Dipartimento di Scienze Politiche

Diritto di Internet: social media e discriminazione

I MINORI E I *SOCIAL NETWORK*: IL CONFINE TRA DIVERTIMENTO E PERICOLO

Relatore:
Prof. Pietro Santo Leopoldo Falletta

Candidata:
Beatrice Marra
Matr. 089252

Anno accademico 2020/2021

Alla mia famiglia

INDICE

Introduzione

Il rapporto dei minori con i *social network* nel corso del tempo si è trasformato.
Quello che costituiva un approccio come divertimento è diventato un accostarsi ai *social* senza rete di protezione, dovuto al fatto di dover scansare sempre più frequentemente le insidie e i pericoli derivanti da un uso improprio e illecito delle piattaforme digitali.
I pericoli per i fanciulli derivanti dal web provengono sia da adulti che da altri minori.
Nel primo capitolo si esaminano le principali forme di violenza online che mettono in pericolo la sicurezza del minore, con alcune definizioni e casi conosciuti di *cyberbullismo* e le sue declinazioni. Si descrivono, inoltre, il *childgrooming* e le *challenge* online.
Nel secondo capitolo si prende in esame in maniera più approfondita il fenomeno delle *challenge* o sfide online, con particolare attenzione alla *Blue Whale Challenge (la balena blu)* e alla *Blackout Challenge*, protagoniste delle recenti pagine di cronaca. L'obiettivo è di dimostrare come un uso dei *social network* poco regolamentato da parte dei ragazzi possa essere terreno fertile di insidie e di attività criminali. A tal proposito, si analizza il sondaggio effettuato tra marzo e aprile 2021 nel Progetto universitario "Diritto di Internet: social media e discriminazione".
Infine, il terzo capitolo si sofferma sull'analisi normativa e giuridica della tutela e della protezione del minore online e sulle attività di prevenzione per contrastare i rischi derivanti dal web. Un contributo prezioso è stato fornito dalla dott.ssa Nunzia Ciardi, Direttrice della Polizia postale e delle comunicazioni.

Capitolo 1
I minori e i rischi sul web

1.1. I nativi digitali e i rischi a cui vanno incontro

Il "nativo digitale"[1] si rapporta intuitivamente alle nuove tecnologie.

La locuzione, introdotta da Marc Prensky[2] nel 2001, indica i nati nell'era digitale e li distingue dagli "immigrati digitali", cioè da coloro nati prima delle tecnologie e che le hanno adottate in un secondo momento.

Riscontriamo una differenza formativa tra minori e adulti, dovuta agli strumenti di apprendimento: i minori acquisiscono conoscenze attraverso l'utilizzo prevalente delle nuove tecnologie, gli adulti si sono formati soprattutto sui libri.

Il minore di oggi è un nativo digitale.

La caratteristica principale consiste nel rapporto degli adolescenti con i *social media*: si connettono nell'arco dell'intera giornata.

I *social media* più diffusi e utilizzati con computer, *smartphone* e tablet sono TikTok, Instagram, Snapchat, Facebook. In questi spazi digitali, che diventano essi stessi luogo di condivisione di idee, di immagini, di video e di commenti, si svolge la vita sociale non solo dei ragazzi ma anche degli adulti.

Il fenomeno si è accentuato ancora di più con l'isolamento e il *lockdown* dovuti alla pandemia da Covid-19 a partire dal 2020.

A ciò ha contribuito l'utilizzo forzato della DAD, la didattica a distanza, che ha moltiplicato le ore trascorse davanti ai *device*.

Interessanti sono i risultati, ancora validi, delle indagini contenute nel "Libro Bianco *Media* e Minori 2.0" del 2018 redatto dall'Agcom, l'Autorità per le garanzie nelle comunicazioni:

1. più di un terzo dei minori di età tra i 9 e i 12 anni ha un profilo personale su un *social network*
2. più di un terzo dei minori di età tra i 12 e i 18 anni conosce qualcuno che non ha l'età anagrafica per poter navigare all'interno dei *social*[3].

[1] Agcom, *Libro Bianco Media e Minori 2.0*, 2018.

[2] Marc Prensky è uno scrittore statunitense, consulente e innovatore nel campo dell'educazione e dell'apprendimento. È l'inventore dei due termini nativo digitale e immigrato digitale. Entrambe le locuzioni sono state descritte per la prima volta in un articolo del 2001 su "*On the Horizon*".

[3] V. Nota 1.

Da tale indagine si può desumere che spesso i minori mentono sulla loro età anagrafica quando si iscrivono ai *social network*.

Ogni piattaforma *social* prevede un'età minima per l'iscrizione. Il punto di riferimento generale è la legge federale degli Stati Uniti *Chidren's Online Privacy Protection* (COPPA) in vigore dal 2000, che raccoglie online informazioni personali su minori di età inferiore ai 13 anni. La legge descrive cosa deve inserire un operatore di un sito web sulla *privacy*, quando e come chiedere il consenso di un genitore e quali sono le responsabilità del web di proteggere la *privacy* e la sicurezza dei minori online e le informazioni personali sui minori di età inferiore 13 anni[4].

Secondo i dati Istat, nel 2019 ben l'87,3% dei minori di età compresa tra gli undici e i diciassette anni ha utilizzato quotidianamente il cellulare, e tre ragazzi su quattro, in quella stessa fascia di età, navigano su Internet tutti i giorni. Quest'ultima quota è cresciuta molto rapidamente: è passata infatti dal 56,2% al 75,0% in soli quattro anni, dal 2016 al 2019[5]. L'utilizzo di Internet è quindi per i nativi digitali non solo parte imprescindibile della loro vita quotidiana e della loro socialità, ma determina anche la loro crescita e la loro istruzione.

All'interno di questo mondo virtuale dove il minore esercita sempre più frequentemente e assiduamente le proprie attività, esiste il rischio concreto che possa rimanere vittima di crimini e pericoli presenti nel web.

Se Internet offre numerose potenzialità, come ad esempio la facilità della ricerca e della connessione con il mondo esterno, contiene tuttavia molteplici insidie, specialmente per i più piccoli, che sono i soggetti più vulnerabili e con meno strumenti di autotutela.

Tale fenomeno è sempre più attuale e in continuo aumento: i dati forniti dalla Polizia postale in occasione del *Safer Internet Day*[6] attestano che nel 2020 si è registrato un aumento del 77% rispetto all'anno precedente di vittimizzazione dei minori. I reati maggiori sono configurati nella pedopornografia online, nel *childgrooming*, nel *cyberbullismo*, nel furto di identità digitale[7].

Alcuni di questi fenomeni sono nati nel mondo reale ma trovano nel mondo virtuale un nuovo spazio dove manifestarsi. Infatti il bullismo, nato nel mondo reale, in Internet ha preso il nome

---

[4] Astone Antonina, *I dati personali dei minori in rete. Dall'internet delle cose all'internet delle persone*, Milano, 2019, p.26.

[5] Istat, *Indagine conoscitiva sulle forme di violenza fra i minori e ai danni di bambini e adolescenti*, Commissione parlamentare per l'infanzia e l'adolescenza, Roma, 1° giugno 2020, p.11.

[6] Cfr *infra* Capitolo 3.

[7] Agi <https://www.agi.it/cronaca/news/2021-02-09/minori-aumentano-vittime-reati-online-11332868/> [ultimo accesso 10 aprile 2021].

di *cyberbullismo*, la pedopornografia è connessa al drammatico fenomeno del *childgrooming* online e le sfide tra ragazzi quali le gare folli con i motorini o le prove di forza per appartenere a un gruppo si sono trasformate in *challenge*, drammatiche sfide online che coinvolgono soprattutto i bambini e gli adolescenti.

Da questa nuova e inquietante realtà virtuale emergono soprattutto le seguenti caratteristiche:

1. il minore che naviga in Internet spesso non è a conoscenza dei pericoli a cui può andare incontro;
2. questi crimini avvengono con molta facilità, soprattutto grazie alla presenza dell'anonimato in alcune piattaforme online e alla possibilità di creare una falsa identità (c.d. *"account fake"*). È attraverso questi *escamotage* che i minori pensano di essere invisibili e si trasformano in "leoni da tastiera";
3. l'importanza di fornire un'educazione digitale sia per le persone più adulte che per i più piccoli per colmare il *bug* educativo dovuto ai *social*. I minori spesso non hanno la percezione del pericolo e non si rendono conto che ciò che pubblicano oggi potrebbe avere serie ripercussioni in futuro**.**

1.2 Il *cyberbullismo*

Il *cyberbullismo* viene definito giuridicamente la prima volta in Italia dalla legge n. 71/2017: *"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, tratta*mento *illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo"*[8].

Ne deriva che il *cyberbullismo* è la forma online del bullismo. Per bullismo si indicano, generalmente, le prepotenze perpetrate da bambini e ragazzi nei confronti di uno o più coetanei[9]. Il termine bullismo deriva dalla parola inglese *bullying* (*to bull*) che significa "*usare prepotenza, maltrattare, intimidire, intimorire*"[10].

[8] Legge n. 71 del 28 maggio 2017 entrata in vigore il 18 giugno 2017.

[9] Cfr. Vocabolario online Treccani, secondo cui per bullismo si intende un "*atteggiamento di sopraffazione sui più deboli, con riferimento a violenze fisiche e psicologiche attuate spec. in ambienti scolastici o giovanili*". Treccani <*http://www.treccani.it/vocabolario/bullismo/> [ultimo accesso: 10 aprile 2021].*

[10] "Smonta il bullo", definizione: <https://www.icdemarchi.edu.it/newsite/smonta-il-bullo/#:~:text=Il%20termine%20bullismo%20deriva%20dalla,confronti%20di%20un%20altro%20individuo>.

Il bullismo è quindi una forma di oppressione fisica o psicologica messa in atto da una o più persone (bulli) nei confronti di un altro individuo percepito come più debole (vittima); viene perpetrato principalmente all'interno del contesto scolastico; si diffonde come una relazione tra tre soggetti: il bullo, la vittima e gli spettatori.

Il *cyberbullismo* è anche una forma indiretta del bullismo: il bullo non si trova davanti alla vittima, ma dietro uno schermo, spesso sotto falsa identità e con un *nickname*.

L'aggressore pensa di essere invisibile perché non c'è il contatto visivo diretto e si nasconde dentro al web: pensa di non essere individuato, i suoi freni inibitori svaniscono e quindi diventa irresponsabile.

Il contesto in cui avviene il *cyberbullismo* è diverso da quello del bullismo del mondo reale. I nativi digitali crescono in una società sempre connessa, dove i *social* sono la quotidianità indipendentemente dal contesto sociale di provenienza. Il bullismo del mondo reale si sviluppa invece all'interno di un gruppo sociale, soprattutto il gruppo classe, in cui agiscono bulli, vittime e spettatori riconoscibili e individuabili.

Il *cyberbullismo* può avvenire attraverso messaggi o pubblicazioni di elementi multimediali in rete che hanno lo scopo di colpire le fragilità della vittima. L'attacco online comporta una diminuzione della difesa del minore, spesso esposto a minacce e senza una possibilità di fuga. Le comunicazioni aggressive possono avvenire in ogni momento e il materiale utilizzato dagli aggressori può essere diffuso in tutto il mondo. Le azioni di bullismo, invece, avvengono prevalentemente durante l'orario scolastico o nel percorso scuola-casa.

I dati Istat evidenziano che il *cyberbullismo* ha colpito il 22,2% di tutte le vittime del bullismo[11]. Spesso le vittime si nascondono e non denunciano i casi di *cyberbullismo* per il senso di vergogna e la paura di una punizione da parte dei genitori che potrebbero vietare l'utilizzo dei loro dispositivi[12].

Un interessante studio distingue il *cyberbullismo* tra improprio e proprio[13]. Il primo avviene nel mondo reale ma poi viene divulgato sui *social* o comunque nell'online. Un esempio è la ripresa con lo *smartphone* di un episodio di bullismo e pubblicato sui *social*. Il *cyberbullismo* proprio nasce all'interno del mondo online e può assumere diverse manifestazioni.[14]

Nel mondo esistono molti casi emblematici di minori vittime di *cyberbullismo* proprio.

---

[11] V. Nota 5.

[12] V. Nota 1.

[13] De Salvatore Ferruccio, *Bullismo e cyberbulling, dal reale al virtuale tra media e new media*, in *Minorigiustizia*, n.4, 2012, p.97.

[14] Cfr *infra* paragrafo 1.2.1: le diverse forme di *cyberbullismo.*

Uno dei casi che ha fatto maggior scalpore e ha avuto una notevole eco mediatica è quello di Amanda Michelle, un'adolescente americana di 15 anni rimasta vittima di *cyberbullismo* con l'esito peggiore: il suicidio, avvenuto il 12 ottobre 2012. Prima di togliersi la vita Amanda ha caricato un video sulla piattaforma YouTube dal titolo "*My story: Struggling, bullying, suicide and self harm*"[15] ("La mia storia: lotta, bullismo, suicidio e autolesionismo"), nel quale mostrando una serie di bigliettini racconta la sua triste esperienza di vittima di *stalking* e delle sue conseguenze. Il video è diventato immediatamente virale e ha attirato le attenzioni dei media in tutto il mondo. Al 12 aprile 2021 si attestavano 14.343.409 visualizzazioni.

Un altro episodio riportato dalla maggior parte delle testate giornalistiche è quello di una ragazza quattordicenne di Padova spinta a suicidarsi per le offese sul suo aspetto fisico ricevute sul *social network* Ask.fm nel febbraio 2014[16].

La piattaforma virtuale "Ask.fm", anche conosciuta come "Ask for me" o semplicemente come Ask, è stata creata in Lettonia nel 2010 e si basa su domande e risposte. La peculiarità di questo *social* è che le domande si possono fare in modalità anonima, senza quindi risalire all'identità, con la conseguenza della crescita di episodi di *cyberbullismo*. Con Ask erano già avvenuti in tutto il mondo episodi analoghi a quello di Padova, per cui la stessa piattaforma *social* è stata accusata di essere corresponsabile, insieme con i *cyberbulli*, di istigazione a togliersi la vita di molti adolescenti.

Dopo il suicidio di una quattordicenne britannica avvenuto il 2 agosto 2013, l'allora primo ministro David Cameron condannò il sito; chiese ai genitori e ai ragazzi di boicottarlo definendolo "*hateful*" e "*vile*"[17]. In un primo momento i fondatori di Ask.fm dichiararono che alcuni dei messaggi contenenti odio e insulti erano stati inviati dalla ragazza stessa, in seguito decisero di collaborare con la giustizia.

La piattaforma Ask nel tempo è stata abbandonata.

