



Ente di Formazione, Didattica e Cultura



Università
degli Studi
della Campania
Luigi Vanvitelli

Corso di Alta Formazione in
Diritto e Problematiche Minorili

TESI

**IL CYBERBULLISMO
TRA OSCURAMENTO E AMMONIMENTO**

Relatore
Ch.mo Avv. Mario Covelli

Candidato
Dott. Pasquale Sticco

A.A. 2017/2018



Ente di Formazione, Didattica e Cultura



● Università
● degli Studi
● della Campania
Luigi Vanvitelli

Corso di Alta Formazione in
Diritto e Problematiche Minorili

TESI

**IL CYBERBULLISMO
TRA OSCURAMENTO E AMMONIMENTO**

Relatore
Ch.mo Avv. Mario Covelli



Candidato
Dott. Pasquale Sticco

A.A. 2017/2018

*A Carolina,
prima vittima acclarata di cyberbullismo.*

INDICE

	<i>pag.</i>
Introduzione	V

CAPITOLO I

Il fenomeno del cyberbullismo

1.	Premessa	1
2.	La Legge n. 71/2017: finalità e definizione di cyberbullismo	3
3.	Il (cyber)bullo	6
4.	La vittima di (cyber)bullismo	8
4.1.	La vittima passiva	8
4.2.	La vittima aggressiva	9
5.	Bullo e vittima: due facce della stessa medaglia?	11

CAPITOLO II

Gli strumenti di tutela

1.	Premessa	14
2.	L'istanza di oscuramento e il ruolo del Garante Privacy	16
3.	Il Piano di azione integrato	23
4.	Le linee di orientamento in ambito scolastico	26
5.	L'informativa alle famiglie	29
6.	Le risorse	30
7.	Il procedimento di ammonimento	31
7.1.	I "reati" presupposti e l'obbligo di denuncia ex art. 331 c.p.p.	34
7.2.	Le conseguenze dell'ammonimento e l'efficacia dell'istituto	37

CAPITOLO III
Le fattispecie di reato

1.	Premessa	39
2.	La sostituzione di persona	42
3.	L'ingiuria	45
4.	La diffamazione come manifestazione del cyberbullismo	49
5.	Cyberbullismo e reati in materia di pedopornografia	55
6.	Cyberbullismo e atti persecutori	57
7.	L'accesso abusivo a sistema informatico	60
8.	Trattamento illecito di dati personali e cyberbullismo	63
	Conclusioni	66
	Bibliografia	68

INTRODUZIONE

Con la legge 29 maggio 2017 n. 71, intitolata “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”, entrata in vigore il 18 giugno 2017, il legislatore italiano intende contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni.

Come sottolineato dal Sen. Palermo nella discussione parlamentare del 26.01.2017, si tratta di un provvedimento “non tecnicamente ma sostanzialmente quadro, poiché prevede una cornice all’interno della quale saranno altri soggetti a doversi muovere. Ed è questo che serve in un contesto di tal genere da parte del Parlamento, il quale deve creare le condizioni affinché, poi, gli attori sociali si mettano in rete e comincino a lavorare per elaborare politiche attive su questa materia”.

Il legislatore ha saggiamente abbandonato la prospettiva (prepotentemente emersa soprattutto con la versione del D.D.L. approvato dalla Camera dei Deputati nel settembre 2016) di inasprire la repressione penale del fenomeno e di estendere la portata applicativa delle norme, oltre le ipotesi di condotte tradizionalmente rientranti nel concetto di “bullismo”, anche a condotte riguardanti maggiorenni. Si puntava, in tal senso, a scavalcare lo spirito organico dell’impianto normativo, inteso in senso preventivo e responsabilizzante, che ponesse al centro l’opera degli istituti scolastici, delle associazioni e delle famiglie, per giungere, invece, ad incrementare gli aspetti repressivi di un fenomeno che ha, ormai, raggiunto dimensioni preoccupanti.

La legge approvata, tuttavia, non ricorre alla “novellazione” (o interpolazione) di norme preesistenti, ma tenta di offrire una regolamentazione unitaria del fenomeno, individuando la sua linea direttrice nella prevenzione piuttosto che nella repressione.

In particolare, l’art. 1 individua le finalità dell’impianto normativo, sottolineando la necessità di porre al centro dell’attenzione i minori coinvolti dal fenomeno del cyberbullismo, sia quelli che ne rappresentano le vittime, sia quelli che, invece, ne rappresentano i “soggetti agenti”. Lo stesso articolo, inoltre, offre per la prima volta una definizione normativa di cyberbullismo, inteso come “*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d’identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di*

dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.

L’ultimo comma dell’articolo in esame, poi, definisce il concetto di “*gestore del sito internet*”, un soggetto cardine nella nuova disciplina per la rimozione dei contenuti dalla rete Internet o il blocco dei trattamenti.

