Il fenomeno del cyberbullismo

Ciberspazio e diritto, vol. 24, n. 75 (3 - 2023), pp. 223-234

Aspetti psicologici e riflessioni sul cyberbullismo in Italia

Lisa Carboni*

Sommario: 1. Bullismo e cyberbullismo. – 2. La sofferenza delle vittime. – 3. Soggetti a cui si rivolge la legge e mondo adulto di riferimento.

1. *Bullismo e cyberbullismo*

Sinteticamente, potremmo definire il bullismo come una forma di aggressività dove è presente «la pianificazione dell'atto, la ripetizione sistematica di un comportamento, la disparità di potere tra chi agisce e chi "subisce", la notorietà dell'atto»[1]. Non è, quindi, una violenza nascosta, dato che, per l'aggressore, riveste particolare importanza il ruolo degli spettatori a cui rendere pubbliche le vessazioni esercitate: «gli atti di bullismo sono più efficaci, nella visione del persecutore, quando avvengono in presenza di testimoni e vengono diffusi attraverso i social network»[2].

Se si pensa, pertanto, alle caratteristiche e alla finalità della violenza, potremmo sostenere che il cyberbullismo non è che l'evoluzione informatizzata del bullismo. *De facto*, però, la tecnologia trasforma e connota in maniera differente la brutalità. Nel caso del cyberbullismo, la connessione alla rete e la vastità potenziale della stessa amplificano le violenze nel tempo e nello spazio: si pensi al tempo di permanenza sui mezzi virtuali ma, anche, alla sopravvivenza dei contenuti immessi (che possono a volte riemergere anche dopo anni), allo spazio di diffusione e alla platea raggiungibile (ivi comprese persone sconosciute alla vittima). Que-

* Laureata in Filosofia e Perfezionata all'Università degli Studi di Milano (in particolare in "Criminalità Informatica e Investigazioni Digitali" e in "Strumenti giuridici per la prevenzione e il contrasto alla violenza di genere").

[1] Cfr. G. Daffi, C. Prandolini, *Mio figlio è un bullo? Soluzioni per genitori e insegnanti*, Trento, Erickson, 2012, p. 15.

[2] Cfr. M.A. Gallina (a cura di), *Dal bullismo al cyberbullismo: strategie socio-educative*, Milano, Franco Angeli, 2019, p. 32.

doi 10.53148/CD202303001

sta mancanza di confini diventa particolarmente temibile, non solo perché chi la subisce si sente senza un luogo sicuro, ma anche perché «la vera matrice simbolica che qualifica lo scontro con il cyberbullo è la mancanza quasi totale di individuazione immediata dell'attacco»[3], considerando che «con l'informatica è anche possibile implementare delle forme di automatizzazione delle espressioni d'odio, inserendo e temporizzando gli attacchi in automatico, a cadenze regolari, anche quando il soggetto attivo è altrove e dedito ad altre attività»[4].

Anche l'aggressore ha mutato fisionomia. La superiorità fisica può essere soppiantata da una migliore conoscenza della tecnologia: «così nel mondo virtuale non conta più il muscolo, ma la maggior capacità di sferrare ogni diverso tipo di attacco informatico»[5] e l'aggressore può, a differenza di quanto avviene in presenza, offendere senza svelare la propria identità alla vittima.

Stante queste premesse, non stupisce che i dati dell'Osservatorio "indifesa" riportino che la maggior parte dei ragazzi si senta esposta quando naviga e che a preoccuparli sia proprio il rischio di cadere vittime di cyberbullismo[6].

La piattaforma ELISA (formazione di *E-learning* degli Insegnanti sulle Strategie Antibullismo), nata a seguito dell'entrata in vigore della legge n. 71/2017 e dell'emanazione delle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo (nota MIUR prot. n. 5515 del 27-10-2017), riporta i seguenti dati rilevati nell'anno scolastico 2021-

[3] Cfr. M. D'Ambrosio, *Cyberbullismo e devianza emozionale. La comprensione del comportamento deviante nella sintesi tra reale e virtuale*, Trento, Erickson, 2020, p. 7.

[4] Cfr. M. Bergonzi Perrone, *Cyberstalking e cyberbullismo*, Milano, Giuffrè Francis Lefebvre, 2022, p. 16.

[5] *Ivi*, p. 19.

[6] «Le nuove generazioni sono consapevoli dei pericoli del web: ben 7 ragazzi su 10 dichiarano di non sentirsi al sicuro quando navigano in rete. A preoccuparli maggiormente è proprio il rischio di cyberbullismo (68,8%), seguito da revenge porn (60%), furto di identità (40,6%) e stalking (35%), ma anche l'alienazione dalla vita reale (32,4%) con la creazione di modelli e standard irraggiungibili è fonte di enorme frustrazione. Al di fuori degli schermi virtuali, invece, il 50% degli adolescenti dice di aver paura di subire violenza psicologica e bullismo (44%)».

Cfr. "Bullismo e cyberbullismo", i dati dell'Osservatorio indifesa, 2022, disponibile al link https://www.minori.gov.it/it/notizia/bullismo-e-cyberbullismo-i-dati-dellosservatorio-indifesa (ultimo accesso in data 8 agosto 2023).