Attualmente siti analoghi a Ask.fm coinvolgono minori, quale ad esempio la piattaforma "*ThisCrush*". Ask ha coinvolto gli adolescenti nel 2013-2014, *ThisCrush* è nato nel 2018 e consente di inviare messaggi alla persona interessata in forma anonima. Anche se *ThisCrush* è nato con l'intento di contattare la persona che piace - da qui il nome "*crush*" ovvero "cotta" nel gergo adolescenziale - molte volte è stato utilizzato per forme di *hate speech.*

[15] Youtube, <https://www.youtube.com/watch?v=vOHXGNx-E7E>.

[16] Il messaggero, https://www.ilmessaggero.it/primopiano/cronaca/suicida_14_anni_ask_fm_bullismo-293475.html [ultimo accesso: 12 aprile 2021].

[17] The Guardian, <https://www.theguardian.com/society/video/2013/aug/08/boycott-websites-david-cameron-video> [ultimo accesso: 13 aprile 2021].

Infatti la possibilità di inviare domande in forma anonima, come in Ask.fm o in *ThisCrush*, conferma il fatto che i ragazzi si sentano legittimati a essere aggressivi e violenti.
Un'ulteriore conferma proviene dal fatto che i minori spesso hanno un comportamento superficiale nel pubblicare i fatti della propria vita sui *social*, prestando il fianco ai *cyberbulli* in agguato: gli adolescenti non si rendono conto delle conseguenze che una pubblicazione su un *social* può avere sul loro futuro.
Del resto, come ha affermato la dott.ssa Nunzia Ciardi, Direttrice della Polizia Postale e delle comunicazioni: "*per i giovani è molto difficile ragionare in termini di proiezione nel tempo e nello spazio*"[18].

1.2.1 Le diverse forme di *cyberbullismo*

Esistono diverse forme di *cyberbullismo*, che a seconda delle sue manifestazioni può essere suddiviso nelle seguenti sottocategorie[19]:

1. *Flaming*: invio di messaggi e insulti dal contenuto aggressivo mirati a scatenare battaglie di odio online[20].

   Il fenomeno riguarda spesso attività di messaggistica online e videogiochi interattivi: spesso i principianti sono presi di mira con aggressioni e attacchi nella *chat* del gioco per la loro inesperienza o errori commessi[21].

   Il *gaming* può avere risvolti positivi per gli adolescenti perché stimola la creatività, aumenta la loro soglia di attenzione e di concentrazione, facilita le capacità di *problem solving* e rappresenta un momento di svago. Tuttavia, come tutte le potenzialità del web, se non controllato e regolamentato può rivelarsi pericoloso per i minori.

   Inoltre un utilizzo eccessivo dei videogiochi può portare alla perdita delle relazioni sociali dal vivo.

   Un esempio è dato dalla sindrome *hikikomori*, sempre più diffusa tra i ragazzi, che si traduce in isolamento e ritiro sociale e, di conseguenza, in una vita sedentaria.

   La sindrome, nata in Giappone, è spesso la conseguenza del fenomeno del bullismo e del *cyberbullismo*. I ragazzi che decidono di isolarsi raccontano di storie di abusi e

[18] Intervista alla dott.ssa Nunzia Ciardi, v. capitolo 3.
[19] Altalex, <https://www.altalex.com/guide/cyberbullismo> [ultimo accesso: 13 aprile 2021].
[20] Nota 1.
[21] Cyberbullismo.com, http://www.cyberbullismo.com/cyberbullismo/tipologie/#:~:text=FLAMING%20%E2%80%93%20Con%20tale%20termine%20si,bullismo)%20per%20una%20durata%20temporale>[ultimo accesso 13 aprile 2021].

scherzi provenienti dalla scuola, di offese ricevute dai compagni scolastici che portano al rifiuto del sistema scolastico nel suo complesso. Scelgono di ritirarsi all'interno della loro camera e diventano sempre più ostili nel socializzare con il mondo esterno; il solo mezzo di contatto con la vita reale per loro è Internet.

Internet e gli strumenti elettronici diventano una dipendenza e portano all'isolamento quando il web viene percepito dai ragazzi come un metodo per sostituire il contatto con le persone nella vita reale. In questo senso quindi la rete rappresenta più una conseguenza che la causa dell'isolamento, e rende più difficile e complesso il percorso di reintroduzione del bambino nel mondo sociale[22].

2. *Harassment*: invio di messaggi ripetuti di contenuto aggressivo e minatorio da parte di uno o più utenti nei confronti di un unico *account*.

   A questo tipo di attività viene spesso correlato il fenomeno del *cyber-stalking*: di fronte a un rifiuto amoroso lo *stalker* molesta e minaccia la persona che ha rifiutato il rapporto. In alcuni casi, il *cyberbullo* anziché agire da solo cerca di coinvolgere altri utenti nella condotta illecita, da qui il nome "*harrasment con reclutamento volontario*".[23]

3. *Denigration*: propaganda e diffusione offensiva di contenuti come audio, fotografie o video della vittima per danneggiare la sua reputazione.

   Il denigratore spesso altera e modifica i contenuti multimediali e li diffonde con lo scopo di denigrare la persona e ledere la sua immagine. In questo caso la *denigration* assume le forme del *deepnude* e *deepfake*.

   La differenza con il *cyber-stalking* è che l'azione illecita può essere una sola, come la diffusione di una foto online, che può essere ripresa da altri utenti e divulgata sui *social network*.

4. *Impersonation*: accesso di un soggetto a uno o più *account* della vittima e con la divulgazione di materiali, ad esempio *chat* private, per metterla in pericolo o crearle dei problemi.

   Spesso il *cyberbullo* si procura le credenziali di un account per rubare l'identità online di una persona, inviare foto e video, scambiare messaggi con altri utenti.

5. *Outing and Trickery*: fa *outing* chi ha ricevuto materiali privati o confidenze della vittima e li divulga senza il suo consenso.

[22] Rivista di Scienze Sociale, Infanzia e Adolescenza tra socialità e solitudine, 2020.
[23] v. Nota 20.

Trickery è l'attività in cui il *cyberbullo* inganna l'altra persona: la sollecita a inviargli contenuti privati confidenziali e li diffonde senza la sua autorizzazione.

1.3 Il *Cybergrooming*

Il *cybergrooming* o c*hild grooming*, è l'adescamento online di soggetti minori da parte degli adulti nell'intento di compiere atti sessuali.
L'adescatore utilizza i numerosi strumenti di Internet: *chat* online, forum di discussione, *social network*, dove spesso si spaccia per adolescente per rendere più facile la lusinga.
Il *grooming* consiste in una "*tecnica psicologica*"[24] da parte dell'abusante nei confronti del minore: il termine inglese *groom* deriva dal verbo "*to groom*", che significa accudire e prendersi cura di una persona psicologicamente e fisicamente per uno scopo illecito.
Anna Salter[25] descrive il *grooming* come una tattica psicologica dell'abusante esercitata nei confronti del minore al fine di soddisfare le proprie tentazioni sessuali e per un rapporto non occasionale ma di lunga durata[26].
A questa forma di adescamento di adulti verso i minori è affiancata quella online: *grooming* online o *cybergrooming*. Il pedofilo può avvicinarsi online ai minori destando meno sospetti rispetto alla modalità *offline*; può entrare nella vita delle vittime dal computer o dallo *smartphone*, grazie ad esempio ai servizi online di messaggistica, ai *social* e ai videogiochi online interattivi.
L'approccio online consente un adescamento più facile rispetto al mondo reale dove la presenza di un adulto in luoghi frequentati dai minori potrebbe suscitare particolare attenzione e sospetti.
Il fenomeno del *grooming* online è stato oggetto di studio presso l'Università di Lancashire dove è stato articolato in diverse fasi[27]:

1. "*Friendship Forming Stage",* dove il *groomer* inizia a conoscere la vittima.
   La durata del tempo trascorso varia a seconda del livello di contatto che il pedofilo raggiunge con il minore. Durante questo intervallo di tempo l'adescatore può chiedere

[24]Eramo Federico, L.N.48/ Sulla criminalità informatica. Aspetti generali e ricadute sulla tutela dei minori dalle insidie telematiche, In Famiglia e Diritto, 2009, p.93.
[25] Salter Anna, psicologa americana, specializzata in crimini sessuali. Tra le sue pubblicazioni: Predators: Pedophiles. (2003) New York: Basic Books, Treating Child Sex Offenders and Victims: A Practical Guide. (1988) Newbury Park, CA, Sage Publications.
[26] Cyberlaws< https://www.cyberlaws.it/en/2019/adescamento-minori-child-grooming/>[ultimo accesso 13 aprile 2021].
[27] Lo studio è stato condotto dall'Università di Lancashire nel 2003. Ha come titolo *A TYPOLOGY OF CHILD CYBERSEXPLOITATION AND ONLINE GROOMING PRACTICES* ed è di Rachel O'Connell.

delle foto al minore per conoscerne l'aspetto e verificarne l'età e l'identità. In questa fase le foto scambiate non sono di natura sessuale.

2. *"Relationship Forming Stage"*, dove l'adulto approfondisce la conoscenza con il minore e avvia un dialogo con diversi argomenti come, ad esempio, la scuola frequentata e informazioni sulla famiglia.
   Generalmente il fine è quello di creare un contatto con il minore e dargli l'illusione di essere il suo migliore amico e confidente.
3. *"Risk Assestement Stage",* dove il pedofilo cerca di ricavare le informazioni sulla vita della vittima: dove vive, dov'è posizionato il suo computer in camera e quante persone lo utilizzano.
   La profilazione del minore è mirata a scoprire le sue attività e anche il livello di controllo dei mezzi elettronici da lui utilizzati da parte dei genitori.
4. "*Exclusivity Stage",* dove avviene il passaggio del pedofilo dalla figura di migliore amico della vittima all'unica persona che può capire il minore veramente.
   La conversazione in questa fase prende una piega diversa e molto più intima.
   Il *groomer* diventa il curatore della vittima e instaura un rapporto di fiducia reciproca e in segreto da tutti gli altri, terreno fertile per l'introduzione della fase successiva della conversazione che si concentra su questioni di natura più intima e sessuale.
5. "*Sexual Stage*", spesso introdotta da domande del tipo "hai mai dato un bacio?" viene poi direzionata verso la drammatica sfera dell'abuso sessuale e dello scambio di materiale pedopornografico.

Alcune ricerche in ambito europeo sull'adescamento online dei minori prendono come riferimento la fascia di età tra i 10 e i 17 anni: di questi circa il 15% ha ricevuto su Internet proposte sessuali e il 34% si è imbattuto in materiali di carattere sessuale senza aver effettuato nessuna ricerca mirata[28].

Gli effetti dell'abuso possono essere drammatici per la salute mentale e psichica del minore. Un ulteriore trauma per la vittima è dato dalla diffusione del materiale ad amici, parenti e conoscenti e la consapevolezza che chiunque potrebbe averlo visto.

Il *dossier* pubblicato da Telefono Azzurro nel 2019 sull'abuso sessuale e la pedofilia, denuncia che il mondo digitale ha aumentato la complessità degli abusi ed è terreno fertile per l'adescamento dei minori: "*Se nel 2015 i casi di adescamento costituivano il 4,7% delle*

[28] Nota 1.

chiamate alla linea 1.96.96, nel 2016 rappresentano il 6,5% delle chiamate, in aumento le segnalazioni per casi di pedopornografia online. Se nel 2015 rappresentavano il 3,3% delle chiamate ricevute per abuso sessuale e pedofilia, nel 2016 rappresentano il 4,3%"[29].

1.4 Le *challenge* sui social: il confine tra divertimento e pericolo

Le sfide sui *social network*, meglio conosciute come *challenge*, consistono nella ripresa video di azioni di varia natura per pubblicarle sui *social*, dove di solito vengono accompagnate da un *hashtag* di riferimento.

Sempre più diffuse e più comuni tra bambini e adolescenti, le sfide sono una fonte di svago e si attuano, generalmente, con la realizzazione di brevi video dove si invitano le altre persone a ripetere l'azione commessa. Successivamente il video viene pubblicato sui *social*.

Le *challenge* sono tante e diverse tra loro. Alcune sfide sono a scopo benefico o semplicemente divertenti; altre, al contrario, sono molto pericolose e rischiose per i minori, e sono le *challenge* estreme.

Una *challenge* innocua è la *Whisper Challenge* che consiste nel riprendere una persona amica che ascolta la musica a tutto volume, mentre l'altra cerca di far intuire alcune parole tramite il labiale. Un'altra è l'*Ice Bucket Challenge* che consiste nel riprendere una persona mentre si versa in testa un secchio d'acqua fredda e ghiaccio[30]. In realtà, quest'ultima è stata lanciata nel 2014 dalla *ASL Association* per sensibilizzare la popolazione sul tema della sclerosi laterale amiotrofica; grazie a questa campagna sono stati raccolti 115 milioni di dollari destinati alla ricerca scientifica per combattere questa patologia[31].

Altre *challenge* sono semplicemente dei balletti con le canzoni in voga del momento pubblicati su TikTok, il *social* utilizzato soprattutto da giovanissimi che consente di creare, condividere e commentare brevi video, come nel caso della *#Savagechallenge* diventata virale durante il *lockdown* del 2020.

Le *challenge* pericolose ed estreme possono tramutarsi in tragedie[32], come ad esempio la *BlackOut Challenge* e la *Blue Whale*. Nella prima il minore prova a resistere il maggior tempo

[29] Dossier Telefono Azzurro, *Abuso sessuale e pedofilia*. *Storie, contesti e nuove sfide*, 2019.

[30] Linkem, https://blog.linkem.com/challenge-da-fare/ [ultimo accesso: 16 aprile 2021].

[31] Als.org, ls.org/ice-bucket-challenge-spending "*The $115 million in donations raised through the 2014 ALS Ice Bucket Challenge spurred a massive increase in The ALS Association's capacity to invest in promising research, the development of assistive technologies, and increased access to care and services for people with ALS*".

[32] Cfr *infra* capitolo 2.

possibile con una cintura stretta attorno al collo. Nella seconda il bambino deve rispettare cinquanta regole, l'ultima è il suicidio.

Le *challenge* online, innocue o pericolose che siano, sono molto popolari tra i giovani, fino a farlo diventare un vero e proprio "boom delle *challenge*"[33].

I minori sono attratti da alcune particolari situazioni quando decidono di affrontare queste sfide[34].