L’art. 2, significativamente rubricato “*tutela della dignità del minore*”, introduce la parte forse più innovativa della legge, ossia la possibilità, non solo per i genitori ma anche per ciascun minore ultra-quattordicenne che abbia subito un atto di cyberbullismo, di inviare al titolare del trattamento (o al gestore del sito o del social media) un’istanza per l’oscuramento, la rimozione o il blocco dei dati personali del minore diffusi in rete (previa conservazione degli originali), stabilendo dei tempi molto ridotti per l’adempimento.

Inoltre, la stessa norma contempla la possibilità, per il caso in cui il soggetto obbligato resti inadempiente (o laddove non sia possibile individuare il titolare o il gestore del sito), di richiedere – con segnalazione o reclamo – l’intervento del Garante per la protezione dei dati personali.

L’art. 3 prevede l’istituzione di un tavolo tecnico, per la prevenzione ed il contrasto del cyberbullismo, presso la Presidenza del Consiglio dei Ministri, senza nuovi o maggiori oneri a carico della finanza pubblica. Il predetto tavolo ha il cruciale compito di redigere, entro sessanta giorni dal suo insediamento, il piano di azione integrato per il contrasto e la prevenzione del cyberbullismo, cui devono attenersi gli operatori che forniscono servizi di social networking e gli altri operatori della rete Internet.

È previsto, infine, che il Ministero dell’Istruzione, dell’Università e della Ricerca, entro il 31 dicembre di ogni anno, trasmetta alle Camere una relazione sugli esiti delle attività svolte dal citato tavolo.

L’art. 4 prevede l’adozione di linee di orientamento per la prevenzione ed il contrasto in ambito scolastico (da aggiornarsi a cadenza biennale) da parte del Ministero dell’Istruzione, dell’Università e della Ricerca, sentito il Ministero della Giustizia,

anche avvalendosi della collaborazione della Polizia Postale e delle Comunicazioni. In particolare, la norma in esame definisce anche il contenuto delle suddette linee ed impone – altra disposizione innovativa – l’individuazione, in ogni istituto scolastico di un docente quale “*referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo*”.

Specifici commi sono, poi, dedicati alla promozione di bandi per il finanziamento di progetti elaborati da reti di scuole (tesi a promuovere sul territorio azioni integrate di contrasto del fenomeno in esame e l’educazione alla legalità), all’uso consapevole della rete nonché a specifici progetti personalizzati per sostenere i minori vittime di atti di cyberbullismo e rieducare i minori artefici di tali condotte.

L’art. 5 regola l’obbligo di informazione tempestiva alle famiglie da parte del dirigente scolastico nonché l’adeguamento dei regolamenti delle istituzioni scolastiche e del patto educativo di corresponsabilità, da attuarsi mediante specifici riferimenti alle condotte di cyberbullismo e l’introduzione di sanzioni disciplinari *ad hoc*, commisurate alla gravità degli atti.

L’art. 6 prevede una relazione annuale – a cura della Polizia Postale e delle Comunicazioni – sugli esiti delle misure di contrasto e contiene le norme in tema di risorse economiche (invero assai limitate).

L’art. 7, infine, estende (con delle peculiarità) l’istituto dell’ammonimento – di cui all’art. 8, commi 1 e 2 del D.L. 23 febbraio 2009, n. 11 – ad alcune condotte in materia di cyberbullismo.

Lungi da qualsivoglia ambizione di esaustività, il presente lavoro ha il mero intento di fornire al lettore uno sguardo di insieme su di una tematica ancora troppo silente.

CAPITOLO I

Il fenomeno del cyberbullismo

SOMMARIO: 1. Premessa - 2. La Legge n. 71/2017: finalità e definizione di cyberbullismo - 3. Il (cyber)bullo - 4. La vittima di (cyber)bullismo - 4.1. La vittima passiva - 4.2. La vittima aggressiva - 5. Bullo e vittima: due facce della stessa medaglia?

1. Premessa

Le statistiche nazionali stilate sulla base di campagne informative condotte dalla Polizia Postale e dalla Società italiana di Pediatria hanno rilevato dati allarmanti: 235 i casi di cyberbullismo trattati dalle Forze dell'ordine specializzate in reati informatici, di cui 88 quelli per minacce, ingiurie e molestie, 70 per furto di identità digitale sui social network, 42 le diffamazioni on-line, ben 327 le vicende di diffusione di materiale pedopornografico e 8 i casi in cui gli autori del reato erano giunti sino al cyberstalking.

Sono stati 31 i minori denunciati all'autorità perché ritenuti responsabili di fattispecie rientranti in questo novero¹.

Nel corso del congresso nazionale della Società italiana di Pediatria, tenutosi a Napoli a fine maggio 2017, sono stati presentati numeri molto simili: il 12% del campione intervistato – poco meno di dieci mila ragazzi tra i 14 e i 18 anni – è stato vittima cyberbullismo ed al 33% è capitato di subire atti di bullismo.