Aspetti psicologici e riflessioni sul cyberbullismo in Italia

Il testo è stato scritto riferendosi volutamente e principalmente a fonti pubblicate negli ultimi anni. Dopo una breve panoramica sugli aspetti del bullismo e del cyberbullismo in Italia, l'Autrice si focalizza sul vissuto delle vittime per poi esporre riflessioni e dubbi sull'incapacità del mondo adulto di dare una risposta coerente alle discriminazioni e alla violenza.

Psychological aspects and reflections on cyberbullying in Italy

The text has been intentionally and primarily written referring to sources published in recent years. After a brief overview of the aspects of bullying and cyberbullying in Italy, the Author focuses on the experience of the victims and then exposes reflections and doubts about the inability of the adult world to provide a coherent response to discrimination and violence.

Ciberspazio e diritto, vol. 24, n. 75 (3 - 2023), pp. 235-250

Cyberbullismo e adolescenza: la dimensione digitale di un fenomeno (anti)sociale

Letizia Mantovani*

Sommario: 1. Introduzione. – 2. Vittime e carnefici: l'ambivalente ruolo degli adolescenti nelle dinamiche di *cyberbullying*. – 3. Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo: la legge 29 maggio 2017, n. 71. – 4. Profili di rilevanza penale. – 5. Il ruolo fondamentale della giustizia minorile.

1. *Introduzione*

Tra le forme di devianza tipiche dell'età giovanile risalta, per frequenza e impatto sociale, il fenomeno del bullismo, i cui tratti distintivi si identificano nella reiterazione di comportamenti ostili e nella prevaricazione del soggetto "bullizzante" nei confronti della vittima[1].

In una dinamica relazionale tra pari si verifica, pertanto, uno squilibrio di potere ingiustificato a favore di chi ricorre a comportamenti aggressivi e discriminatori per affermare la propria personalità[2]. Tale condizione di disuguaglianza può essere determinata da diversi fattori, anche fra loro combinati, quali il ricorso alla forza fisica, l'età dei coinvolti, il contesto socioculturale di provenienza e, nel caso in cui gli atti vengano perpetrati all'interno di dinamiche di gruppo, il numero degli aggressori[3].

* Avvocato e dottoranda presso il dipartimento "Cesare Beccaria" dell'Università degli Studi di Milano.

[1] Cfr. L. Savonardo, R. Marino, *Adolescenti always on: social media, web reputation e rischi online*, collana "Culture giovanili", Milano, Franco Angeli, 2021.

[2] Cfr. D. Olweus, *Bullismo a scuola. I ragazzi oppressi, ragazzi che opprimono*, Firenze, Giunti Editore, 2007.

[3] Cfr. A.L. Pennetta, G. Zilliotto, *Bullismo, cyberbullismo e nuove forme di devianza*, Torino, Giappichelli Editore, 2019.

doi 10.53148/CD202303002

Particolare rilievo assume, poi, la dimensione sociale connaturata al fenomeno del bullismo e alle sue manifestazioni. Se non può esserci prevaricazione senza una vittima che la subisca, è allora necessaria una base relazionale in cui tale dinamica possa realizzarsi.

Sotto questo aspetto, oltre ai tradizionali luoghi fisici di aggregazione, nell'ultimo ventennio, hanno assunto sempre maggior rilievo nuove forme di relazione sociale, il cui presupposto di funzionamento è rappresentato dalla connessione digitale tra le persone. Divenuti parte integrante dell'esperienza quotidiana di milioni di utenti in tutto il mondo, infatti, i social media sono universalmente percepiti come ambienti di relazione, in cui è possibile costruire e gestire legami sociali. La quotidianità del vissuto personale viene, così, proiettata in una dimensione virtuale, dove l'interazione con l'altro è più immediata e più semplice. Si può, quindi, dire che l'utilizzo di tali piattaforme costituisce una forma di espressione dell'identità individuale, all'interno di una formazione sociale che, per quanto "dematerializzata", mostra evidenti caratteri di realtà.

Con la nascita di questo nuovo modello di comunicazione, il web ha assunto una funzione sempre più "partecipativa", consentendo la creazione e la circolazione di contenuti mediante il contributo delle persone che degli stessi fruiscono[4]. Tali dinamiche di condivisione hanno acquisito, giocoforza, una valenza culturale sempre più pregnante: il concetto di "community" identifica, infatti, una collettività che non è solo destinataria di un flusso di informazioni, ma che ne diviene altresì utilizzatrice, interprete e, in ultima istanza, co-creatrice.

La frequenza e la trasversalità delle interazioni tra emittenti e riceventi rendono le dinamiche di condivisione, nell'era digitale, parte integrante dell'esperienza sociale. Le relazioni che si instaurano sui social media sono, infatti, caratterizzate da reciprocità e da una situazione di assoluta parità, quanto a disponibilità di mezzi e capacità di comunicazione, tra gli utenti.

Tra gli aspetti che caratterizzano questa tipologia di dinamiche sociali, oltre alla permanenza online degli scambi avvenuti sui social network e alla loro tracciabilità, assume particolare rilevanza anche il fenomeno del "collasso dei contesti". Se la rappresentazione di sé è solitamente frutto di

[4] Cfr. D. Bennato, *Sociologia dei media digitali. Relazioni sociali e processi comunicativi del web partecipativo*, Bari, Editori Laterza, 2011.