L'intrattenimento è una di queste. I ragazzi spesso riproducono e replicano sui *social* i video degli amici o di personaggi famosi. Lo fanno anche per trovare una propria identità, per verificare i propri limiti e sfidare sé stessi anche all'estremo. Inoltre, per loro è importante sentirsi accettati dal gruppo e per questo accettano, o sono costretti psicologicamente ad accettare, a partecipare a sfide anche estreme. Alcune volte sono spinti dal desiderio di fare colpo e di emergere all'interno del gruppo, poiché la sfida viene percepita come necessaria per diventare virale sui *social*.

La natura di queste sfide avviene infatti in un contesto relativamente nuovo, quello dei *social*. Il video può diventare virale tra i giovani in poco tempo e raggiungere un pubblico potenzialmente vario e in ogni parte del mondo.

La partecipazione ad alcune delle *challenge* può portare anche in questo caso a esiti tragici. La morte di una bambina di dieci anni avvenuta il 21 gennaio 2021 a Palermo a causa dell'attuazione di una di queste *challenge* estreme, la *BlackOut Challenge*, è la dolorosa dimostrazione della estrema pericolosità di tali sfide.

[33] Trend Online, https://www.trend-online.com/tecnologia/boom-delle-challenge/.

[34] agendadigitale.eu/cultura-digitale/challenge-su-internet-cosa-sono-e-come-difendersi/.

Capitolo 2

Le *challenge* sui *social network*

2.1 La *Blue Whale Challenge*

La *challenge* per antonomasia è la *Blue Whale,* ed è la più pericolosa.
La *Blue Whale Challenge* nasce nel *social network* russo "*VKontakte*", paragonabile al nostro Facebook. Infatti, come in Facebook, si possono creare contenuti, esprimere le proprie idee, iscriversi a gruppi o community, mettere likes e salvare i post più apprezzati[35]. Il *social* russo è stato fondato nel 2006 da Pavel Durov[36] e oggi ha raggiunto 95 milioni di utenti attivi al mese. All'interno di questo spazio virtuale prende forma la *Blue Whale*.
Riscontriamo tracce di questa *challenge* nel 2013, ma la sua pericolosità emerge solo nel 2016, in seguito alla pubblicazione dell'articolo-inchiesta[37] della giornalista russa Galina Mursalieva, riguardante il suicidio di minori collegato a questa sfida mortale.
La giornalista rivela che durante l'anno 2015 in Russia si sono suicidati centrotrenta ragazzi e, di questi, ottanta erano riconducibili alla folle e drammatica *Blue Whale Challenge*. Infatti tutte le ottanta vittime si erano lanciate dai tetti dei palazzi più alti in città, avevano filmato la loro "impresa" e l'avevano diffusa nel web.
Questa sfida mortale negli anni si è andata sempre più diffondendo in tutto il mondo, riempiendo le pagine di cronaca.
L'articolo prendeva ad esempio anche la morte per suicidio della sedicenne Rina Palenkova nel novembre 2015. L'adolescente aveva pubblicato sul suo profilo *Vkonkate* un video dove preannunciava la propria morte. All'interno del suo profilo *social* gli inquirenti hanno trovato materiali che potevano essere ricondotti sia alle chat e ai gruppi della morte sia alle 50 regole *challenge*, come la pericolosa sigla "*f57*".
Ecco le famigerate 50 regole della Blue Whale Challenge[38]:

1. Incidetevi sulla mano con il rasoio "f57" e inviate una foto al curatore
2. Alzatevi alle 4.20 del mattino e guardate video psichedelici e dell'orrore che il curatore vi invia direttamente

[35] https://sociagency.it/vkontakte-vk-com-il-social-media-russo/.
[36] Pavel Valer'evič Durov è un imprenditore russo. Ha fondato il social *VKontakte* oggi chiamato VK e l'app di messaggistica Telegram.
[37] Pubblicato su *Novaya Gazeta*, maggio 2016.
[38] L'elenco è stato ripreso dal sito: https://www.scienzeforensi.org/blog/index.php?id=gcgnx70y.

3. Tagliatevi il braccio con un rasoio lungo le vene, ma non tagli troppo profondi. Solo tre tagli, poi inviate la foto al curatore
4. Disegnate una balena su un pezzo di carta e inviate una foto al curatore
5. Se siete pronti a "diventare una balena" incidetevi "yes" su una gamba. Se non lo siete tagliatevi molte volte. Dovete punirvi
6. Sfida misteriosa
7. Incidetevi sulla mano con il rasoio "f57" e inviate una foto al curatore
8. Scrivete "#i_am_whale" nel vostro status di VKontakte
9. Dovete superare la vostra paura
10. Dovete svegliarvi alle 4.20 del mattino e andare sul tetto di un palazzo altissimo
11. Incidetevi con il rasoio una balena sulla mano e inviate la foto al curatore
12. Guardate video psichedelici e dell'orrore tutto il giorno
13. Ascoltate la musica che vi inviano i curatori
14. Tagliatevi il labbro
15. Passate un ago sulla vostra mano più volte
16. Procuratevi del dolore, fatevi del male
17. Andate sul tetto del palazzo più alto e state sul cornicione per un po' di tempo
18. Andate su un ponte e state sul bordo
19. Salite su una gru o almeno cercate di farlo
20. Il curatore controlla se siete affidabili
21. Abbiate una conversazione con una “balena" (con un altro giocatore come voi o con un curatore) su Skype
22. Andate su un tetto e sedetevi sul bordo con le gambe a penzoloni
23. Un'altra sfida misteriosa
24. Compito segreto
25. Abbiate un incontro con una "balena"
26. Il curatore vi dirà la data della vostra morte e voi dovrete accettarla
27. Alzatevi alle 4.20 del mattino e andate a visitare i binari di una stazione ferroviaria
28. Non parlate con nessuno per tutto il giorno
29. Fate un vocale dove dite che siete una balena.

Le regole dalla numero 30 alla numero 49 ripetono ossessivamente le precedenti: dicono di svegliarsi ogni giorno alle 4.20 del mattino, di guardare video e filmati genere horror, di ascoltare la musica che il curatore invia alla vittima, di procurarsi atti di autolesionismo con tagli in varie parti del corpo. Tutto questo parlando a una “balena” immaginaria.

L'ultima regola, la numero 50, è il suicidio, che secondo gli ideatori è l'unico mezzo per riprendere in mano la propria vita. Quest'ultima regola ha un enorme impatto emotivo sulle menti di adolescenti facilmente suggestionabili.

L'esito nefasto diventa inevitabile.

Il nome della *challenge,* cioè la balena blu o azzurra, rimanda al particolare comportamento di questi animali. Infatti quando si allontanano dal gruppo o perdono il loro orientamento, spiaggiano in riva, non sono più in grado di rientrare nell'acqua e muoiono.

Da qui la similitudine con le vittime di questo gioco.

Il curatore seleziona accuratamente le giovani vittime che si sentono escluse e disorientate dalla società. La profilazione degli adolescenti è mirata a creare gruppi con finalità di morte con ragazzi e ragazze che cercano una via di fuga dalla propria vita.

Il fondatore della *Blue Whale,* Philipp Budeikin, era uno studente di psicologia russo. Arrestato a San Pietroburgo nel 2017, ha confessato di non essersi mai pentito e ha definito le proprie vittime "scarti biologici".

Nello stesso anno è stato arrestato un altro curatore senza scrupoli, Ilya Sidrov, un postino russo ventiseienne, che ha dichiarato di aver adescato trentadue minorenni e di aver dato loro regole precise, le cinquanta sopra riportate, con l'obiettivo di portarle al suicidio.

Le chat della morte dove si svolgeva la *challenge* hanno allarmato l'opinione pubblica; le istituzioni hanno reagito e preso alcune misure per contrastare questa aberrazione.

In Russia è stato approvato un decreto per inasprire le pene sull'istigazione al suicidio dei minori: la deputata Irina Yarovaya sosteneva che la *Blue Whale* era una "guerra contro i bambini" e l'ha definita "un'attività criminale organizzata e intenzionale"[39].

La Duma russa il 28 aprile 2017 ha approvato una legge in cui vengono inasprite le pene per coloro che creano gruppi e chat della morte, come i gruppi della *Blue Whale,* reato punibile con una reclusione fino a sei anni.

Anche l'Italia ha preso misure per contrastare questo fenomeno.

L'eco mediatica si espande dopo il servizio di inchiesta delle Iene andato in onda nel maggio 2017, dove tra l'altro il giornalista Matteo Viviani si era recato in Russia per parlare con i genitori dei ragazzi rimasti vittime della *Blue Whale Challenge*.

Alcuni giornalisti italiani ritennero però che il servizio delle Iene fosse una *fake news*.

In realtà era vero che i video mandati in onda riguardavano ragazzi che si erano suicidati gettandosi dai palazzi, ma non erano vittime dirette della *Blue Whale*: le cause erano altre.

[39] V. Nota 38.

Le Iene, in un altro servizio mandato in onda subito dopo, hanno ammesso l'errore di non aver verificato accuratamente l'attendibilità dei video.

Gli stessi video erano stati mandati in onda dalla SpiegelTv tedesca: nel servizio però veniva spiegato ai telespettatori che potevano non essere del tutto attendibili.

Prima delle Iene, nel marzo 2017 le testate giornalistiche "Il Messaggero" e "Il Giornale" avevano già pubblicato due articoli sulla estrema pericolosità del fenomeno.

Il titolo dell'articolo del Messaggero è "*Blue Whale: il gioco che ha già portato al suicidio 130 adolescenti*"[40] e descrive la *challenge* come un girone perverso con un finale drammatico; il titolo dell'articolo del Giornale è "*Un nuovo "gioco" dell'orrore spopola tra i giovani: il Blue Whale*"[41] e sottolinea il carattere violento di questo folle "gioco".

In Italia, la Polizia postale nel corso degli ultimi anni ha elaborato cinque regole di contrasto alla *Blue Whale* per ragazzi e adulti[42].

La prima regola individua la necessità del dialogo sui pericoli e i rischi del web sia con la propria famiglia sia nella scuola.

La seconda e la terza regola sono rivolte agli adulti: prestare attenzione ai cambiamenti di umore del ragazzo, ai peggioramenti della sua rendita scolastica e a quanto viene raccontato dall'adolescente.

La quarta e la quinta regola sono rivolte ai ragazzi: denunciare chiunque tenti di manipolare la loro vita e controllare accuratamente i gruppi a cui vengono aggiunti nel web[43].

Negli ultimi anni anche i *social network* hanno avuto consapevolezza della pericolosità della *Blue Whale;* Instagram in particolare ha creato dei centri di assistenza per gli adolescenti che si trovano in difficoltà.

Infatti quando su Instagram si inseriscono le parole *Blue Whale*, il *social* fa apparire questa notifica: "*Possiamo aiutarti? I post con parole che cerchi spesso incoraggiano comportamenti che possono causare dolore o condurre anche alla morte. Se stai attraversando un momento difficile, ci piacerebbe aiutarti*".

Dopo questo messaggio appare un link di supporto che invita a:

1. contattare un amico o inviare un messaggio a qualcuno di cui ci si fida

---

40 https://www.ilmessaggero.it/primopiano/esteri/blue_whale_gioco_ha_gia_portato_al_suicidio_130_adolescenti-2294375.html.

41 https://www.ilgiornale.it/news/cronache/nuovo-gioco-dellorrore-spopola-i-giovani-blue-whale-1371180.html.

42 V. Nota 37.

43 *Ibidem.*

2. parlare con un volontario di una linea di assistenza con indicazioni precise, quali ad esempio il telefono amico, il telefono rosa, il telefono azzurro
3. scoprire cosa può far stare meglio, ad esempio lettura di suggerimenti che sono stati utili ad altre persone.

2.2 La *Blackout challenge*

La morte di una bambina di Palermo di soli dieci anni, avvenuta a gennaio 2021 a causa dell'attuazione della sfida online *Blackout Challenge,* ha scosso profondamente l'opinione pubblica.

Questa *challenge*, chiamata anche *hanging challenge*, consiste nello sfidare gli utenti delle piattaforme social, in particolare TikTok, a trattenere il respiro per il maggior tempo possibile.

La *challenge* istiga ad avvolgersi una cintura stretta intorno al collo in modo tale da provocare per alcuni secondi la sensazione di perdita di coscienza e la stessa euforia di quando a 7mila metri di quota ci si trova senza ossigeno.

Gli iniziali pochi secondi, quando si ripete la *challenge*, possono facilmente aumentare, diventare minuti e portare alla morte per asfissia.

Antonella, la bambina palermitana decenne, aveva utilizzato la cintura di un accappatoio e l'aveva stretta forte intorno al collo fino a morire.

A fine marzo 2021 un episodio analogo è avvenuto in Piemonte, protagonista una ragazza dodicenne. La minore si è suicidata con la cintura di un accappatoio, con lo stesso *modus operandi* della vittima di gennaio.

La *Blackout Challenge,* fenomeno piuttosto recente, purtroppo non è nuovo.

Infatti nel settembre 2018 è morto a Milano Igor, un ragazzo di appena quattordici anni.

Igor è stato trovato impiccato nella sua camera con una corda legata alla traversa del letto a castello.

Dalle indagini è emerso che il minore aveva da poco visualizzato alcuni video sulla piattaforma YouTube; riguardavano azioni pericolose messe in atto da ragazzi, che le filmavano e poi le postavano sul web.

Uno di questi video si intitolava "*Le cinque challenge pericolose che i ragazzi fanno*"[44], tra cui la *blackout challenge*.

[44] https://www.open.online/2021/02/03/caso-igor-maj-blackout-challenge-intervista-pm-cristian-barilli/.

Viene descritta come una perdita transitoria di coscienza con tecniche di soffocamento e di pochi secondi di stato di euforia.

In seguito alla morte di altri bambini, la Procura dei minori ha aperto un fascicolo per "istigazione al suicidio" a carico di ignoti[45].

Per questo reato, nella pratica sembrerebbe alquanto difficile giungere a una condanna.

Un caso eclatante riguarda proprio il caso "Igor".

Infatti il Giudice per le indagini preliminari del Tribunale di Milano, con decreto del 21 marzo 2021**,** ha deciso di archiviare il procedimento ex art. 582 c.p. aperto nei confronti dei due indagati.

Gli indagati erano i titolari di due canali YouTube sui quali erano stati caricati il video visionato da Igor e un altro che citava e discuteva del fenomeno della sfida del *blackout.*

Le prove a carico dei due indagati sono state considerati insufficienti per due motivi:

1. per difetto di dolo, di far "*sorgere, rafforzare o agevolare il proposito suicidario nella indistinta platea degli utenti della rete Internet, potenziali destinatari del video*".

   La magistratura ha sostenuto che i video non erano finalizzati all'emulazione delle *challenge* e che gli indagati avevano avvertito nei loro video sulle conseguenze delle sfide pericolose. Infatti riportavano immagini di persone che erano finite in gravi condizioni di salute.
2. la volontà suicida non è mai esistita nel ragazzo.