Identica la percentuale di coloro che hanno dichiarato di aver preso parte ad episodi di bullismo².

Tra questi numeri ne figurano alcuni che, se adeguatamente enfatizzati, fanno riflettere ma soprattutto fanno comprendere quanto urgente fosse l'intervento legislativo: anzitutto, ben il 68% delle vittime ha sostenuto di non aver mai parlato con nessuno di quanto stava subendo, e questo corrisponde al profilo della vittima

¹ “Una vita da social”, campagna della Polizia Postale contro il #cyberbullismo, 5 febbraio 2017.

² “I bambini crescono” – Minori: vittima di bullismo un ragazzo su tre, http://www.ilmattino.it/napoli/cronaca/napoli_pediatria_cyberbullismo – 2472546.

prediletta di bullismo: un/una ragazzino/a più immaturo degli altri, molto legato e dipendente dalle regole dei genitori, ai quali nulla racconta, vuoi perché si vergogna, vuoi per proteggerli dall'onta e dal dolore, secondo un meccanismo di ribaltamento dei ruoli molto diffuso.

Dall'altro lato, ben l'11% degli intervistati ha dichiarato di approvare gli insulti rivolti a personaggi famosi ed un ulteriore 13% ha confessato di essere stato lui stesso autore di commenti pesanti.

Un ulteriore sondaggio, affidato a Skuola.net e all'Università di Firenze, ha poi svelato che il 40% del campione ha dichiarato di trascorrere *on-line* più di cinque ore al giorno.

Numeri altissimi, che imponevano una risposta ferma, la quale a sua volta passa attraverso un imprescindibile molteplice approfondimento del fenomeno.

2. La Legge n. 71/2017: finalità e definizione di cyberbullismo

Con la legge n. 71 del 29 maggio 2017, intitolata *“Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”* (G.U. n.127 del 3 giugno 2017), entrata in vigore il 18 giugno 2017, il legislatore italiano ha risposto all’esigenza – sempre più drammatica – di *“contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni”*³.

La normativa in esame – una delle prime in Europa – si focalizza sui profili educativi e di prevenzione del cyberbullismo, introducendo sia strumenti di tutela dei ragazzi nel ruolo di vittima (l’istanza di oscuramento) sia strumenti di responsabilizzazione degli stessi nel ruolo attivo di bulli (l’ammonimento).

La legge ha il merito di richiamare l’attenzione su un tema complesso, di rafforzare il Patto educativo fra scuole e famiglie e di costituire un punto di partenza nel contrasto al fenomeno del cyberbullismo attraverso la previsione di un piano di azione integrato e di un Tavolo tecnico e di monitoraggio.

Il testo rafforza il ruolo ed il lavoro svolto dal Ministero dell’Istruzione, dell’Università e della Ricerca in materia di prevenzione e contrasto al cyberbullismo attraverso la formazione dei docenti, del personale Ata, l’adozione di specifiche linee guida, l’attenzione per l’educazione al corretto uso delle nuove tecnologie.

Le finalità del provvedimento sono illustrate all’art. 1, ai sensi del quale *“La presente legge si pone l’obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l’attuazione degli interventi senza distinzione di età nell’ambito delle istituzioni scolastiche”*.

La stessa norma, al secondo comma, contiene la definizione – prima ed unica nel nostro ordinamento – di cyberbullismo, che ricomprende *“qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d’identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un*

³ Art. 1, comma 1, L. n. 71/2017 in <http://www.normattiva.it>.

minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.

La sopra citata definizione, tuttavia, risulta carente rispetto agli elementi costitutivi del cyberbullismo, tradizionalmente individuati dalla ricerca e dalla dottrina italiana ed europea⁴, quali, ad esempio, lo squilibrio di potere e forza, la ripetizione dei comportamenti nel tempo.

La definizione contenuta nella legge rischia, pertanto, di ricomprendere fattispecie anche molto differenti dal cyberbullismo.

Difatti, secondo il richiamato art. 1, qualsiasi azione – anche l’invio di un solo sms o la pubblicazione di un post – potrebbe rientrare nella definizione di “cyberbullismo”, con il rischio concreto di aumento di conflitti e contenziosi.

Si osserva, poi, come l’elemento psicologico nell’intenzionalità degli episodi di cyberbullismo non sia finalizzato a “isolare la vittima”, quanto in realtà a mettere al centro la stessa vittima di uno spettacolo di prevaricazione e violenza, vittima che diventa – suo malgrado – protagonista involontaria⁵.

Inoltre, la richiamata definizione di cyberbullismo non cita in alcun modo il divieto di discriminazioni ed il principio delle pari opportunità, principi che dovrebbero ispirare le attività educative.