Cyberbullismo e adolescenza: la dimensione digitale di un fenomeno (anti)sociale

I continui e repentini cambiamenti determinati dall'inarrestabile evoluzione tecnologica hanno comportato l'insorgenza di inedite forme di disagio sociale, delle quali le nuove generazioni, native digitali, sono le principali vittime. A destare preoccupazione è, in particolare, il ricorso degli adolescenti alle nuove tecnologie per commettere azioni aggressive e prevaricatrici nei confronti dei coetanei. La possibilità di avvalersi dell'anonimato e la presenza di una barriera virtuale tra persecutore e vittima consentono l'abbandono di ogni inibizione, con il rischio concreto di una spirale crescente di violenza. Il presente contributo analizza la classificazione del fenomeno del cyberbullismo sotto il profilo giuridico e presenta una disamina delle principali forme di tutela, preventive e repressive, individuate dall'ordinamento italiano per contrastarne la diffusione.

Cyberbullying and adolescence: the digital dimension of an (anti)social phenomenon

The dramatic increase in the use of new technologies as a part of our everyday life has important social implications, especially among adolescents. Reported as an aggressive, intentional act carried out by juveniles, cyberbullying aims to socially exclude, threaten, insult, or shame another person, using new communication devices. The aim of this paper is to provide a brief overview of the actions the Italian legal system has adopted to prevent and counteract the cyberbullying phenomenon.

Ciberspazio e diritto, vol. 24, n. 75 (3 - 2023), pp. 251-272

Minori e diritto all'oblio: la normativa sul cyberbullismo e il ruolo del Garante per la protezione dei dati personali

Nicola Nappi[*]

Sommario: 1. Nozione e brevi cenni sulle caratteristiche del cyberbullismo. – 2. Inquadramento storico-normativo del fenomeno del cyberbullismo. – 3. Il diritto all'oblio dei minori sancito dall'art. 2 della l. 71/2017. – 4. Il ruolo del Garante per la protezione dei dati personali nella rimozione dei contenuti. – 5. Conclusioni.

1. *Nozione e brevi cenni sulle caratteristiche del cyberbullismo*

Il cyberbullismo emerge come una manifestazione della diffusione di contenuti aggressivi online, dove si manifestano espressioni d'odio dirette verso singoli individui, a volte senza una chiara motivazione. Tale fenomeno si configura come una serie di autentici attacchi personali, connotati da una natura aggressiva e dannosa.

Nell'ormai lontano 2002, fu l'educatore canadese Bill Belsey a coniare il termine, descrivendo il fenomeno come un comportamento ostile e ripetuto, deliberatamente perpetrato attraverso l'utilizzo di strumenti informatici e, più precisamente, «Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, which is intended to harm others»[1].

[*] Giurista, Master Universitario di II livello in Informatica Giuridica, nuove tecnologie e diritto dell'informatica, Master Universitario di I livello in Diritto delle Nuove Tecnologie ed Informatica Giuridica, Corso di Specializzazione Universitario in Regulatory Compliance, Corso di Specializzazione Universitario in European Business Law, Corso di Perfezionamento Universitario in Criminalità Informatica e Investigazioni digitali, Consulente esperto qualificato nell'ambito del trattamento dei dati.

[1] Cfr. B. Belsey, *Cyberbulling: an emerging threat to the "always on" generation*, 2005, disponibile al link https://www.cyberbullying.ca/ (ultimo accesso in data 29/09/2023).

Successivamente, poi, furono delineate precisamente cinque diverse tipologie di condotte socialmente tipiche[2] e sette categorie di strumenti tipicamente utilizzati a tal fine[3], e cioè:

i) gli SMS;
ii) gli MMS;
iii) le telefonate moleste;
iv) le e-mail;
v) le *chat room*;
vi) i sistemi di messaggistica istantanea;
vii) i siti web.

Quanto alle condotte, invece, si è soliti parlare di *flaming* quando ci si trova dinanzi alla diffusione di messaggi elettronici caratterizzati da un tono aggressivo, violento, volgare e denigratorio, mirati a danneggiare un soggetto più vulnerabile. Questo comportamento è tipicamente breve e si verifica durante la presenza online delle persone coinvolte.

Si parla di *harassment*, invece, in presenza dell'invio di numerosi messaggi informatici dal contenuto volgare, aggressivo e minatorio da parte di uno o più soggetti e diretti verso un individuo specifico. Questo comportamento si distingue dal *flaming* in quanto il primo è contraddistinto dalla cosiddetta "asimmetria di potere" tra le parti (il cyberbullo o i cyberbulli da un lato, la vittima dall'altro), nonché dalla persistenza e dalla ripetitività nel tempo delle condotte aggressive, le cui azioni non dipendono dalla presenza online della vittima in un ambiente condiviso. A questa tipologia di comportamento si associa anche il cosiddetto *cyberstalking*, che si verifica quando il persecutore non accetta la decisione della vittima di porre fine a una relazione affettiva e intraprende azioni persistenti per contattare e molestare la vittima, anche attraverso canali informatici o telematici come telefonate, e-mail, messaggi, etc.

Si parla di *denigration*, invece, in presenza di comportamenti contraddistinti dalla diffusione informatica o telematica di notizie, fotogra-

[2] E cioè il *flaming*, l'*harassment*, la *denigration*, la *impersonation* e l'*outing and trickery*, così come individuate da N. E. Willard, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats and Distress*, Illinois, Research Press, 2007.