   La sua *challenge* non aveva lo scopo di togliersi la vita ma di cimentarsi in una sfida pericolosa e provare l'ebrezza del soffocamento per pochi secondi.

   Viene esclusa l'ipotesi di omicidio colposo ex art 580 c.p. perché non ci sono "*né profili di colpa della condotta degli indagati - o di altri soggetti responsabili del sito su cui i video per cui è processo sono girati - né la sussistenza di un nesso di causalità tra eventuali condotte (anche omissive ed eventualmente qualificabili come negligenti imprudenti o imperite o inosservanti di leggi, regolamenti, ordini e discipline) e l'evento morte come si è concretamente verificato*".

Per quanto riguarda invece la responsabilità della piattaforma YouTube, il Giudice ha concluso che la società non risulta responsabile di alcun illecito amministrativo.

I casi esaminati e i procedimenti aperti dalle Procure fanno emergere il vuoto di tutela nell'ambito del digitale e in particolare nei *social network*, come dimostra anche l'intervento del Garante per la protezione dei dati personali, in particolare su TikTok, che mira a colmarlo.

[45] https://www.studiocataldi.it/articoli/41686-blackout-challenge-e-istigazione-al-suicidio.asp#par1.

2.3 Misure del Garante per la protezione dei dati personali

Il Garante per la protezione dei dati personali - il Garante italiano della Privacy - ha preso diverse iniziative a tutela dei minori nei *social network*.

Un'azione particolarmente incisiva è stata quella verso TikTok, il *social network* più popolare e quindi con più fattori di rischio per i minori.

Già nel 2020 l'Authority si è fatta promotrice di una *Task force* europea verso il *social*, e anche a livello nazionale ha riscontrato alcune problematiche[46].

Una di queste è la modalità di iscrizione a TikTok. Teoricamente le regole sanciscono il divieto di iscrizione al di sotto dei 13 anni, in pratica possono essere facilmente aggirate: è sufficiente inserire una data di nascita falsa.

Un'altra criticità è il profilo utente, preimpostato da TikTok come pubblico: i contenuti sono perciò visibili a tutti senza filtri.

Inoltre le norme italiane sulla privacy prevedono che i minori di 14 anni possono iscriversi ai *social* solo con il consenso dei genitori, e su questo TikTok non fa nessuna verifica.

A seguito del tragico evento della bambina palermitana[47] e del clamore mediatico conseguente, il Garante ha adottato un provvedimento d'urgenza fino al 15 febbraio 2021[48] con il blocco immediato dell'uso dei dati personali degli utenti di cui non è possibile accertare con sicurezza l'età. TikTok si è adeguata alle misure richieste:

1. ha inviato un messaggio agli utenti italiani, chiedendo di indicare di nuovo la data di nascita per utilizzare ancora la piattaforma
2. se un utente fosse stato minore di 13 anni, avrebbe rimosso definitivamente l'*account*
3. ha migliorato la possibilità di segnalare la presenza di utenti minori di 13 anni.

Il Garante, tuttavia, non ha ritenuto tali modifiche sufficienti a tutelare adeguatamente i minori, per cui ha emesso un altro provvedimento a marzo 2021[49], questa volta anche nei confronti di Facebook e di Instagram, sulle modalità di iscrizione e sulle misure adottate per verificare l'età dei minori.

[46] Comunicato stampa 24 gennaio 2020, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9249688.
[47] Vedi Capitolo 2 pag 20.
[48] Comunicato stampa 22 gennaio 2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524224 e Provvedimento 22 gennaio 2021 [doc. web n. 9524194], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524194.
[49] Provvedimento 25 marzo 2021 [doc. web n. 9574709], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9574709.

TikTok si è impegnata a implementare ulteriormente le misure di sicurezza in Italia per i minori. In effetti tra il 9 febbraio e il 21 aprile 2021 sono stati 12 milioni e mezzo gli utenti italiani ai quali è stato chiesto di confermare di avere più di 13 anni per accedere alla piattaforma e sono stati oltre 500 mila gli utenti rimossi perché non avevano ancora 13 anni.

Il Garante tuttavia non ritiene ancora tali misure sufficienti.

Infatti ha chiesto a TikTok ulteriori interventi per escludere i minori di 13 anni dalla piattaforma.

TikTok in sintesi si è ulteriormente impegnata a:

1. garantire la cancellazione entro 48 ore degli account al di sotto dei 13 anni di età
2. rafforzare i meccanismi di blocco dei dispositivi utilizzati dagli infratredicenni per accedere
3. studiare e elaborare soluzioni per minimizzare il rischio per i bambini al di sotto dei 13 anni
4. nuove iniziative di comunicazione per educare a un uso consapevole e sicuro della piattaforma e ricordare che non è adatta ai ragazzi di età inferiore ai tredici anni[50].

2.4 *Challenge* sui social: rischi e tutela dei minori. Un sondaggio

Le *challenge* online sono oggetto di studio e di approfondimento nel progetto "*Challenge sui social: rischi e tutela dei minori*"[51], all'interno dell'insegnamento "Diritto di Internet: social media e discriminazione", anno accademico 2020/2021, Università LUISS Guido Carli.

Le caratteristiche del progetto sono:

1) dimostrare l'effetto negativo di un uso dei *social* non controllato e regolamentato sui minori
2) denunciare le conseguenze e gli effetti sui minori di *challenge* popolari e pericolose sui *social network*
3) verificare la correlazione tra la partecipazione dei minori alle *challenge* e l'aspetto psicologico-educativo
4) alcune interviste
5) la somministrazione di un questionario per un sondaggio.

[50] https://www.labparlamento.it/garante-privacy-richiama-tik-tok-su-minori/

[51] Il progetto "*Challenge sui social: rischi e tutela dei minori*" è stato elaborato tra marzo e giugno 2021 da Flavia Cavalli, Chiara D'Addesa e Beatrice Marra.

Il questionario del sondaggio è stato somministrato tra marzo e aprile 2021 a 202 minori italiani. La fascia di età scelta va dai dodici ai diciassette anni.

Le domande contenute nel "Sondaggio per lavoro di ricerca sulle *challenge* che si diffondono sui *social network*" sono le seguenti:

1) Quanti anni hai? - Seleziona una fascia d'età: 12-14 anni o 15-17 anni
2) Sei un maschio o una femmina?
3) Sei iscritto/hai TikTok?
4) Se sì, a che età più o meno ti sei iscritto?
5) Se lo hai, quante ore passi in media su TikTok?
6) I tuoi genitori sanno che usi TikTok e che cos'è?
7) Conosci alcune *challenge* pericolose (come la *Blue Whale*, la *Blackout Challenge*) che girano su TikTok?
8) Conosci qualche altra *challenge* diversa da quelle che abbiamo menzionato nella domanda di prima? Se sì scrivilo qui
9) Hai mai partecipato o conosci qualcuno (amico, parente, conoscente) che ha partecipato a queste *challenge*?
10) Avete mai parlato a scuola con i professori di questo argomento?

Il primo obiettivo del sondaggio è di comprendere la correlazione tra l'età del minore, il sesso e la popolarità del *social network* TikTok.

La domanda sull'età di iscrizione vuole scoprire se i minori mentono sulla loro età anagrafica quando si iscrivono al social[52], considerata l'età minima di iscrizione di 13 anni.

Un altro elemento di analisi riguarda la consapevolezza delle pericolosità nei *social* e quanti sono in grado di definire il confine tra divertimento e pericolo.

Le domande "Conosci alcune *challenge* pericolose (come la *Blue Whale* e la *Blackout Challenge*) che girano su TikTok?" e "Conosci qualche altra *challenge* diversa da quelle che abbiamo menzionato nella domanda di prima?" vogliono stabilire se il minore è consapevole della pericolosità delle *challenge* e se ne esistono altre non menzionate nel questionario.

Le domande "Avete mai parlato a scuola con i professori di questo argomento?" e "I tuoi genitori sanno che usi TikTok e che cos'è?" hanno l'obiettivo di comprendere la misura e la qualità del dialogo su questi temi in famiglia e nella scuola.

[52] Capitolo 1.

Infine, la domanda “Hai mai partecipato o conosci qualcuno (amico, parente, conoscente) che ha partecipato a queste challenge?” ha la finalità di comprendere quale sia la gravità del fenomeno tra i minori.

Il primo dato che emerge dal sondaggio è che su 202 minori, ben 189 sono iscritti al *social* TikTok, come risulta nel grafico 1.

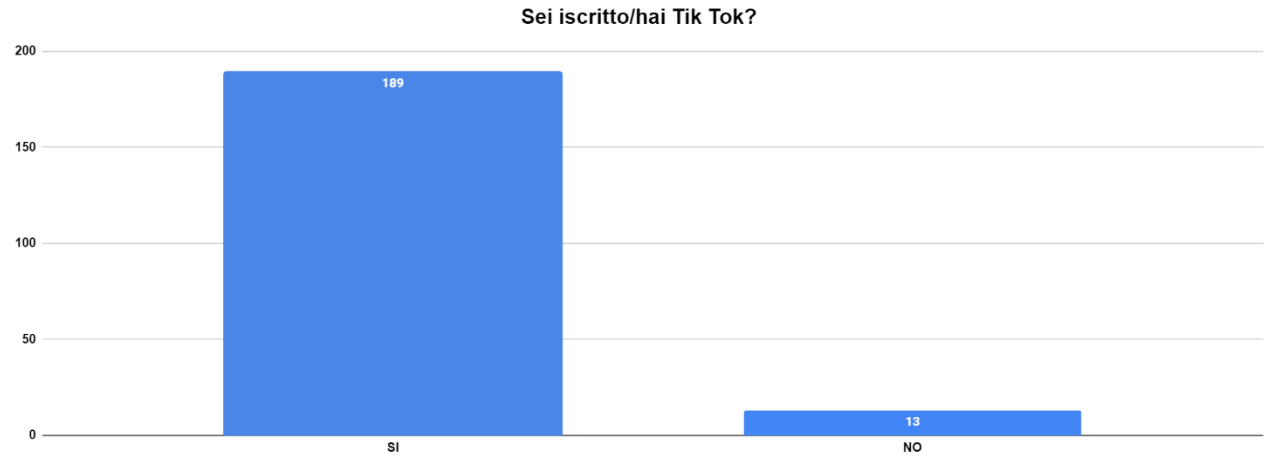

Grafico 1. Iscrizione a TikTok. Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

L’età del campione è composta prevalentemente da ragazzi di 15-17 anni di età: sono 154 su 202.

Di conseguenza, i ragazzi nella fascia d’età 12-14 anni, sono 48.

Le ragazze sono 163, i ragazzi 39.

I dati sono riportati nei grafici 2 e 3.

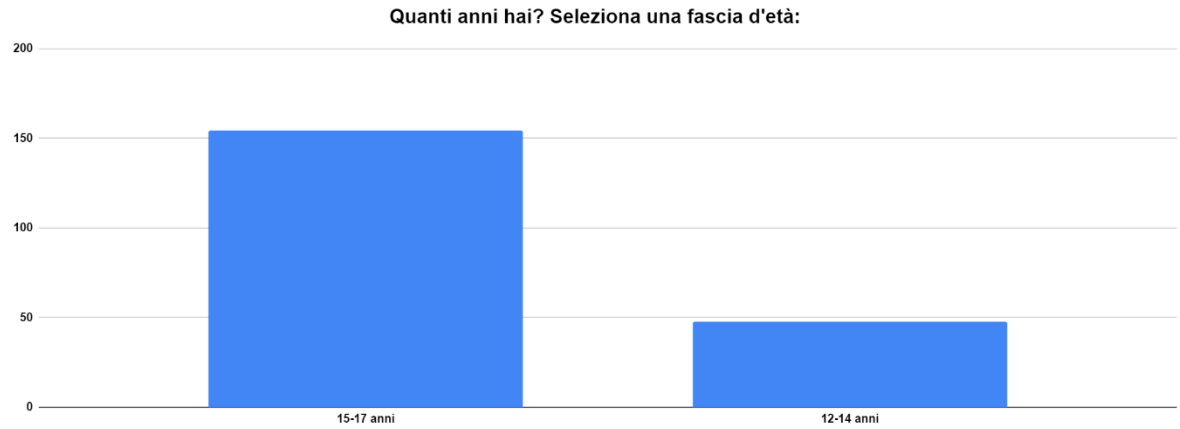

Grafico 2. Quanti anni hai? Seleziona una fascia d’età. Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

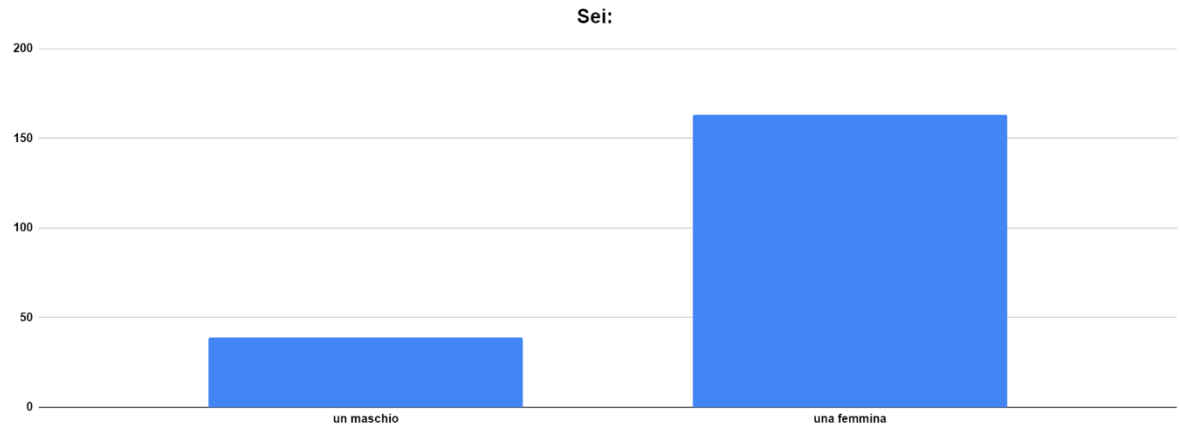

Grafico 3 – Sei maschio o femmina? Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

Dai dati emerge che ben 66 minori su 202 si sono iscritti al *social network* quando ancora non avevano compiuto 13 anni.

Tra questi, due bambini si sono iscritti al *social* quando avevano 8 anni, quattro a 9 anni e sei a soli 10 anni.

Sei ragazzi hanno risposto che si sono iscritti alla piattaforma quando si chiamava Musical.ly.

Nell'agosto 2018 le due piattaforme Musical.ly e TikTok si fondono in un *social* unico che prende il nome di quest'ultimo.

