communication Technologies that are undoubtedly marking a before and after in human history. This phenomenon brings with it, in addition to undoubted advantages, a number of risks. contribution aims to address the most relevant risks that minors may encounter in the use of new technologies, focusing in particular on cyberbullying in schools; and, secondly, to raise some questions and indicate some possible solutions united by the need for constitutional law to be decisively involved in addressing these problems, thus integrating other branches of law (mainly criminal and civil law) and other disciplines (such as psychology and pedagogy).

Key words: ITC, young people, cyberbullying