[3] Cfr. P.K. Smith, "Cyberbullying: its nature and impact in secondary school pupils", «Journal of Child Psychology and Psychiatry», vol. 49, 2008, pp. 376-385.

Minori e diritto all'oblio: la normativa sul cyberbullismo e il ruolo del Garante per la protezione dei dati personali

Dopo aver delineato in breve le caratteristiche tipiche del cyberbullismo, la sua definizione e il contesto normativo attualmente vigente, il contributo esamina il ruolo del Garante della protezione dei dati personali nella rimozione dei contenuti lesivi della dignità fisica e morale delle vittime, nell'ottica di quanto disposto dall'art. 2, comma 2, l. 71/2017 (c.d. legge sul cyberbullismo). Ma tale legge appare oggi come depotenziata, soprattutto a seguito dell'entrata in vigore del GDPR e della conseguente riforma del Codice Privacy.

Minors and the right to be forgotten: cyberbullying legislation and the role of the Italian Data Protection Authority

After briefly outlining the typical characteristics of cyberbullying, its definition, and the current regulatory framework, the paper examines the role of the Italian Data Protection Authority (Garante della protezione dei dati personali) in the removal of content that is harmful to the physical and moral dignity of victims, in line with the provisions of Article 2, paragraph 2, Law 71/2017 (the so-called cyberbullying law). However, this law now appears to be weakened, especially following the implementation of the General Data Protection Regulation (GDPR) and the subsequent reform of the Italian Privacy Code.

Il minore e i servizi della società dell'informazione

Ciberspazio e diritto, vol. 24, n. 75 (3 - 2023), pp. 275-290

Servizi della società dell'informazione: protezione dei dati dei minori e *accountability* dei genitori

Antonio Ciccia Messina[*]

SOMMARIO: 1. Il quadro normativo: l'articolo 8 del Regolamento generale sulla protezione dei dati (GDPR). – 2. Ambito di applicazione. – 3. La disciplina dei trattamenti di dati appartenenti a particolari categorie. – 4. La nozione di offerta diretta di servizi della società dell'informazione. – 5. La soglia di età nel GDPR e nel Codice Privacy. – 6. La verifica dell'età del minore. – 7. La doverosa *accountability* dei genitori. – 8. Il consenso per i minori di età inferiore alla soglia. – 9. La legge nazionale sui contratti.

1. *Il quadro normativo: l'articolo 8 del Regolamento generale sulla protezione dei dati (GDPR)*

L'articolo 8 del GDPR disciplina le condizioni applicabili al consenso dei minori di età in relazione ai servizi della società dell'informazione.

Il primo paragrafo dell'articolo 8 prevede che il trattamento di dati personali del minore di età, nel caso in cui si applichi l'articolo 6 GDPR, paragrafo 1, lettera a) e per quanto riguarda l'offerta diretta di servizi del-

[*] Saggista, Professore a contratto di "Tutela della privacy e trattamento dei dati Digitali" (Università della Valle d'Aosta), Data Protection trainer ed Esaminatore per la certificazione TUV "Privacy Officer e consulente della privacy (CDP)" e per la certificazione "DPO Profili Privacy UNI 11697:2017". Impegnato con passione nella divulgazione e nella diffusione della cultura della privacy, ha firmato numerosi *instant book*, oltre a 6.500 articoli per il quotidiano giuridico "ItaliaOggi" e per altre testate cartacee e on line. Ha pubblicato 45 libri, di cui 21 monografie in materia di privacy ed è autore di frammenti informativi su Linkedin (https://www.linkedin.com/in/antonio-ciccia-messina-7674011aa/). È Privacy Officer e Consulente Della Privacy Certificato Tüv Italia n. Cdp-211, nonché DPO - Responsabile Della Protezione Dei Dati Personali, Certificato Tüv, Schema PRV/ UNI 11697:2017 n° "PRV_035-DPO. Ha tenuto oltre 1.000 corsi di formazione ed ha esaminato per la certificazione delle competenze "privacy" oltre 50 DPO e Privacy Officer. È autore e speaker di un videocorso in materia di GDPR, di cui sono state distribuite oltre 15.000 licenze.

la società dell'informazione ai minori, sia lecito ove il minore abbia almeno 16 anni. Qualora il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. L'ultimo periodo del primo paragrafo autorizza gli Stati membri a stabilire per legge un'età inferiore, al fine della formulazione del consenso per i trattamenti dei dati considerati dall'articolo 8 medesimo, purché non inferiore ai 13 anni.

Il secondo paragrafo obbliga il Titolare del trattamento ad adoperarsi 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.

Il paragrafo 3 dichiara la salvezza delle disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

La corretta applicazione dell'articolo 8 presuppone una altrettanto corretta interpretazione, che si delinea qui di seguito alla stregua di un commentario dell'articolo 8 medesimo nelle sue proposizioni partitamente analizzate.

Si avverte che, se non diversamente indicato, gli articoli citati *infra* appartengono al 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, qui di seguito siglato "GDPR").

2. *Ambito di applicazione*

L'ambito di applicazione della norma citata è ristretto alla sola ed unica ipotesi esplicitamente descritta dall'*incipit* della disposizione: «Qualora si applichi l'articolo 6, paragrafo 1, lettera a) […]».

Il perimetro dell'ambito di applicazione è, dunque, quello contornato dall'articolo 6, paragrafo 1, lettera a), del quale qui si riporta lo stralcio che interessa: «Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità».