Le risposte sono evidenziate nel grafico 4:

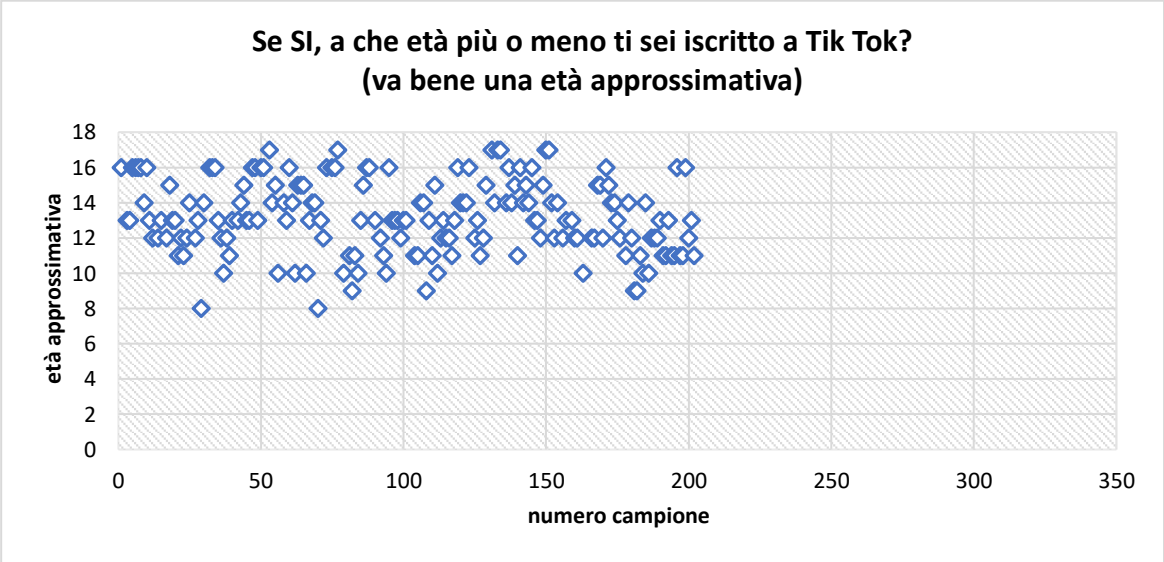

Grafico 4. Età iscrizione a TikTok. Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

Per quanto riguarda il tempo passato davanti alla piattaforma TikTok durante l'intera giornata, il 47,6% guarda i video in media 1-2 ore al giorno, il 23,3% consulta il *social* per 30 minuti e il 29,1% sta davanti allo schermo per 2 o più ore, come è riportato nel grafico 5:

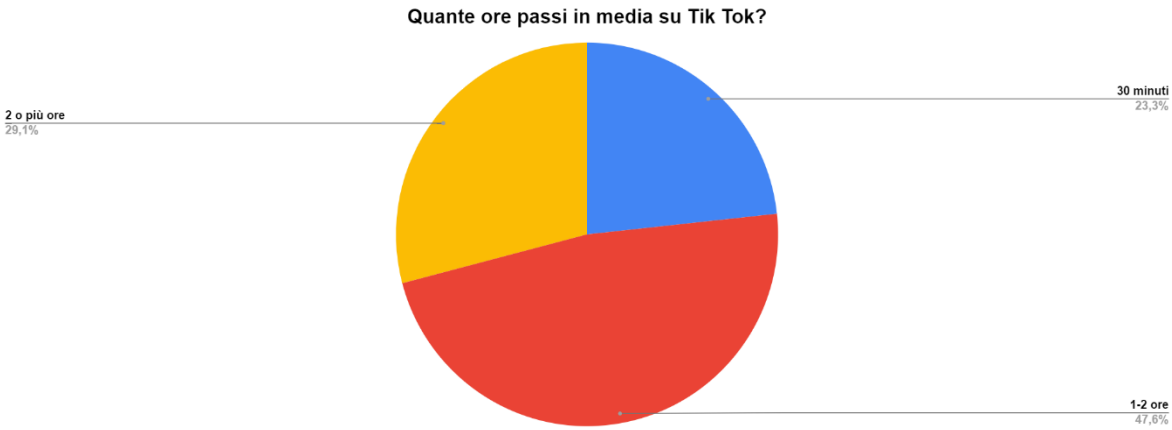

Grafico 5. Tempo in media al giorno su TikTok. Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

Dal sondaggio è emerso che i minori conoscono bene le *challenge Blue Whale* e *Blackout*. Infatti su 202 intervistati, ben 128 conoscono queste *challenge*, pari al 63,4% di sì e al 36,6% di no.
Queste percentuali sono riportate nel grafico 6:

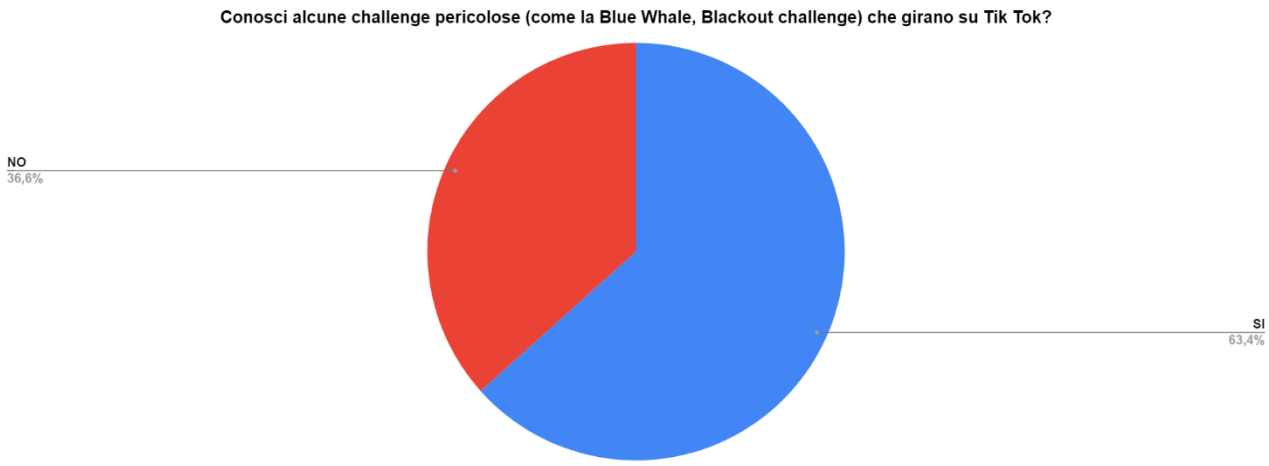

Grafico 6. Conosci alcune challenge pericolose? Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

Per quando riguarda il dialogo tra i ragazzi e i genitori, in particolare se questi ultimi sono a conoscenza dell'iscrizione da parte dei figli minori al *social*, il grafico 7 mostra che il 15,3% dei genitori del ragazzo non sono a conoscenza di tale uso e il restante 84,7% sì:

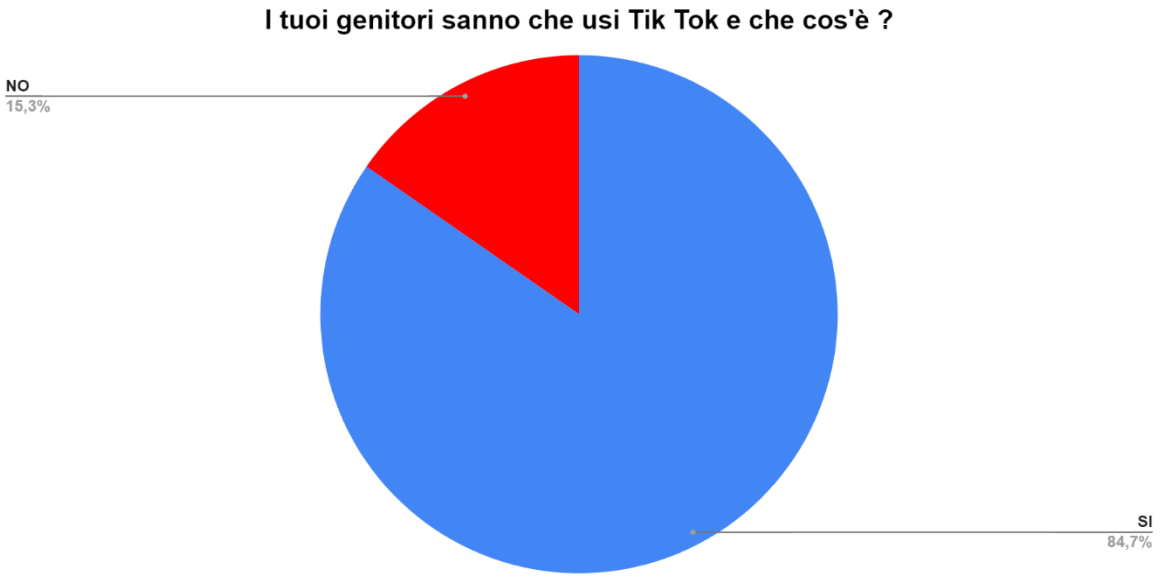

Grafico 7. I tuoi genitori sanno che stai su TikTok e che cos'è? Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

Emerge un *bug* educativo nel mondo del digitale, confermato dal fatto che molte volte la scuola non parla direttamente con i ragazzi della pericolosità delle *challenge*, che se non sono opportunamente controllate, possono portare a tragedie irrimediabili.
Nel sondaggio solo 76 minori hanno affermato di averne parlato a scuola, come si evince dal grafico 8:

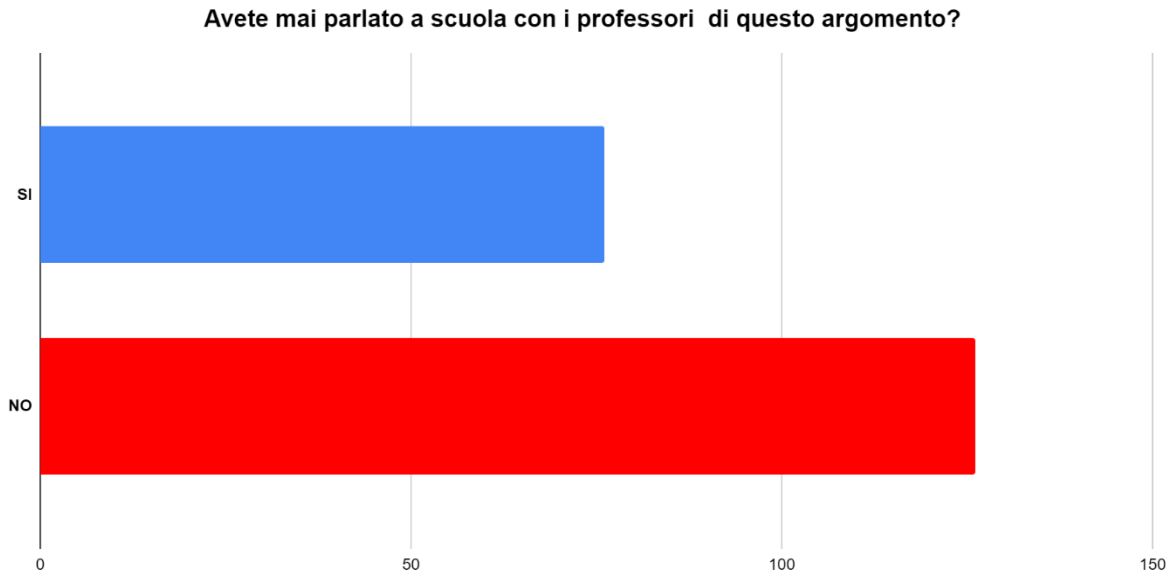

Grafico 8. Avete mai parlato a scuola con i professori di questo argomento? Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

Alla domanda "Hai mai partecipato o conosci qualcuno (amico, parente, conoscente) che ha partecipato a queste challenge?" solo tre minori hanno risposto sì.
È da notare che due minori hanno dichiarato di avere tra i 12-14 anni e altri due di essersi iscritti alla piattaforma TikTok all'età di 11 anni, quindi con ben due anni in anticipo rispetto al divieto della piattaforma di iscriversi al di sotto dei 13 anni. Si tratta del 2,0% del campione.
Questi dati sono riportati nel grafico 9:

Grafico 9. Hai mai partecipato o conosci qualcuno che ha partecipato a queste challenge? Fonte: Progetto *Challenge sui social: rischi e tutela dei minori*.

Dal sondaggio sono emerse informazioni interessanti sulla conoscenza e l'utilizzo di altre due challenge potenzialmente pericolose oltre a quelle menzionate nel questionario: la "*Skullbreaker challenge*" e la "*Bugs bunny challenge*".
La "*Skullbreaker challenge*" viene descritta dal giornale Open come "un atto di bullismo che può uccidere"[53]. Si tratta di una sfida che ha avuto un'ampia diffusione su TikTok.
Sono tre i protagonisti di questa *challenge*: due artefici e una vittima.
La sequenza del gioco perverso si svolge in presenza: i due complici saltano insieme, poi fanno saltare la vittima. Quando è il momento della vittima di saltare, i due complici le fanno uno sgambetto, anzi, le danno contemporaneamente un calcio ciascuno, e la vittima cade violentemente a terra con il rischio di rompersi la testa. Da qui il nome *Skullbreaker o Rompecraneos* in Sudamerica.
Tutta la sequenza è ripresa in un video girato con lo smartphone.

[53] https://www.open.online/2020/02/22/skullbreaker-challenge-un-atto-di-bullismo-che-puo-uccidere-la-verifica-sui-tre-presunti-casi-di-morte/

Nel questionario sono state menzionate anche altre *challenge* ritenute dai ragazzi pericolose: la "*Momo Challenge*", la "*Bugs bunny challenge*" e ancora "*challenge dove si postano video del proprio corpo mostrando le proprie insicurezze*".

La prima *challenge* diventa virale con la diffusione di Momo, una foto di una orripilante figura di donna-uccello con gli occhi sporgenti, i capelli neri e lunghi, il corpo tozzo e le zampe da rapace, ideata in Giappone da Keisuke Aisawa.

Per contrastare la diffusione della *challenge* la polizia irlandese ha pubblicato un comunicato su Facebook dove spiega in cosa consiste la pericolosità della sfida: Momo infatti invita i giovani ragazzi a provocarsi danni fisici e autolesionismo fino al suicidio indotto.

La "*Bugs bunny challenge*" prevede che chi la attua sia sdraiato a pancia sotto, con i piedi che sbucano da dietro la testa per assomigliare a un coniglio. Deve muovere i piedi con i calzini bianchi come se fossero le orecchie del coniglietto *Bugs Bunny* e muoversi a tempo di musica. La colonna sonora è un brano rap russo del 2018, dove si fa riferimento al coniglio dei cartoni animati.