Il sopra citato principio di pari opportunità deve essere declinato non solo sotto il profilo dei rapporti fra uomini e donne, ma anche sotto i profili dell’orientamento sessuale, religioso, politico, età, razza e lingua.

Si osserva, infatti, come molteplici episodi di cyberbullismo, anche molto gravi, abbiano come vittime soggetti diversamente abili o soggetti omosessuali o in transizione di genere.

Il richiamo alle pari opportunità costituisce un profilo fondamentale in considerazione dell’impatto sociale del fenomeno del cyberbullismo e nell’ottica di inclusione dei ragazzi.

⁴ Olweus Dan, *Bulling at School: What we know, and what we can do*, 1996;
Barone Lucio, *Bullismo e cyberbullismo: riflessioni, percorsi di intervento, prospettive*, 2016;
Battaglia Adriana, *Cyberbullismo: il nuovo male oscuro*, Gorle Marna, 2016;
Berti Mauro, Valorzi Serena, Facci Michele, *Cyberbullismo: guida completa per genitori, ragazzi e insegnanti*, Reverdito, 2017.

⁵ Bassoli Elena, Russo Paolo, *Contrasto al cyberbullismo: una legge utile?*, in *Il Quotid. Giur.*, 2017.

La definizione contenuta nel testo di legge in esame non ricomprende, poi, i ragazzi e le ragazze che assistono a episodi di bullismo come spettatori, soggetti che risultano, secondo gli ultimi dati Istat, in forte aumento⁶.

Al riguardo, si evidenzia che per contrastare e prevenire questi fenomeni risulta imprescindibile coinvolgere anche questi soggetti nelle azioni di prevenzione, informazione e sensibilizzazione.

⁶ Istat, *Il Bullismo in Italia: comportamenti offensivi e violenti fra i giovanissimi*, dicembre 2015.

3. Il (cyber)bullo

Come ricordato dal Prof. Giovanni Ziccardi, nel momento in cui lo studioso si domanda come internet abbia cambiato il panorama del bullismo appaiono subito chiari alcuni aspetti.

Il primo, palese, è che prima della rete gli atti di bullismo terminavano quando la vittima usciva dall'ambiente nel quale si trovava – ad esempio la scuola – e si allontanava dalla fonte diretta delle minacce.

Oggi la dinamica è cambiata completamente, rendendo il fenomeno sia più difficile da contenere sia molto più complesso da ignorare⁷.

Cyberbullismo altro non è che bullismo messo in atto attraverso le nuove tecnologie e spesso colpisce chi è già vittima nella vita “di tutti i giorni”, col che non si sostiene affatto che il mondo di internet non sia “reale”; anzi, al contrario, soprattutto nell'adolescenza dei nativi digitali, per i quali l'approvazione ed il senso del gruppo dei pari permane con potenza eguale, a volte maggiore, quando ci si sposta dal cortile alla rete.

Chi ha già iniziato a predisporre azioni concrete per insegnare ai ragazzini a difendersi da attacchi informatici anche di cyberbulli, infatti, mette in guardia gli adulti dalla tentazione di consolare i figli minimizzando sull'importanza del web e di ciò che lì passa ed accade: per i giovani un commento su un *social network* è reale esattamente quanto un insulto ricevuto in corridoio a scuola.

Gli specchietti riassuntivi normalmente presenti nei libri di psicologia sono molto chiari sul punto quando descrivono le varie tipologie di bullismo: mentre durante i primi anni della scuola elementare – quindi dai 6 agli 8 anni di età dei protagonisti – sono presenti solo azioni di prevaricazione fisica (percosse, spintoni, danneggiamenti degli oggetti), verbale/psicologica (insulti, minacce...) e relazionale/psicologica (esclusione da parte del gruppo, manipolazione delle reti sociali di cui è intessuta l'accettazione sociale del prevaricato), quando ci si sposta nella fascia di età 9-12 anni a questi tipi si aggiungono molestie sessuali, aggressività nel rapporto di coppia e soprattutto cyberbullismo⁸.

⁷ Ziccardi Giovanni, *L'odio on-line. Violenza verbale e ossessioni in rete*, Cortina ed., 2016.

⁸ Zanetti Maria Assunta, Renati Roberta, Berrone Carlo, *Il fenomeno del bullismo, tra prevenzione ed educazione*, ED. Magi, 2015.

Un passaggio che risente dell'inevitabile traslazione degli interessi del/la ragazzo/a: dal gioco e dalla relazione personale, fisica, verso l'approdo al mondo digitale ed i suoi diversi criteri comunicativi.