Servizi della società dell'informazione: protezione dei dati dei minori e accountability *dei genitori*

L'articolo 8 del GDPR, relativo alle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione, pone molti problemi interpretativi ed applicativi.
Da una rigorosa analisi letterale e sistematica della norma risulta che:

i) in relazione al trattamento di dati di minori di età, il Titolare del trattamento non può, a sua scelta, optare per la base giuridica del consenso quando ricorrono altre condizioni di liceità;

ii) nell'ambito di applicazione dell'articolo 8, paragrafo 1, del GDPR sono compresi i servizi della società dell'informazione che non sono elemento di un contratto, rispetto al quale il minore di età sia incapace di agire;

iii) ai fini dell'articolo 8 GDPR, il consenso del minore di età non è condizione di liceità del trattamento di dati personali appartenenti a particolari categorie riferiti al minore di età;

iv) chi offre un servizio della società dell'informazione è obbligato a dichiarare motivatamente se il servizio offerto è di natura contrattuale oppure non contrattuale e se i servizi sono diretti solo a maggiori di età, oppure solo a minori di età, oppure indistintamente a maggiorenni e minorenni;

v) le regole, parametrate al rischio, relative alle tecniche da usare per la verifica della minore età, servono a misurare la responsabilità del Titolare. Peraltro, se si appura *ex post* che il servizio è stato in concreto fruito da una persona di età inferiore a quella ammessa, il trattamento deve in ogni caso cessare;

vi) doveri e poteri assegnati dal Codice civile ai genitori (rappresentanza negli atti civili e adozione delle scelte relative alla istruzione ed educazione dei figli) si applicano anche a proposito delle decisioni relative alla fruizione dei servizi della società dell'informazione;

vii) una proattività, tipica degli istituti ispirati all'*accountability*, è senz'altro dovuta dai genitori anche in relazione alla gestione del consenso al trattamento dei dati dei minori relativo ai servizi della società dell'informazione.

Information society services: child data protection and parental accountability

With reference to the terms and conditions applicable to the consent stated by minors involved in information society services, article 8 of the GDPR presents many issues related to its exact meaning as well as to the consequent effective actions to be taken.
A strictly literal and systematic analysis of the regulation proves that:

i) to legitimize the data processing of minors, the data controller is non enabled, at its free choice, to opt for the legal ground of consent if other conditions of lawfulness must be followed;

ii) article 8 of the GDPR does not cover all information society services, but only the ones that cannot be included in a contract that the minor is not enabled to sign;

iii) in accordance with article 8 of the GDPR, the consent of the minor is not a legal ground for the processing of special categories of personal data referring to the minors;

iv) those who offer information society services are obliged to justifiably state whether the service offered is contractual based or non-contractual based and whether the services are directly offered only to adults or only to minors or without distinction to adults and minors;

v) the provisions, appropriated to the risk, relating to the tools to be implemented for the age verification of minors, are useful for assessing the responsibility of the controller. Moreover, if it is shown ex post that the service has actually been used by a person under the age of the allowed one, the processing must in any event cease;

vi) the Italian Civil Code's provisions about duties and powers conferred on parents (representation in civil acts and adoption of decisions relating to the education of children) also apply to decisions relating to the use of information society services;

vii) parents must act proactively also in the management of consent to the processing of children's data amid the provision of information society services.

Ciberspazio e diritto, vol. 24, n. 75 (3 - 2023), pp. 291-306

Un anno di SPID per il minore

Andrea Garilli, Marta Gaia Castellan*

Sommario: 1. Caratteri generali di SPID. – 2. Profili di responsabilità genitoriale. – 3. Elementi distintivi di un processo di richiesta di SPID per il minore. – 4. Gestione dei dati di contatto del minore. – 5. Evidenze relative allo *status* familiare e alla responsabilità genitoriale. – 6. Profili di trattamento dei dati personali del minore. – 7. Conclusioni.

1. *Caratteri generali di SPID*

SPID, il Sistema Pubblico di Identità Digitale, esiste in Italia da quasi dieci anni e il numero di identità erogate è di quasi 36 milioni.

Il suo utilizzo per l'accesso ai servizi in rete di enti pubblici ed organizzazioni private, già consolidato nel periodo pre-COVID, è diventato massivo a partire dal 2020. La scala temporale riportante il numero di utilizzi negli ultimi anni è riassumibile come segue:

i) nel 2019: oltre 55 milioni di volte;
ii) nel 2020: 143.872.687 volte;
iii) nel 2021: 571.238.162 volte;
iv) nel 2022: 1.036.223.617 volte;
v) nel mese di maggio 2023: 104.869.114 volte;
vi) nel mese di giugno 2023: 91.211.462 volte.

I dati relativi all'utilizzo di tale identità digitale sono in continua crescita non solo in termini di numerosità e di utilizzo, ma anche per tipologia. Esistono, infatti, diverse varianti' di SPID: per persona fisica ad uso

* *Trust Specialists* nell'area di *Business and Solutions Compliance* presso uno dei principali Gestori dell'Identità digitale SPID in Italia.

personale[1] e ad uso professionale[2], per persona giuridica[3], ad uso professionale della persona giuridica[4].