La *challenge* è apparentemente semplice e innocua, se non fosse per la variante più ammiccante e esplicita, che sfocia nella pedopornografia.

Infine dal sondaggio emergono le *challenge* dove si postano video del proprio corpo e si mostrano le proprie insicurezze.

Queste sfide sono collegate al problema dei disturbi del comportamento alimentare.

I disturbi alimentari come l'anoressia e la bulimia si manifestano principalmente in età adolescenziale. Tali disturbi sono in costante aumento, accentuato dalla pressione mediatica e da modelli socioculturali che influenzano lo sviluppo dell'identità del minore.

Un esempio è la *A4 Waist Challenge*: una sfida dove i ragazzi, e soprattutto le ragazze, si fotografano tenendo tra le mani davanti al busto un foglio di carta formato A4 per mostrare la loro magrezza.

Scopo della *challenge* è che le linee dei fianchi spariscano dietro al foglio[54].

Le *challenge estreme* sono quindi pericolose per tutti ma soprattutto per i minori, più fragili e con inferiori strumenti di autotutela.

C'è bisogno di un coordinamento delle istituzioni, delle scuole e delle famiglie per evitare che i minori cadano nelle trappole delle sfide perverse.

[54] Nota 1.

Capitolo 3
La tutela online dei minori:
gli elementi significativi in giurisprudenza

3.1. Le fonti giuridiche sovranazionali a tutela dei minori e nell'affermazione dei loro diritti

I diritti fondamentali dei minori vengono affermati per la prima volta dalla Convenzione di New York del 20 novembre 1989, ratificata in Italia con la legge 27 maggio 1991, n. 176.
Il trattato del 1989, meglio conosciuto come "Convenzione dei diritti del fanciullo" (*Convention on the Rights of the Child*), sancisce il principio del c.d. "diritto all'ascolto del fanciullo".
L'articolo 12 infatti stabilisce che gli Stati garantiscono al fanciullo il diritto di esprimere liberamente la sua opinione su ogni questione che lo interessi; le sue opinioni vanno prese in considerazione in relazione alla sua età e al suo grado di maturità.
La Convenzione tratta anche del diritto all'identità personale e alla riservatezza del fanciullo.
Gli articoli 8 e 16 infatti introducono il principio secondo cui "nessun fanciullo sarà oggetto di interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza, e neppure di affronti illegali al suo onore e alla sua reputazione", e il "diritto alla protezione della legge contro tali interferenze o tali affronti".
Anche nella "Carta dei diritti fondamentali dell'unione europea"[55] (*Charter of Fundamental Rights*) si può prevedere l'estensione ai minori del principio contenuto nell'articolo 7 secondo il quale "ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni".
Il quadro normativo sovranazionale si completa con la "Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali" (*European Convention on Human Rights and Fundamental Freedoms*) del 4 novembre 1950, che all'articolo 8 recita: "ogni persona (e dunque anche il minore) ha diritto al rispetto della propria vita privata e familiare". Il trattato è stato ratificato in Italia con la legge del 4 agosto 1955, n. 848.

[55] Carta dei diritti fondamentali dell'Unione europea (2016/C 202/02), 7.6.2016, in Gazzetta ufficiale dell'Unione europea C 202/389.

Questi fondamentali riferimenti e principi normativi sovranazionali hanno consentito che i minori si trasformassero da semplice oggetto di protezione nei rapporti giuridici familiari a soggetti titolari di diritti fondamentali.
Non si può quindi prescindere da tali diritti nell'analisi delle problematiche e dei rischi connessi all'uso delle nuove tecnologie da parte dei minori e al tempo stesso non ne va limitato l'ingresso.
Infatti l'accesso alla rete è stato considerato dal prof. Stefano Rodotà "tra le attività realizzatrici della persona"[56].

3.2. Il Regolamento europeo 2016/679: la tutela alla riservatezza dei minori nel digitale

Nella normativa sovranazionale, particolare rilevanza ha assunto per la tutela dei minori nel mondo digitale il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, il c.d. "Regolamento generale sulla protezione dei dati" o "*General Data Protection Regulation*" (GDPR).
Il Regolamento stabilisce i principi di protezione sul trattamento dei dati delle persone fisiche e ha trovato applicazione diretta in tutti gli Stati membri a partire dal 25 maggio 2018[57].
Il legislatore europeo, infatti, ha voluto normare i pericoli connessi al graduale aumento nell'uso dei media online da parte dei minori, quale diretta conseguenza della "rivoluzione digitale".
Tali pericoli derivano dalla massiccia circolazione di dati riferiti a bambini sempre più piccoli, anche di età inferiore ai dodici anni.
Ha quindi inserito nel Regolamento due disposizioni specifiche per proteggere la dignità, la riservatezza e l'immagine dei fanciulli.
Le disposizioni si concretizzano nell'articolo 8 e nell'articolo 17.
L'articolo 8 riguarda le "Condizioni applicabili al consenso dei minori in relazione ai servizi della società delle informazioni" e l'articolo 17 il "Diritto alla cancellazione", il c.d. "diritto all'oblio".
I due articoli sono strettamente collegati e si rivolgono esclusivamente ai servizi offerti dalle società di informazione[58].

[56] Stefano Rodotà, *Il diritto di avere diritti*, Roma-Bari, Editori Laterza, 2012, pp. 378 ss.
[57] Regolamento (UE) del 27 aprile 2016 del Parlamento europeo e del Consiglio 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.
[58] Cfr. atti del Convegno "Facebook et similia (profili specifici dei social network)", organizzato presso la Facoltà di Giurisprudenza di Pavia il 30 settembre e il 1° ottobre del 2011. Gli atti del Convegno sono stati pubblicati negli

Prevedono che un minore possa dare un consenso consapevole al trattamento dei suoi dati in rete solo dal sedicesimo anno di età.

Nel caso in cui il fanciullo abbia un'età inferiore a 16 anni, il trattamento dei dati si può considerare lecito solo se e nella misura in cui il consenso sia prestato liberamente dal titolare della responsabilità genitoriale e non dal minore stesso.

Per la prima volta quindi, attraverso il Regolamento, l'Unione europea fissa un'età minima per l'accesso ai servizi di informazione in rete e per l'accesso ai *social* media.

Il legislatore europeo sull'età minima ha lasciato liberi gli Stati membri di abbassare l'età fino a 13 anni: l'Italia ha scelto di portare la soglia minima a 14 anni di età.

I *social* media hanno fissato l'età minima a 13 anni per l'iscrizione in autonomia ai vari portali, in linea con il "*Children's online Privacy Protection Act"* (COPPA), una legge federale degli Stati Uniti in vigore dal 21 aprile 2000[59].

COPPA obbliga i siti Web a chiedere l'autorizzazione dei genitori prima di raccogliere informazioni personali sui bambini minori di 13 anni[60].

Per effettuare il controllo su tali soglie, il Regolamento europeo sancisce che il titolare del trattamento debba verificare che il consenso sia effettivamente prestato o autorizzato da chi esercita la responsabilità genitoriale[61].

Infatti l'articolo 8 al secondo paragrafo prevede che il titolare del trattamento si attivi, con tutti i sistemi tecnici disponibili, per verificare il rispetto della regola sul limite d'età. Si tratta di un'indicazione significativa perché, nonostante la formale raccomandazione da parte dei gestori di non mentire al momento dell'inserimento dei propri dati personali, raccomandazione accompagnata dalla minaccia di recedere in caso di trasgressione della regola, nei fatti non viene attuata nessuna politica di controllo.

Il concetto è ribadito anche nelle Linee Guida adottate a maggio 2020 dal Gruppo dei Garanti europei. L'età minima richiesta dalla normativa è un requisito di validità del consenso e dunque di liceità del trattamento: i titolari di quest'ultimo, qualora l'utente dichiari di aver superato l'età del consenso digitale, debbano compiere "sforzi ragionevoli" e controlli appropriati, nonché proporzionati alla natura e ai rischi delle attività di trattamento, per verificare la veridicità dell'affermazione[62].

Annali italiani del diritto d'autore, della cultura e dello spettacolo (diretti da L.C. Ubertazzi), Milano, Giuffrè, 2011. Il tema è stato poi approfondito da C. Perlingieri, Profili civilistici dei social networks, Napoli, Esi, 2014.

[59] V. *supra* pag. 5.

[60] Nota 59.

[61] V. *supra* pag. 20-21.

[62] European Data Protection Board, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, versione 1.1., adottate il 4 maggio 2020.

Proprio perché nativi digitali, i più giovani sono in grado di eludere con estrema facilità le norme poste a tutela dei loro dati e perciò il Regolamento affronta il problema responsabilizzando il titolare del trattamento.

Nel Regolamento europeo, inoltre, vengono espressamente evidenziati in due specifici "Considerando", il Considerando 38 e il Considerando 58, i problemi legati all'inconsapevolezza dei minori relativamente ai rischi e alle conseguenze di far circolare i propri dati personali in un contesto così vasto e pericoloso come sono i social.

- Il Considerando 38 prevede espressamente che i minori "*meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali*.
- Il Considerando 58 è stato elaborato con l'intenzione di tutelare il minore nella comprensione del linguaggio, che deve essere idoneo nelle informative che vengono loro rivolte dato che "*i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente*" e dall'idea che il trattamento dei dati di un minore comporti, di per sé, rischi particolarmente rilevanti e tali da dover essere valutati con grande attenzione.

Per tutelare al meglio i minori e proteggere la sfera privata rispetto alla scelta delle regole del sito, è di importanza fondamentale quindi la presenza del genitore al momento della conclusione dell'accordo, cioè quando il giovane utente compila il relativo format e accetta tutte le clausole contrattuali che sono riportate nel sito.

Il Garante per la protezione dei dati personali in un opuscolo sui *social network* pubblicato nel 2009[63], intitolato "Attenzione agli effetti collaterali", ha evidenziato che le tecniche di tutela più efficaci sono quelle che si fondano sull'autodeterminazione e quindi su una gestione consapevole dei dati personali, propri e altrui.

[63] *Vademecum* sui *social network*, consultabile nel sito www.garanteprivacy.it, nel quale il Garante invitava alla prudenza e alla cautela: "Pensa bene prima di pubblicare i tuoi dati personali (soprattutto nome, indirizzo, numero di telefono) in un profilo-utente o di accettare con disinvoltura proposte di amicizia". "Astieniti dal pubblicare informazioni personali e foto relative ad altri senza il loro consenso. Potresti rischiare anche sanzioni penali". Si consiglia, ancora, in contrasto con le indicazioni contenute nei siti, di utilizzare pseudonimi differenti per ciascuna rete a cui si aderisce, omettendo di inserire la data di nascita o altre informazioni personali nel nickname.

I dati sui *social* infatti possono essere ripubblicati da altri utenti e indicizzati su motori di ricerca; sono potenzialmente destinati a rimanere intrappolati in rete e condannati a un eterno presente non controllabile e non più modificabile.

Inoltre lo sfruttamento commerciale delle informazioni personali, definite anche come il "nuovo petrolio della società digitale"[64], costituisce una delle principali attività delle imprese che forniscono servizi digitali.

Le informazioni sono una risorsa preziosa per gli interessi economici e commerciali del titolare della piattaforma, in quanto vengono utilizzate per indirizzare le prestazioni pubblicitarie all'interno del network.

Per tali ragioni i ragazzi vanno avvertiti del fatto che i propri dati personali rappresentano una parte della loro identità non solo virtuale, e che una volta immessi in rete, sfuggono alla possibilità di controllo, rendendo a volte quasi impossibile l'eliminazione completa di tutti i contenuti generati dall'utente: post, commenti, immagini, video, ecc...

I contenuti infatti restano in rete anche se si sceglie di disattivare l'account.

È in quest'ambito perciò che il GDPR, il Regolamento sulla protezione dei dati 2016/679, all'articolo 17 afferma fortemente nel sistema il Diritto alla cancellazione, il c.d. "diritto all'oblio"[65].

Tra le situazioni tassative in cui è possibile esercitare il diritto alla cancellazione dei dati è esplicitamente prevista l'ipotesi di illiceità del trattamento per violazione della regola contemplata all'articolo 8, che riguarda i dati raccolti relativamente all'offerta di servizi della società delle informazioni.

Per capire la portata di questa nuova regola è necessario tuttavia richiamare anche un altro Considerando del GDPR, il n. 65, nel quale viene espressamente precisato che "il diritto alla cancellazione dei dati acquista particolare rilevanza se l'interessato ha prestato il proprio consenso quando era minore e quindi non pienamente consapevole dei rischi derivanti dal trattamento".

In questi casi l'interessato deve poter essere messo in condizioni di procedere all'eliminazione, anche se ha raggiunto la maggiore età.

Gli utenti, in altri termini, potranno sempre esigere dal titolare del trattamento la cancellazione dei dati inseriti online quando ci sia stata violazione della regola contenuta all'articolo 8,

[64] Francesco Pizzetti, *Il prisma del diritto all'oblio*, in *Il caso del diritto all'oblio*, Torino, Giappichelli, 2013, pag.41.

[65] V. *supra* par 3.1. pag.30

relativa all'età minima necessaria per esprimere validamente in autonomia il consenso al trattamento dei dati effettuato dai siti di socializzazione.

3.3 La legge sul *cyberbullismo*

In Italia il riferimento giuridico più importante e innovativo per contrastare il *cyberbullismo* è la legge n. 71 del 29 maggio 2017[66], comunemente nota come la "Legge sul *cyberbullismo*".
L'iter della legge è stato travagliato: i due rami del Parlamento, la Camera dei Deputati e il Senato della Repubblica, hanno infatti avuto visioni contrapposte sulla sua natura.
Il Senato già nel 2014 annunciava i principi ispiratori di natura educativa e rivolti esclusivamente ai minori; la Camera voleva invece una legge di natura repressiva estesa agli adulti e al bullismo in generale.
Il testo approvato ha visto prevalere le ragioni del Senato; nell'ordinamento italiano esiste quindi una legge con misure prevalentemente a carattere educativo e rieducativo.
La legge si compone di sette articoli; l'essenza è la dignità del soggetto minore, sia esso vittima o carnefice.