Qui può acuirsi la generale sfiducia che la vittima coltiva per il mondo adulto, che lo accomuna al bullo, secondo quanto ancora una volta ci specificano gli esperti: quest'ultimo non si fida del genitore (e, quindi, gli tace come si comporta) perché teme di diventare oggetto di derisione ed aggressività verbale o fisica, si aspetta che reagisca contro di lui, così impedendogli di entrare in contatto con i propri aspetti di vulnerabilità, dei quali non riesce a farsi carico. Il bullo teme che le sue emozioni creino irritabilità nel genitore più che una vera preoccupazione, e manca di mentalizzazione, cioè della capacità di capire se stesso e gli altri in termini di emozioni, sentimenti ed intenzioni⁹.

Dal canto suo, nemmeno la vittima si rivolge al genitore per impedire che sia ferito dalla sua vulnerabilità e che questa ferita narcisistica possa dar luogo ad altre ulteriori situazioni di umiliazione, come rivolgersi direttamente al bullo, ai suoi genitori o alle autorità scolastiche.

⁹ Zanetti Maria Assunta, Renati Roberta, Berrone Carlo, *Il fenomeno del bullismo, tra prevenzione ed educazione*, ED. Magi, 2015.

4. La vittima di (cyber)bullismo

A questo argomento che, costituisce il cuore di questo capitolo, sarebbe davvero molto interessante poter dedicare un lavoro intero, se non altro perché la vittima è la figura più negletta tra tutti i soggetti del reato, o almeno lo era nella configurazione tradizionale del nostro sistema processual-penalistico tuttora in vigore.

Si fa fatica, molta fatica, ad introdurre in questo ingranaggio spazi di manovra e di tutela ulteriori e diversi rispetto agli scarsissimi mezzi già predisposti dal legislatore, e quelle poche evoluzioni rimodernanti che siamo riusciti ad ottenere negli ultimi anni derivano quasi esclusivamente dagli obblighi internazionali cui l'Italia ha dovuto adeguarsi.

In armonia col *modus procedendi* già adottato per l'autore di condotte di cyberbullismo, i paragrafi che seguono sono dedicati alla disamina del profilo della vittima, partendo dalla constatazione che quest'ultima presenta un insieme di caratteristiche che la contraddistinguono e permette di raggrupparla sostanzialmente in due fondamentali e differenti tipologie: la vittima passiva (o vittima sottomessa) e la vittima aggressiva (o vittima provocatrice).

4.1. La vittima passiva

La vittima passiva, o sottomessa, o vittima *tout court*, è così denominata perché subisce le prepotenze senza riuscire a difendersi. Tenzialmente è più ansiosa ed insicura degli studenti in generale; spesso è cauta, sensibile e calma.

Se attaccata da altri studenti, in genere questa vittima reagisce piangendo (almeno nelle prime classi) e chiudendosi in se stessa.

Generalmente soffre di scarsa autostima, ha un'opinione negativa di sé e della propria situazione, si considera spesso fallita e si sente stupida, timida e poco attraente. Solitamente vive a scuola una condizione di solitudine ed abbandono e non ha un buon amico in classe.

Non è un soggetto aggressivo né molesto, anzi spesso tiene un atteggiamento negativo verso la violenza e l'uso di mezzi violenti.

Secondo lo psicanalista italiano Cristiano Rocchi, nel suo rapporto con il bullo la vittima può sviluppare un meccanismo di identificazione ossia, sovrastata da un

potere schiacciante e fuori controllo, sottomettersi alla volontà dell'aggressore, abdicare, rinunciare alla propria persona, consegnandosi ed identificandosi esattamente con ciò che il bullo si aspetta e vuole.

Può giungere a sentire, da un lato, ciò che l'aggressore sente e, dall'altro, ciò che l'aggressore vuole, arrivando addirittura ad anticipare le mosse del bullo per minimizzare il danno ed avere maggiori possibilità di sopravvivenza.

Il suo atteggiamento e comportamento pare segnalare agli altri l'insicurezza, l'incapacità nonché l'impossibilità o difficoltà di reagire di fronte agli insulti ricevuti.

Ed invero, la principale reazione di questa vittima dinanzi a fenomeni di bullismo è il ritiro: questi bambini imparano a tenersi lontano da certi posti a scuola – ove è più frequente la vittimizzazione – e molte volte, a causa dell'evitamento che permea il loro funzionamento sociale, cominciano anche ad avere un declino nei loro risultati scolastici. Spesso incolpano se stessi per ciò che sta loro accadendo, rinforzando la propria percezione di essere inetti¹⁰.

Sembra siano carenti, peraltro, di efficaci strategie per prevenire e risolvere efficacemente i problemi emotivi e, una volta vittimizzati, non sono capaci di affrontare in modo adeguato le emozioni che derivano dalla situazione stressante e negativa, sperimentando frustrazione, senso di fallimento e traumi.

Nel bullismo, inoltre, sembra essere un dato costante la differenza di corporatura tra incube e succube, ovviamente a favore del primo; diversamente, una volta spostatisi on-line, sembra affievolirsi la possibilità che la goffaggine o la balbuzie – giusto per fornire qualche esempio – catalizzino le malevoli intenzioni del cyberbullo e veicolino un attacco.