Cercando di fornire una definizione semplice ed universale, si può definire SPID come un set di credenziali (username, che coincide con l'indirizzo e-mail, e password) che rappresentano l'identità digitale di una persona fisica o giuridica (o allo stesso tempo entrambe in alcuni casi) e che viene utilizzata per accedere ai servizi online di pubbliche amministrazioni e privati[5] sia in Italia che in Unione europea.

È essenziale specificare che l'identità in questione è composta di una serie di informazioni e attributi, principalmente anagrafici e di contatto. Tali informazioni sono raccolte e verificate dal Gestore dell'Identità[6] (anche "Gestore", o "Identity Provider") al momento della richiesta dell'identità SPID, e vengono confermate da questo ogniqualvolta l'utente titolare delle proprie credenziali si autentichi per accedere ad un servizio online, trasmettendo al Gestore i dati necessari all'autenticazione. Tale modalità – esplicata in maniera necessariamente generica – consente al *Service Provider* di verificare univocamente l'identità del soggetto che richiede l'autenticazione ad un servizio.

L'introduzione di cui sopra può essere chiarita attraverso un esempio: se un utente accede alla propria area riservata nel sito dell'Agenzia delle Entrate con le proprie credenziali SPID, al momento dell'inserimento

[1] Si tratta della tipologia di SPID utilizzata dal privato cittadino, per l'accesso ai servizi online delle Pubbliche Amministrazioni e delle organizzazioni di diritto privato.

[2] Destinato a lavoratori dipendenti e/o professionisti per l'accesso a servizi online specifici, per esempio dipendenti di una società o professionisti appartenenti a un Ordine specifico.

[3] Particolare tipologia di SPID riportante, tra gli attributi identificativi, le sole informazioni della persona giuridica. Si tratta di un'identità digitale richiesta dai rappresentanti legali di un'organizzazione, o da persona dotata dei necessari poteri.

[4] Differente dallo SPID per persona giuridica "semplice", in quanto gli attributi dell'utenza SPID, in questo caso, comprendono sia le informazioni relative alla persona fisica appartenente all'organizzazione, sia quelle dell'organizzazione stessa.

[5] Se e quando previsto dal servizio in questione. I "Service Provider SPID" necessitano di finalizzare apposito accreditamento presso l'AgID (Agenzia per l'Italia Digitale) per poter fornire i propri servizi mediante autenticazione SPID.

[6] Al momento della pubblicazione del presente articolo, a titolo esemplificativo e non esaustivo, tra i principali Gestori di Identità si possono menzionare Poste Italiane, Aruba, InfoCert, Namirial, Sielte, Lepida.

Un anno di SPID per il minore

SPID, il Sistema Pubblico di Identità Digitale, ha da poco incluso in via sperimentale i minorenni, dando loro la possibilità di avere una propria identità digitale e di fruire di servizi online a loro dedicati.
Sono previste due fasce d'età, con delle differenze: dai 5 anni ai 14 anni e dai 14 anni ai 18 anni.
AgID, Agenzia per l'Italia Digitale, ha pubblicato le "Linee Guida operative per la fruizione dei servizi SPID da parte dei minori".
La particolarità più importante è che l'identità del minore è legata all'identità del genitore, sia nella fase di richiesta, riconoscimento e rilascio, che nella fase di utilizzo, che può avvenire solo su autorizzazione del genitore.
L'adesione è facoltativa e il suo successo dipenderà dai servizi che verranno offerti (ad esempio, i servizi scolastici).

SPID for underage users

SPID, the Italian Public Digital Identity System, has recently included underage users on an experimental basis, giving them the opportunity to obtain and manage their own digital identity and for accessing online services designed for them. There are two age groups involved, with some differences: from 5 to 14 years old and from 14 to 18 years old.
AgID, the Agency for Digital Italy, has published the "Operational Guidelines for the Use of SPID Services by underage Users".
The most important feature is that the underage user's identity is linked to parent's identity, in request, recognition and issuance phases, as well as in the usage phase, with parental authorization.
Participation is optional and its success will depend on the services offered (e.g., school services).

Ciberspazio e diritto, vol. 24, n. 75 (3 - 2023), pp. 307-322

Sistemi di *age verification*. Una prima esplorazione fra salvaguardia dell'interesse prioritario del minore e protezione dei dati personali

Michele Martoni*

Sommario: 1. Identificazione e verifica dell'età. Un chiarimento e la normativa sul trattamento dei dati personali. – 2. Come le piattaforme verificano l'età. Alcuni esempi. – 3. Alla ricerca di sistemi appropriati e proporzionati. – 4. SpID per i minori e l'eID Wallet. – 5. Brevi note conclusive.