- Art. 1: "Finalità e definizioni"
  L'obiettivo è di contrastare il *cyberbullismo* in tutte le sue manifestazioni, con azioni preventive e strategiche di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, con l'attuazione di interventi nell'ambito delle istituzioni scolastiche.
- Art. 2: "Tutela della dignità del minore"
  Viene inserita la possibilità per il minore almeno quattordicenne, o per i suoi genitori, di richiedere al titolare del trattamento dei dati l'oscuramento, la rimozione o il blocco di qualsiasi dato personale e, nel caso non ci fosse riscontro, la facoltà di ricorrere al Garante per la protezione dei dati personali.
- Art. 3: "Piano di azione integrato"
  È uno strumento di collaborazione e coordinamento per contrastare il *cyberbullismo*.
  Prevede il coinvolgimento di diverse istituzioni:
  - ✓ Autorità governative: la Presidenza del Consiglio dei Ministri, il Ministero dell'istruzione, dell'università e della ricerca (Miur), il Ministero della giustizia

[66] Legge 29 maggio 2017, n. 71, pubblicata in G.U. 3 giugno 2017, n. 127, recante *"Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"*.

- ✓ Autorità amministrative: il Garante per la protezione dei dati personali (Gpdp), l'Autorità per le garanzie nelle comunicazioni (Agcom), il Garante per l'infanzia e l'adolescenza
- ✓ la Polizia postale.

- Art. 4: "Linee di orientamento per la prevenzione e il contrasto in ambito scolastico"
  Le azioni di carattere preventivo coinvolgono soprattutto le Istituzioni scolastiche che devono individuare tra i docenti un proprio referente. Il suo ruolo è di coordinare le iniziative di prevenzione e di contrasto del *cyberbullismo* e quelle di carattere educativo attraverso programmi di sostegno.
- Art. 5: "Informativa alle famiglie, sanzioni in ambito scolastico e progetti di sostegno e di recupero"
  Questo articolo è una delle più importanti novità della legge; infatti è prevista l'informativa alle famiglie da parte del dirigente scolastico che venga a conoscenza di atti di *cyberbullismo* e quindi attiva "adeguate azioni di carattere educativo".
- Art. 6: "Rifinanziamento del fondo di cui all'articolo 12 della legge 18 marzo 2008, n. 48"
  Il Ministero dell'Economia e delle finanze può apportare variazioni al bilancio per sostenere il Fondo per il contrasto della pedopornografia su Internet e per la protezione delle infrastrutture informatiche di interesse nazionale.
- Art. 7: "Ammonimento"
  È prevista la procedura dell'ammonimento se non c'è stata querela o denuncia. Il questore "convoca il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale" e lo ammonisce: non applica quindi misure di carattere penale.

Le radici della legge per contrastare il *cyberbullismo* si possono rinvenire già nella nostra Costituzione, in particolare negli articoli 2 e 3.
Infatti l'articolo 2 recita: "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo… *omissis*… e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale".
L'articolo 3 inoltre afferma che "Tutti i cittadini hanno pari dignità sociale... *omissis*… È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona

umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese".

La legge scaturisce anche da alcuni antefatti significativi e propedeutici.

- 2007: Miur, Linee di indirizzo generali e azioni a livello nazionale per la prevenzione e la lotta al bullismo, poi richiamate dalla legge.
- 2007: Ministero dello Sviluppo Economico (Mise), Codice di Autoregolamentazione anti-*cyberbullismo* riconosciuto poi all'interno della legge 71 del 29 maggio 2017 all'articolo 3, comma 3, nel quale è previsto appunto "il codice di autoregolamentazione per la prevenzione e il contrasto del *cyberbullismo*, a cui devono attenersi gli operatori che forniscono servizi di *social network* e gli altri operatori in rete".
- 2015: Ministero dell'Istruzione, Ministero dell'Università e della Ricerca (Miur), Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al *cyberbullismo* nelle quali si sottolinea che "è fondamentale far comprendere la nozione basilare secondo cui la propria ed altrui sicurezza in rete non dipende solo dalla tecnologia adottata (software anti-virus, antimalware, apparati vari etc.) ma dalla capacità di discernimento delle singole persone nel proprio relazionarsi attraverso la Rete".
- 2015: la legge n. 107 (c.d. "buona scuola") all'articolo 1 comma 7 lett. h) evidenzia la necessità che gli studenti sviluppino delle "competenze digitali degli studenti, con particolare riguardo al pensiero computazionale, all'utilizzo critico e consapevole dei *social network* e dei media nonché alla produzione e ai legami con il mondo del lavoro".

Per quanto concerne la giurisprudenza in materia, questa non è ancora copiosa, data la relativamente recente entrata in vigore della legge.

La prima sentenza europea per atti di *cyberbullismo* è stata emessa dal Tribunale per i minorenni di Torino il 19 dicembre 2018.

Il fatto risale al 2013: alcuni ragazzi avevano diffuso un video su Facebook nel quale fingevano rapporti sessuali con una minore in evidente stato di alterazione dovuto ad alcol.

In seguito alla pubblicazione del video la ragazza aveva ricevuto in poco tempo 2.600 insulti via *social*.

Carolina non ha retto alla vergogna e al dileggio e si è suicidata gettandosi dal balcone di casa.

I cinque ragazzi responsabili sono stati rinviati a giudizio ottenendo la "messa alla prova", provvedimento attraverso il quale i minori sono stati affidati a esperti per un percorso rieducativo e riabilitativo.

I giudici hanno constatato il ravvedimento dei ragazzi, nel frattempo diventati maggiorenni, e quindi i reati sono cancellati perché la misura imposta ha adempiuto alla funzione rieducativa.
Anche a seguito di questo episodio è scaturita la necessità e l'urgenza di una legge sul *cyberbullismo*, fortemente voluta anche dal papà della ragazza suicida.
Altre sentenze, come quella del Tribunale di Sulmona e del Tribunale per i Minorenni di Caltanissetta, emesse sempre nel 2018, riguardano la responsabilità genitoriale[67].

3.4 La responsabilità genitoriale

In relazione ai problemi e ai rischi del mondo virtuale per i minorenni nativi digitali emerge un elemento sostanziale: la responsabilità dei genitori.
Il controllo genitoriale può esercitarsi attraverso il *parental control*, il "controllo dei genitori": strumento sempre più utilizzato nelle famiglie perché permette di scegliere e impostare appositi filtri ai contenuti digitali a cui i più piccoli possono accedere. I *parental control* si installano attraverso la creazione di un profilo utente personale del minore dal quale farlo connettere.
Gli strumenti di *parental control* sono dei filtri o dei blocchi che, una volta attivati costituiscono un valido aiuto per i genitori dei ragazzi minorenni.
Gli strumenti possono essere attivati con diverse modalità:

1. l'attivazione di *white list* che definiscono i contenuti e gli ambienti a cui il figlio o la figlia possono accedere
2. l'attivazione di *black list*, cioè una lista di siti o parole chiave di ricerca a cui viene proibito l'accesso.

I genitori quindi rivestono un ruolo chiave nella realizzazione dei diritti dei bambini in generale, e nell'ambiente del digitale in particolare.
È quindi fondamentale che i genitori nella cura dei figli in relazione all'ambiente digitale, forniscano informazioni, risorse e servizi di aiuto per i minori[68].
Per quanto concerne la giurisprudenza in materia, anche in questo caso, come nel *cyberbullismo*, non è ancora copiosa, data la relativamente recente entrata in vigore della legge.
In giurisprudenza ci sono due sentenze significative: quella del Tribunale di Sulmona[69] e quella del Tribunale per i Minorenni di Caltanissetta[70].

---

[67] V. *infra* pag. 39.
[68] Livingstone Sonia., Lievens Eva, Carr John, *Handbook for policy makers on the rights of the child in the digital environment*, Council of Europe, November 2020.
[69] Tribunale di Sulmona, Sez. Civ., 9.4.2018, n. 103.
[70] Tribunale per i minorenni di Caltanissetta, sentenza 8 ottobre 2019.

1. Sentenza del Tribunale di Sulmona, sezione civile, 9 aprile 2018, n. 103

È la prima sentenza che sancisce la responsabilità per "*culpa in educando*" ex art. 2048 c.c. dei genitori degli autori dei fatti illeciti e il risarcimento.

Un gruppo di minorenni, tramite un falso profilo sul *social network* Facebook, aveva diffuso e pubblicato, senza alcuna autorizzazione, una fotografia senza veli di una ragazza loro coetanea.

Tale foto era stata in precedenza realizzata e inviata dalla medesima a un conoscente, dietro richieste e insistenze di quest'ultimo, con la rassicurazione che nessun altro ne avrebbe preso visione.

Il giudice ha rilevato una carenza educativa da parte dei genitori dei ragazzi coinvolti, e i loro comportamenti sono stati ritenuti giudicati lesivi di diritti attinenti alla sfera della persona, costituzionalmente rilevanti e protetti (ex art. 2 della Costituzione), come il diritto alla riservatezza, alla reputazione, all'onore, all'immagine. Ha perciò condannato i genitori dei *cyberbulli* a risarcire i danni non patrimoniali patiti dalla vittima e dai suoi familiari.

Il Tribunale ha riconosciuto inoltre che dalla pubblicazione su Facebook della foto della ragazza era stata lesa anche la reputazione dei suoi genitori, in quanto "esposti alla critica sociale della comunità di appartenenza".

2. Sentenza del Tribunale per i minorenni di Caltanissetta, 16 luglio 2018

Ribadisce il "*culpa in educando*" dei genitori che omettano di impartire una adeguata educazione ai figli minori all'utilizzo dei mezzi di comunicazione telematici, in questo caso è stata la messaggistica telefonica istantanea usata in modo improprio: la diffusione tramite rete Internet di foto che ritraevano una minore nell'intimità.

Il giudice ha ravvisato a carico dei genitori gli stessi profili di responsabilità nella mancata verifica e controllo sull'effettivo recepimento, da parte dei loro figli minori, degli insegnamenti dati.

Nella sentenza si ribadisce l'obbligo giuridico di vigilanza e verifica dei genitori nella tutela della dignità dei minori, quali soggetti deboli, non sufficientemente maturi per un uso corretto dei mezzi telematici; la tutela peraltro è solennemente sancita dagli articoli 16 e 3 della Convenzione di New York 20 novembre 1989 sui diritti del fanciullo posti a garanzia del diritto dei minori a non subire interferenze illecite nella loro vita privata, in correlazione alla protezione del diritto alla dignità e all'onore, nonché al superiore interesse dei soggetti deboli in ogni procedimento giurisdizionale che li riguardi.

3.5 Intervista esclusiva alla Direttrice della Polizia postale e delle comunicazioni

Tra le numerose e lodevoli iniziative delle istituzioni nazionali a tutti i livelli ci sono quelle attuate dalla Polizia postale e delle comunicazioni, che con competenza e abnegazione svolge quotidianamente un compito di vigilanza e protezione a tutela dei diritti dei minori, in particolare per i reati online.
Una preziosa testimonianza è quella della Direttrice della Polizia postale dott.ssa Nunzia Ciardi, che ha rilasciato la seguente intervista esclusiva.

1) *Dott.ssa Ciardi, ad oggi quali sono i reati online più diffusi a discapito dei minori?*

   I reati che riguardano i minori sono molti. Vanno dall'adescamento alla pedopornografia, dal *cyberbullismo* inteso come fenomeno e tutti i reati a questo connessi, fino a tutte quelle forme di aggressione che troviamo anche negli adulti, che però per gli adolescenti e i bambini assumono un enorme rilievo come il *revenge porn*, lo *stalking*, la sostituzione di persona con il furto di profili. Insomma, è un piccolo universo di reati che riguardano i ragazzi.

2) *Una delle insidie del web di cui si è sentito parlare ultimamente sono le challenge pericolose sui diversi social network, mi viene in mente Tik Tok. Cosa può fare un adulto per evitare che il proprio figlio incorra in questi pericoli?*

   Una regola assoluta è difficile darla: dipende molto dalle fasce d'età coinvolte. In generale, i ragazzi in età molto precoce, spesso parliamo di bambini che sono vittime di reati in modo progressivamente più frequente, non andrebbero mai lasciati soli davanti a un dispositivo, soprattutto per un lungo tempo, perché il dispositivo si connette potenzialmente a un mondo vastissimo, quindi a una serie di immagini e situazioni estremamente rischiose. Basti pensare a un bambino piccolissimo che gioca o che sta facendo dei giochi scaricati sul proprio dispositivo: quante volte appare la pubblicità o un pop up attrattivo per il quale basta un click e si trova su un sito di tutt'altra natura rispetto al gioco che sta facendo. Pensiamo anche all'esposizione precoce alla pornografia che ha riconosciuto una serie di danni emotivi e neurologici nei ragazzi molto piccoli.
   La navigazione accompagnata perciò dovrebbe essere la regola nei bambini.

Il discorso è diverso per gli adolescenti, ai quali bisognerebbe comunque aver trasmesso un'educazione oltre che globale anche di determinate regole di convivenza civile, nella vita reale e in rete.

Occorrono inoltre regole per stare online, di navigazione sicura, di come si debba frequentare la rete, sull'anonimato o non anonimato.

Per i giovani è molto difficile ragionare in termini di proiezione nel tempo e nello spazio, perché sono portati a fare un ragionamento immediato: pubblico una foto adesso senza pensare che quella foto rimarrà nella rete e poi sarà difficilissimo toglierla. Quindi, se è una foto che potrà creare imbarazzo in futuro, dopo sarà molto difficile tornare indietro sulle proprie decisioni e non sarà possibile cancellarla.

Il ragionamento in prospettiva non è un atteggiamento naturale nei ragazzi; bisogna invece insegnare loro cosa potrebbe succedere nel tempo e che cosa significa la rete.

Questa è l'attività che noi come Polizia facciamo nelle scuole, dove ci rechiamo allo scopo di divulgare i criteri per una navigazione sicura e per sfruttare al massimo le potenzialità della rete senza rischiare di cadere in trappole che sono molto pericolose e molto dolorose.

3) *Parlando proprio di scuole, quali percorsi dovrebbero attivare al fine di ridurre i rischi?*

Le scuole dovrebbero rendersi conto che i ragazzi, pur essendo molto pratici sotto il profilo tecnico, spesso non hanno la preparazione psicologica per confrontarsi con un mondo difficile come la Rete. Occorrerebbe dar loro delle indicazioni e gli insegnanti devono essere degli adulti di riferimento. Mi rendo conto che in un campo come questo non sia facile, perché l'adulto spesso arretra di fronte a un mondo che conosce meno sotto un profilo tecnico.

Ritengo tuttavia che non serve una preparazione tecnica per insegnare e per dare ai ragazzi gli elementi necessari per un comportamento equilibrato sulla rete.

Vale la pena per tutti impegnarsi in una conoscenza quanto meno sommaria dei meccanismi della rete perché è un mondo in cui i ragazzi non devono essere lasciati soli.