4.2. La vittima aggressiva

Si definiscono vittime aggressive, o provocatrici, o ancora vittime/bulli, quelle che sono caratterizzate da una combinazione di entrambi i modelli reattivi, quello ansioso e quello aggressivo, a volte iperattivi, spesso con notevoli problemi di concentrazione, che comportano loro quel nervosismo e quella irritazione che di regola causa reazioni negative da parte di alcuni o, addirittura, di tutti i compagni.

¹⁰ Zanetti Maria Assunta, Renati Roberta, Berrone Carlo, *Il fenomeno del bullismo*, op. cit., pag. 43.

In tal caso, le dinamiche in cui si connoterà l'eventuale bullismo sono diverse da quelle viste poc'anzi; parimenti, anche le conseguenze sulla vittima a tratti si differenziano: ed invero, le vittime aggressive, pur presentando comunque depressione, ansia sociale, bassa autostima e rifiuto da parte dei pari, si distinguono dalle vittime passive perché, come i bulli, tengono comportamenti aggressivi ed antisociali.

Per certi autori¹¹ presentano caratteristiche tipiche dei bambini con disturbo da deficit d'attenzione ed iperattività; altri¹², invece, ne evidenziano la problematicità a prescindere dal coinvolgimento in episodi di bullismo.

Questi bambini sono sgraditi persino agli adulti, perché causano tensione ed irritazione e risultano ancora più isolati rispetto alle vittime passive – che trovano un minimo di solidarietà quantomeno tra le altre vittime – e questo li pone in una condizione di svantaggio sociale ancora più accentuata. Difatti, usano l'aggressività reattiva vuoi per combattere le prevaricazioni vuoi per riaffermarsi, in una girandola quasi infinita di alienazione e isolamento.

Come aggressori si qualificano “inefficaci” perché, a differenza dei bulli, i loro attacchi non comportano i risultati prefissi; come vittime, invece, si definiscono “ad alto conflitto”, per differenziarle dalla categoria delle passive che, come visto dianzi, esibiscono un atteggiamento sottomesso, altrimenti detto “a basso conflitto”¹³.

¹¹ Kumpulainen Kristiina, *Bullying and psychiatric symptoms among elementary school-age children*, in *Child Abuse and Neglect*, 1998.

¹² Schwartz D., *The aggressive victim of bullying. Emotiona and behavioral disregulation as a pathway to victimization by peers*, in J. Juvonen, S. Graham, New York, Guilford Press, 2001.

¹³ Perry D.G., Perry L.C. e Kennedy E., *Conflict and the development of antisocial behavior*, in C.U. Shantz, W.W. Hartup, Cambridge Univ. Press, 1992.

5. Bullo e vittima: due facce della stessa medaglia?

Il titolo è preso in prestito da un articolo¹⁴ che si propone di offrire alcuni indici rivelatori da cui un adulto – un genitore, in particolare – possa trarre il sospetto che al figlio stia capitando di venire preso di mira dai compagni: oscillazioni inaspettate nel rendimento scolastico, bruschi cambiamenti di abitudini o di umore, frequenti assenze scolastiche, anche di nascosto, rifiuto a tornare a scuola, mancanza di rapporti coi compagni, isolamento.

L'autrice ipotizza che, accanto alle tipologie già ricordate, possa esistere un terzo genere di possibile vittima, che non è né antipatica né debole o frustrata ma, esattamente all'opposto, che suscita gelosia per un'amicizia che può vantare, o invidia per il suo successo, e così via. Che sia in una parola "diversa" ma non perché straniera, o professante un'altra religione, ma perché più bella, fortunata e popolare. Ecco, probabilmente questa ulteriore profilazione si adatta molto bene al fenomeno quando ci si trasferisce in rete dove – come può immaginarsi – sono estremamente frequenti gli *hate speech*, le manifestazioni di odio *on-line*, rivolte dai ragazzi verso persone note, ma – al contempo – si registrano anche espressioni di attacco tra pari che si conoscono e si frequentano nella vita di tutti i giorni.

Si è visto, analizzando la vittima passiva, come possa sviluppare tratti che in psicanalisi identificano la figura dell'adolescente "come se".

Quest'ultimo è un soggetto all'apparenza normale, dalle capacità intellettive integre, con espressioni emotive apparentemente normali ma una disposizione del tutto passiva verso l'ambiente, con notevole prontezza a percepire i segnali del mondo esterno e a modellare, di conseguenza, se stesso ed il proprio comportamento¹⁵.

Le sue reazioni affettive sono "come se", ossia non autentiche. È un soggetto molto suggestionabile, in quanto passivo e con tendenza automatica all'identificazione, che però può nascondere quasi completamente la sua aggressività e la sua mitezza virare bruscamente in cattiveria aperta e così, da vittima, diventare bullo.