1. *Identificazione e verifica dell'età. Un chiarimento e la normativa sul trattamento dei dati personali*

Chi scrive ha da tempo concentrato le ricerche sull'impatto che l'abitare gli spazi digitali, per come sono concepiti, codificati e disegnati, può produrre sui "non adulti" (per semplicità, ci si riferirà ad essi utilizzando il termine "minori"). Questo contributo si propone di avviare una prima esplorazione sui sistemi di identificazione e verifica dell'età nell'ambiente digitale, soffermandosi sulle questioni giuridiche legate alla protezione dei dati personali che dovrebbero orientarne la progettazione. Si propo-

* Ricercatore a tempo determinato di tipo "B" di Informatica giuridica al Dipartimento di Giurisprudenza dell'Università degli Studi di Urbino. Insegna Informatica giuridica e Cyber Security nel medesimo Ateneo. Abilitato al ruolo di Professore di seconda fascia. Responsabile e docente del modulo in tema di diritti dell'interessato del Master in Trattamento dei dati personali e Data Protection Officer, Università di Bologna. Nel medesimo Ateneo insegna nel Master in Diritto delle nuove tecnologie e nel Corso di Alta Formazione in Data Protection e Privacy Officer. Membro della Società Italiana di Filosofia del Diritto, della Italian Society for Law and Literature (ISLL), della Associazione di studi su Diritto e Società. Membro della redazione e revisore in diverse riviste scientifiche anche di fascia A. Avvocato del Foro di Bologna iscritto nell'elenco speciale dei docenti e ricercatori. Autore di diverse pubblicazioni scientifiche, è, fra le altre iniziative, anche referente del progetto "Insieme nella Rete" realizzato dalle scuole di ogni ordine e grado del circondario imolese, avente ad oggetto l'educazione alla cittadinanza elettronica.

ne, inoltre, di ripercorrere, seppur a volo d'angelo, alcune iniziative europee in atto.

Ogni piattaforma digitale che offre contenuti e servizi accessibili a minori dovrebbe considerare se, per tali contenuti e per il tipo di servizio fornito, sia necessario conoscere l'identità dell'utente o sia sufficiente limitarsi a verificarne l'età.

Si pone, allora, il quesito se ed in che misura occorra svolgere una verifica al momento dell'accesso e, successivamente, chi dovrebbe svolgerla.

Pare, quindi, rilevante valutare cosa sia necessario conoscere: ad esempio, che un certo individuo supera una determinata età ("ha più di *tot* anni"); che ha una certa età ("ha *tot* anni" o, ancora più nel dettaglio, "è nato in data *x*"); quale sia la sua identità personale anagrafica.

Al di là della complessità tecnica di queste operazioni e della difficoltà applicativa collegata al carattere transfrontaliero delle piattaforme e alla coesistenza di utenti di diverse nazionalità, l'accertamento dell'identità e la verifica dell'età implicano certamente una o più operazioni di trattamento di dati personali ai sensi dell'art. 4 del Regolamento UE n. 679/2016 (c.d. GDPR).

Come noto, ogni operazione di trattamento, ivi comprese quelle in argomento, devono rispettare i principi generali di cui all'art. 5 del GDPR e, più nello specifico, per quanto qui ci occupa, il principio di minimizzazione. Ne consegue che i dati personali oggetto di trattamento devono essere limitati a quanto necessario rispetto alle finalità per le quali sono raccolti e dovrebbero essere trattati solo quando la finalità del trattamento non sia ragionevolmente conseguibile con altri mezzi.

Già con il decreto legislativo n. 196/2003 (c.d. Codice Privacy), il trattamento dei dati personali doveva svolgersi nel rispetto del principio di necessità codificato all'art. 3 il quale disponeva che i «sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità».

Occorre dunque chiedersi preliminarmente quale sia la finalità del trattamento che seguirebbe l'identificazione e/o la verifica dell'età per poi definire quale sia il dato "minimo" e "necessario".

Sistemi di age verification. *Una prima esplorazione fra salvaguardia dell'interesse prioritario del minore e protezione dei dati personali*

Il contributo approfondisce il tema dei sistemi di *age verification* nell'ambiente digitale, affrontando, in particolare, le questioni legate alla protezione dei dati personali. La verifica dell'età implica, infatti, il trattamento di dati personali, che deve essere effettuato in conformità con il Regolamento UE n. 679/2016 (GDPR) e, fra gli altri, nel rispetto del principio di minimizzazione dei dati. Alla luce di alcuni esempi di come le piattaforme gestiscono la fase di verifica dell'età, si pone l'attenzione sulla protezione dei minori e sulla necessità di sistemi di *age verification* adeguati e proporzionati, che rispettino i diritti e le libertà dei minori. Vengono, quindi, ripercorse alcune iniziative istituzionali di diversi Paesi europei; fra queste, più nello specifico, vengono riprese le Linee Guida operative dell'AgID per l'utilizzo dei servizi SPID da parte dei minori. Viene, inoltre, introdotta la proposta di "European digital identity wallet" (*eID Wallet*). Nelle conclusioni, emerge la necessità di un equilibrio tra sicurezza del minore e protezione dei diritti e libertà individuali nel contesto dei sistemi di *age verification* negli ambienti digitali.

Age verification systems. An initial exploration between safeguarding the best interests of the child and protecting personal data

The paper explores the topic of age verification systems in the digital environment, addressing, in particular, data protection issues. Age verification implies, in fact, the processing of personal data, which must be carried out in accordance with EU Regulation No. 679/2016 (GDPR) and, among others, in compliance with the principle of data minimisation. In light of some examples of how platforms handle the age verification phase, attention is drawn to the protection of minors and the need for adequate and proportionate age verification systems that respect the rights and freedoms of minors. Some institutional initiatives of several European countries are then reviewed; among these, more specifically, the AgID operational guidelines for the use of SPID services by minors are taken up. The proposal for a "European digital identity wallet" (eID Wallet) is also introduced. The conclusions highlight the need for a balance between child safety and the protection of individual rights and freedoms in the context of age verification systems in digital environments.