4) *La pandemia, secondo lei, ha amplificato i rischi a cui sono esposti i ragazzi?*

Sicuramente la pandemia ha aumentato tutti i reati digitali, compresi quelli che vedono una vittimizzazione dei minori.

È chiaro che la rete è stata un supporto fondamentale in un momento doloroso come questo perché ci ha permesso di rimanere in contatto con i nostri affetti quando la realtà non ci ha consentito di farlo fisicamente. Ha permesso, ad esempio, la didattica a distanza, lo *smart working*, gli acquisti online. Tutto quello che non si poteva fare fisicamente lo si è fatto digitalmente.

Quindi, se da un lato la rete è stata una risorsa importantissima in un momento come questo, dall'altro lato ha comportato un aumento di ore di connessione e di occasioni per chi voleva approfittare in modo criminale di questa aumentata esposizione e quindi anche i reati sono cresciuti, forse sono gli unici reati che hanno avuto un forte aumento insieme alla violenza domestica.

I reati tradizionali hanno avuto una contrazione, mentre sul *cyber* si è avuta una dilatazione degli atti illeciti.

5) *Secondo lei, il legislatore dovrebbe introdurre norme più severe per arginare i rischi che corrono i giovani sul web?*

Le norme ci sono. Qualcuna forse andrebbe adattata meglio però non sono le norme il problema. Il problema è che si tratta di un mondo che sta cambiando molto velocemente e spesso sono proprio gli strumenti a disposizione che non sono così adattabili e così veloci al cambiamento.

Pensiamo ad esempio alla preparazione dei nostri operatori di Polizia, siamo costretti a una formazione costante perché i fenomeni mutano con grandissima rapidità e non hanno nascite graduali: in genere i fenomeni sulla rete esplodono, inoltre ci sono delle sfide che nascono all'improvviso, e piattaforme che nel giro di poco diventano utilizzatissime come nessun altro servizio riesce a fare.

È un mondo con cui bisogna confrontarsi con una mentalità diversa.

6) *Come opera la Polizia Postale per far rispettare le norme esistenti?*

In molti modi. La Polizia fa la sua attività di tipo classico, quella investigativa, quindi sostanzialmente individua gli autori di condotte illecite e lo fa in vari campi: la Polizia postale è competente in modo esclusivo o prevalente in alcune macroaree di riferimento quali la protezione delle infrastrutture critiche, la pedopornografia online e tutti i reati di

aggressione online, i crimini finanziari, il *financial cyber crime*, il terrorismo online, i reati sui *social network*.
Sono tutte aree di riferimento molto vaste in cui la Polizia postale esercita la sua attività specialistica perché è evidente che per contrastare determinati tipi di reati occorra una preparazione tecnica e specialistica di altissimo livello.
Dedichiamo una grandissima attenzione anche alla prevenzione perché riteniamo che in questo campo la prevenzione e soprattutto l'introduzione di una cultura dello stare in rete sia fondamentale.
È necessaria la prevenzione anche per difendersi dagli attacchi che subiscono le aziende ma in particolare è importante per i ragazzi, proprio perché trattandosi di minori la strada migliore è quella dell'educazione e della cultura di un uso consapevole della rete.

7) *A tal proposito, dott.ssa Ciardi, ha qualche consiglio da dare ai minori che subentrano in questa attività online spesso inconsapevoli dei rischi a cui vanno incontro?*

Bisogna pensare. Bisogna in qualche modo rinunciare se non del tutto ma in modo sensibile a quell'immediatezza che ci espone ai rischi. Di conseguenza quando pubblichiamo, anche quando mettiamo un *like* a un post aggressivo di un amico nei confronti di un altro, dobbiamo pensare al tipo di violenza, che fa del male.
Il fatto di stare dietro un dispositivo spesso ci fa sentire meno le conseguenze dei nostri gesti. Poiché siamo isolati in un contesto protetto non ci rendiamo conto delle conseguenze delle nostre azioni. Dobbiamo allenarci a fare questo tipo di esercizio. Non rinunciare a interagire, non rinunciare ai *social* e alle parti produttive e anche belle e affascinanti della rete però ragionare, pensare, proiettare nel futuro le nostre azioni e non cedere a quella istintualità che spesso ci fa ignorare i rischi.

Conclusioni

Igor, Antonella, Amanda, Carolina, sono i nomi dei ragazzi minorenni che purtroppo oggi non ci sono più a causa dei pericoli insiti nella rete.

Infatti i minori di oggi, nativi digitali, sempre più frequentemente sono le vittime dei pericoli generati dal mondo virtuale.

Le nuove generazioni crescono a contatto con la tecnologia ed è sempre più sfumata la linea che separa la vita online da quella offline. Le attività che i ragazzi, ma anche i bambini, svolgono online o attraverso gli strumenti tecnologici hanno, quindi, spesso conseguenze anche nella loro vita reale.

In molti casi si tratta di gravissime violazioni della reputazione, della dignità e, soprattutto, della sessualità - intesa come diritto fondamentale - dei minori, amplificati dall'uso delle tecnologie e, in particolare, dei *social network*.

Cyberbullismo, *cybergrooming*, pedopornografia online, *challenge* pericolose online quali *Blue Whale Challenge* e *Blackout Challenge*, possono trasformarsi in vere tragedie.

Il confine tra divertimento e pericolo si fa sempre più sottile.

Un uso dei *social* poco regolamentato può essere terreno fertile di insidie e di attività criminali.

L'intervento del legislatore e un'azione di coordinamento risultano indispensabili per limitare i rischi del minore nel web. Gli strumenti legislativi a tutela del minore ci sono.

Occorre una maggiore attenzione nell'educazione dei ragazzi e nel dialogo con loro in un ambiente online costruttivo che possa avere risvolti positivi anche nelle relazioni tradizionali.

È importante incoraggiare i giovani a sviluppare un pensiero critico e consapevole sulle opportunità ma anche sulle insidie e sulle trappole del web.

L'uso improprio e illecito di Internet e dei siti di socializzazione può ledere una pluralità di interessi costituzionalmente protetti ed essere fonte di gravissimi danni anche a lungo termine.

Tali danni possono condurre anche alla condanna dei genitori tramite il pagamento di un risarcimento economico alle vittime dei loro figli.

La sensibilizzazione dei genitori diventa fondamentale affinché prestino più attenzione ai comportamenti dei figli, in particolare rispetto al divertimento e al pericolo nel web.

BIBLIOGRAFIA

ASTONE Antonina, *I dati personali dei minori in rete. Dall'Internet delle cose all'Internet delle persone*, Milano, Giuffrè, 2019

Atti del Convegno "*Facebook et similia (profili specifici dei social network)",* Facoltà di Giurisprudenza, Pavia 30 settembre - 1° ottobre 2011. Pubblicati negli Annali italiani del diritto d'autore, della cultura e dello spettacolo (diretti da L.C. Ubertazzi), Milano, Giuffrè, 2011

BATTELLI Ettore (a cura di), *Diritto privato delle persone minori di età,* Torino, Giappichelli, 2021

DE SALVATORE Ferruccio, *Bullismo e cyberbulling, dal reale al virtuale tra media e new media*, in *Minorigiustizia*, n. 4, 2012, p.97.

ERAMO Federico, *Sulla criminalità informatica. Aspetti generali e ricadute sulla tutela dei minori dalle insidie telematiche,* in *Famiglia e Diritto*, 2009, p.93

LIVINGSTONE Sonia, LIEVENS Eva, CARR John, *Handbook for policy makers on the rights of the child in the digital environment,* Council of Europe, November 2020

O'CONNEL Rachel, *A typology of child cybersexploitation and online grooming practices*, *Cyberspace Research Unit University of Central Lancashire*, 2003

PIZZETTI Francesco, *Il prisma del diritto all'oblio*, in *Il caso del diritto all'oblio*, Torino, Giappichelli, 2013, p. 41

PERLINGIERI Carolina, *Profili civilistici dei social networks*, Napoli, Esi, 2014

PRENSKY Marc, *Digital Natives, Digital Immigrants*, *on the Horizon*, Lincoln: MCB University Press, 2001a, 2001b

RODOTA' Stefano, *Il diritto di avere diritti*, Roma-Bari, Editori Laterza, 2012, pp. 378 ss

SALTER Anna, *Predators: Pedophiles, Rapists, and Other Sex Offenders: Who They Are, How They Operate, and How We Can Protect Our Children*. New York: Basic Books, 2003

SALTER Anna, *Treating Child Sex Offenders and Victims: A Practical Guide*. Newbury Park, CA, Sage Publications, 1988

AGCOM, *Libro Bianco Media e Minori 2.0*, 2018

Dossier telefono azzurro, *Abuso sessuale e pedofilia. Storie, contesti e nuove sfide*, 2019

ISTAT, *Indagine conoscitiva sulle forme di violenza fra i minori e ai danni di bambini e adolescenti,* Commissione parlamentare per l'infanzia e l'adolescenza, Roma, 1° giugno 2020, p.11

Rivista di scienze sociale, *Infanzia e Adolescenza tra socialità e solitudine*, 2020.

Vademecum, I suggerimenti del Garante per tutelare la tua privacy quando pubblichi immagini online, Garante per la protezione dei dati personali, novembre 2020

SITOGRAFIA

https://www.agi.it/cronaca/news/2021-02-09/minori-aumentano-vittime-reati-online-11332868/ [ultimo accesso 10 aprile 2021]

https://www.altalex.com/guide/cyberbullismo> [ultimo accesso: 13 aprile 2021].

https://blog.linkem.com/challenge-da-fare/ [ultimo accesso: 16 aprile 2021]

https://www.Coe.int [ultimo accesso: 25 maggio 2021]

http://www.cyberbullismo.com/cyberbullismo/tipologie [ultimo accesso: 13 aprile 2021]

https://www.cyberlaws.it/en/2019/adescamento-minori-child-grooming [ultimo accesso 13 aprile 2021]

https://www.garanteprivacy.it [ultimo accesso: 25 maggio 2021]

https://www.icdemarchi.edu.it/newsite/smonta-il-bullo [ultimo accesso: 21 aprile 2021]

https://www.ilgiornale.it/news/cronache/nuovo-gioco-dellorrore-spopola-i-giovani-blue-whale-1371180.html

https://www.ilmessaggero.it/primopiano/cronaca/suicida_14_anni_ask_fm_bullismo-293475.html [ultimo accesso: 12 aprile 2021].

https://www.ilmessaggero.it/primopiano/esteri/blue_whale_gioco_ha_gia_portato_al_suicidio_130_adolescenti-2294375.html

https://www.labparlamento.it/garante-privacy-richiama-tik-tok-su-minori/

https://www.open.online/2021/02/03/caso-igor-maj-blackout-challenge-intervista-pm-cristian-barilli/

https://www.open.online/2020/02/22/skullbreaker-challenge-un-atto-di-bullismo-che-puo-uccidere-la-verifica-sui-tre-presunti-casi-di-morte

https://sociagency.it/vkontakte-vk-com-il-social-media-russo

https://www.scienzeforensi.org/blog/index.php?id=gcgnx70y

https://www.studiocataldi.it/articoli/41686-blackout-challenge-e-istigazione-al-suicidio.asp#par1

https://telefonoazzurro.it [ultimo accesso: 10 maggio 2021]

https://www.treccani.it [ultimo accesso: 10 aprile 2021]

https://www.theguardian.com/society/video/2013/aug/08/boycott-websites-david-cameron-video [ultimo accesso: 13 aprile 2021]

https://www.trend-online.com/tecnologia/boom-delle-challenge/

agendadigitale.eu/cultura-digitale/challenge-su-Internet-cosa-sono-e-come-difendersi

https://www.youtube.com/watch?v=vOHXGNx-E7E

NORMATIVA

Carta dei diritti fondamentali dell'unione europea (2016/C 202/02), 7.6.2016, in Gazzetta ufficiale dell'Unione europea C 202/389

Regolamento (UE) del 27 aprile 2016 del Parlamento europeo e del Consiglio 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

Legge 29 maggio 2017, n. 71, pubblicata in G.U. 3 giugno 2017, n. 127, recante *"Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"*

European Data Protection Board, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, versione 1.1., adottate il 4 maggio 2020

GIURISPRUDENZA

Tribunale di Torino, Sentenza 19 dicembre 2018

Tribunale di Sulmona, Sentenza 9 aprile 2018, n. 103

Tribunale per i minorenni di Caltanissetta, sentenza 8 ottobre 2019

ABSTRACT

Today's minors are, by definition, native digitals and easily relate to new technologies.
The typical child is increasingly focusing most of his everyday activities within the virtual world, bearing the risk of becoming a victim of serious issues on the web.
If on the one hand the Internet offers several possibilities, such as the chance to do some research incredibly easily and connecting with the outside world, on the other it also hides many pitfalls, especially for the youngest, who are the most vulnerable and with less tools to prevent and defend themselves from such dangers.
The aim of the thesis is to provide a general framework of the risks that minors face, including cyberbullying in all its different forms, such as cybergrooming and online pedopornography.
Some of these phenomena emerge in the real world but find a new space to manifest themselves in the virtual one. A striking example can be found in how bullying evolved into cyberbullying.
The second chapter analyzes an increasingly popular phenomenon among young people: online challenges. When discussing this phenomenon, there definitely is a fine line between the words "fun" and "danger". Online challenges are progressively spreading among children and teenagers; they come as a source of entertainment and are generally implemented with the creation of short videos of one person encouraging the other to repeat a particular action. Then the video is published on social media, especially on TikTok. Regarding this social network, the Italian Data Protection Authority has developed several initiatives to protect minors.
Unfortunately, these types of challenges come off as incredibly dangerous, rather than entertaining. The Blue Whale Challenge and the Blackout Challenge are two main examples of this type of phenomena that have turned into real tragedies. Luckily, there are tools to protect young people.
This chapter will also display a survey carried out among 200 minors aged from 12 to 17 years to understand their level of awareness of the risks they daily put themselves into. The results show an incredibly worrying situation in our country that is clearly underestimated.
The fundamental rights of the child are affirmed for the first time by the New York Convention of 20 November 1989. In addition to that, even in the Charter of Fundamental Rights, the principle contained in Article 7, which states that "everyone has the right to respect for his or her private and family life, home and communications", can be extended to minors.
Furthermore, in supranational legislation, the "General Data Protection Regulation" (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 has gained particular

importance for the protection of minors in the digital world; or "General Data Protection Regulation" (GDPR).

In Italy, the most important and innovative legal reference to counter cyberbullying is the law N. 71 of 29 May 2017, commonly known as the "Law on cyberbullying".

Finally, a substantial element emerges regarding the problems and risks of the virtual world for digital native minors: the responsibility of parents; they play a key role in the implementation of children's rights in general, and in the digital environment.