Una simile eventualità non è frequente, ma può accadere; come può accadere che – semplicemente – la vittima arrivi al limite della sopportazione e/o trovi la forza di

¹⁴ Mattioli Patrizia, *Il bullo e la vittima: due facce della stessa medaglia?* In *Il Fatto Quotidiano* del 29 gennaio 2016.

¹⁵ Senise Tommaso, *L'adolescente "come se"*, in www.spiweb.it, Rivista della Società Psicoanalitica italiana.

reagire alle prese in giro, alle offese, alle calunnie, reagisca e riesca ad avere la meglio sul bullo. E a quel punto, inspiegabilmente, le stesse persone che prima non erano mai intervenute (insegnanti, educatori, dirigenti scolastici, ecc.) di colpo lo facciano ma, a quel punto, contro la persona sbagliata. Sembra un paradosso, ma capita che sia la vittima a venir additata come bullo dopo che per mesi, o per anni, ha subito e patito: il bullo di un tempo diventa il povero ragazzo aggredito da un violento, quello malmenato solo perché scherzava un po'.

Questa situazione, nota come contro-bullismo, è variamente denunciata dalle fonti di informazione dell'ambiente scolastico: lì ne si parla con agra ironia, riconducendo comunque anche questa inaccettabile interversione dei ruoli alla tendenza, purtroppo molto diffusa, a mostrarsi indulgente verso chi commette crimini, anche gravi, e colpevolisti verso chi – dopo aver subito ingiustizia – finalmente reagisce¹⁶.

A questa situazione, tuttavia, non va parificato l'altro fenomeno – altrettanto studiato e presente – del controbullismo reale, ossia quel tentativo di imitazione dell'aguzzino che spinge la vittima a compiere atti di prevaricazione su altri coetanei.

Si è più volte detto, infatti, che nel bullismo i ruoli non sono chiari e definiti e possono evolvere e confondersi nel tempo, e questo è ancora più vero in rete. Secondo una stima presentata da Alexandra Hua alla Pediatric Academic Societies del 2016, chi è stato vittima di bullismo e cyberbullismo sviluppa il 38% di possibilità in più di trasformarsi a sua volta in aggressore¹⁷. Non si tratta solo di una reazione ai soprusi subiti, ma del comportamento che può sviluppare chi è più impulsivo, emotivo, insicuro, chi manca di abilità sociali e di capacità di *problem solving*, e spesso risulta segnato da disagi psicologici diversi.

Il controbullismo è certamente una conseguenza (negativa) del ritardo con cui si affronta un caso di bullismo o, peggio, della carenza di intervento sulla vittima a favore, magari, solo di manovre repressive e punitive sull'aggressore.

La materia del cyberbullismo, da questo punto di vista, risulta ancora più allarmante, in quanto lontana dagli occhi di insegnanti e genitori, serpeggiante sui display degli smartphone e incontrollatamente idonea a raggiungere migliaia di persone in pochi attimi.

¹⁶ In <http://www.educabimbi.it/quando-la-vittima-di-bullismo-reagisce>.

¹⁷ Cohen Children's Medical Center of New York studies on bullying, in <http://www.healthdesk.it/ricerca/bullismo/-quando-vittima-trasforma-carnefice>.

Lo scambio tra carnefice e vittima può essere subitaneo e costante, in un circolo vizioso sempre più stringente, che avvolge tutti, ma che può essere spezzato (forse solo) dagli spettatori.

CAPITOLO II

Gli strumenti di tutela

SOMMARIO: 1. Premessa - 2. L'istanza di oscuramento e il ruolo del Garante Privacy - 3. Il Piano di azione integrato - 4. Le linee di orientamento in ambito scolastico - 5. L'informativa alle famiglie - 6. Le risorse - 7. Il procedimento di ammonimento - 7.1. I "reati" presupposti e l'obbligo di denuncia ex art. 331 c.p.p. - 7.2. Le conseguenze dell'ammonimento e l'efficacia dell'istituto.

1. Premessa

La legge n. 71 del 29 maggio 2017 costituisce un fondamentale punto di partenza nel percorso di prevenzione e contrasto del cyberbullismo, finora privo di una normazione unitaria, in Italia come in Europa.

È una legge di diritto mite e partecipativo, che introduce nuovi strumenti di tutela e di responsabilizzazione nei confronti di soggetti di minore età.

In particolare, per la vittima prevede l'istanza di oscuramento; per gli autori di atti di cyberbullismo la procedura dell'ammonimento.

La legge in esame ha finalità preventive e non repressive, non demonizza Internet, che è uno strumento straordinario di conoscenza e condivisione dei nostri ragazzi, ed è coerente con le indicazioni contenute nella legge n.107/15 di riforma della scuola ed il Piano nazionale agenda digitale.