Le nuove frontiere di interazione virtuale

Ciberspazio e diritto, vol. 24, n. 75 (3 - 2023), pp. 325-338

I minori online tra videogiochi e metaverso

Giovanni Ziccardi*

Sommario: 1. Lo studio di UNICRI. – 2. L'approccio del Governo statunitense. – 3. Il nuovo rapporto tra minori e videogiochi. – 4. Alcuni suggerimenti per i genitori. – 5. Il ritardo delle aziende e delle piattaforme. – 6. Le minacce più comuni. – 7. Individuare i fattori di rischio.

1. *Lo studio di UNICRI*

Nel 2022 UNICRI, istituto di ricerca delle Nazioni Unite, ha reso pubblico uno studio[1] volto ad analizzare i rischi che legano minori, ambiente dei videogiochi ("gaming") e comportamenti criminali nel metaverso.

Dal contenuto del rapporto, appare evidente come il tema dei crimini aventi a oggetto le frodi, l'aggressione, lo sfruttamento e l'abuso sessuale di minori online sia un fenomeno in aumento da quando le piattaforme digitali sono entrate a far parte sempre più intensamente della vita quotidiana dei bambini e dei ragazzi. Allo stesso tempo, un uso accorto e creativo della tecnologia si può rivelare estremamente utile per mitigare alcuni dei rischi che si andranno a breve a evidenziare[2].

Sono quattro, in particolare, i fattori di criticità evidenziati nella sintesi iniziale dello studio:

* Professore di Informatica giuridica presso l'Università degli Studi di Milano. Già Jean Monnet Professor of EU Data Governance, Cybersecurity and Digital Fundamental Rights. Componente del Comitato Sicurezza ICT e del Comitato Etico di Ateneo. Coordinatore del Centro di Ricerca in Information Society Law (ISLC). Coordinatore dei Corsi di Perfezionamento in "Coding for Lawyers & Legal Tech" e "Criminalità Informatica e Investigazioni Digitali".

[1] Lo studio di UNICRI, intitolato *Gaming and the Metaverse* e pubblicato nel mese di novembre del 2022, è disponibile in Internet all'indirizzo https://unicri.it/Publication/Gaming-and-the%20Metaverse.

[2] Cfr. rapporto UNICRI, cit., p. 4.

i) un aumento di forme di cyberbullismo che avvengono anche sulle piattaforme di videogiochi e che coinvolgono, ormai, ben la metà degli adolescenti online;
ii) un aumento dei casi di adescamento di minori a fini sessuali, comportamento criminale che ha registrato, purtroppo, un picco storico nel 2021 a causa della pandemia;
iii) un incremento nella circolazione online di materiale legato all'abuso sessuale di minori, e
iv) un aumento di segnalazioni pervenute alle Forze dell'ordine e ai servizi di assistenza delle piattaforme con riferimento a tali reati o ad altri comportamenti illeciti[3].

2. *L'approccio del Governo statunitense*

Sul sito governativo federale *stopbullying.gov*, gestito con finalità informative dal Dipartimento della Salute degli Stati Uniti d'America, una sezione specifica è dedicata alla prevenzione del bullismo nei videogiochi e, soprattutto, a elaborare una descrizione accurata – e sempre aggiornata – dei principali rischi legati al gioco online.

In particolare, sono stati da tempo individuati i seguenti cinque punti critici.

i) Bilanciamento di aspetti positivi vs. aspetti negativi. Sebbene il *gaming* vanti un grande potenziale positivo, è anche un ambiente nel quale si possono verificare episodi di cyberbullismo.
ii) Un fiorire di comportamenti aggressivi. Se qualche bambino o ragazzo non si comporta correttamente durante il gioco, gli altri giocatori possono iniziare a offenderlo o a fare commenti negativi che possono immediatamente trasformarsi in atti di bullismo o, addirittura, arrivare a far escludere la persona dal gioco (e, quindi, dal gruppo).
iii) Effetti disinibitori legati all'anonimato. L'anonimato dei giocatori, e l'uso degli *avatar*, consentono agli utenti di creare *alter ego* o versioni fittizie di sé stessi, il che fa parte del divertimento alla base del gioco.

[3] Cfr. rapporto UNICRI, cit., p. 6.

I minori online tra videogiochi e metaverso

La diffusione del *gaming* online, soprattutto tra i soggetti di minore età, ha condotto alla nascita di nuove modalità di gioco, in cui l'utente non si ritrova più semplicemente a interagire con il proprio dispositivo ma, al contrario, si interfaccia con una vasta platea di giocatori con cui instaura vere e proprie interazioni sociali. Questo ha, inevitabilmente, portato con sé nuove possibilità criminali, idonee a mettere in pericolo le attività dei minori stessi. Il presente articolo si propone di ripercorrere le peculiarità del nuovo rapporto tra giovani e videogiochi, evidenziandone i fattori di rischio principali e valutando i possibili piani di intervento.

Children online: videogames and the metaverse

The spread of online gaming, especially among underage individuals, has led to the emergence of new modes of gaming, in which the user no longer simply interacts with his own device but, on the contrary, interfaces with a vast audience of players with whom he establishes real social interactions. This has, inevitably, brought with it new criminal possibilities, suitable for endangering the activities of minors themselves. This article aims to go over the peculiarities of the new relationship between young people and videogames, highlighting its main risk factors and evaluating possible intervention plans.