La pietra angolare del provvedimento è costituita, infatti, dall'educazione all'uso consapevole di internet, in un mondo sempre più connesso, complesso e veloce, dove non vi è più alcuna differenza tra on-line ed off-line, al fine di formare nuovi cittadini digitali.

Nel prevedere un piano strutturale di intervento in ogni ordine di scuola con l'istituzione della figura del referente avente il compito di coordinare le strategie e le iniziative in materia e la formazione per tutto il personale scolastico, il provvedimento prevede un'alleanza educativa non solo tra scuola e famiglia ma una sinergia educativa con la rete dei servizi territoriali.

Il tavolo permanente interministeriale, coordinato dal Miur, rappresenta la struttura a livello nazionale in cui elaborare il piano integrato sulla prevenzione, il contrasto e la cura ed elaborare gli aspetti regolamentari con le aziende digitali.

Il tavolo interministeriale incardinato alla Presidenza del Consiglio, poi, istituisce sistemi di studio e monitoraggio sul fenomeno, al fine di comprendere le origini, gli effetti e l'evoluzione del cyberbullismo, con la previsione di campagne informative di prevenzione e sensibilizzazione.

2. L'istanza di oscuramento e il ruolo del Garante Privacy

Come noto, la legge n. 71/2017 introduce una serie di misure di carattere educativo e formativo, finalizzate in particolare a favorire una maggiore consapevolezza tra i giovani del disvalore di comportamenti persecutori che, generando spesso isolamento ed emarginazione, possono portare a conseguenze anche molto gravi su vittime in situazione di particolare fragilità.

Tra le disposizioni introdotte ve ne sono alcune dirette a prevenire la propagazione e/o diffusione di immagini, informazioni e, più in generale, di file lesivi della personalità del minore attraverso la rete.

Si tratta, in particolare, dell'art. 2, ai sensi del quale il minore che abbia compiuto 14 anni e sia vittima di bullismo informatico (nonché ciascun genitore o chi esercita la responsabilità sul minore) può rivolgere istanza al gestore del sito internet o del *social media* o, comunque, al titolare del trattamento per ottenere provvedimenti inibitori e prescrittivi a sua tutela (oscuramento, rimozione, blocco di qualsiasi altro dato personale del minore diffuso in rete, previa conservazione dei dati originali).

Il titolare del trattamento o il gestore del sito internet o del *social media* deve comunicare, entro 24 ore dall'istanza, di aver assunto l'incarico e provvedere sulla richiesta nelle successive 48 ore. In caso contrario, ovvero nell'ipotesi in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del *social media*, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, che deve provvedere – in base alla normativa vigente – entro le successive 48 ore.

La disposizione deve essere correttamente interpretata per comprendere quali soggetti siano destinatari, in prima istanza, delle richieste di rimozione da parte dei minori, dei loro genitori o di chi esercita la responsabilità sugli stessi.

La legge sul cyberbullismo introduce, infatti, nel nostro ordinamento un principio di forte novità, in virtù del quale la responsabilità di rimuovere i contenuti lesivi è solo in capo a gestori e piattaforme che inseriscono i contenuti stessi: social network e gestori di web.

Da questo punto di vista, la legge circoscrive in maniera più precisa anche le definizioni che avevano fatto da sfondo al precedente tentativo di regolamentare il

tema in esame, *id est* il codice di autoregolamentazione del cyberbullismo approntato (solo in bozza, però) nel 2013 dal Ministero dello sviluppo economico.

L'art. 1 del Codice, infatti, indicava i seguenti soggetti tra i destinatari del provvedimento, prevedendo che “*Gli operatori che forniscono servizi di social networking, i fornitori di servizi on-line, di contenuti, di piattaforme User Generated Content e social network che aderiscono al presente Codice, di seguito denominati «aderenti», si impegnano ad attivare appositi meccanismi di segnalazione di episodi di cyberbullismo, al fine di prevenire e contrastare il proliferare del fenomeno*”¹.

La legge n. 71, peraltro, innova anche rispetto al Decreto Legislativo n. 70 del 2003, ossia il decreto sul commercio elettronico.

L'art. 1, comma 3, della legge in commento statuisce, infatti, che “ai fini della presente legge, per «gestore del sito internet» si intende il prestatore di servizi della società dell'informazione, diverso da quelli di cui agli articoli 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, che, sulla rete internet, cura la gestione dei contenuti di un sito in cui si possono riscontrare le condotte di cui al comma 2”, mentre il comma 2 dell'art. 2 – come visto dianzi – prevede l'obbligo di attivarsi solo per il gestore del sito internet o del *social media*.

Cambia, dunque, l'impostazione del decreto legislativo n. 70/2003 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico)² che, almeno nell'interpretazione che ne è stata fornita sinora dalle Autorità amministrative indipendenti (si pensi all'AGCOM in materia di rimozione di contenuti in grado di violare il diritto d'autore), avrebbe consentito di inviare richieste di rimozione anche a soggetti quali l'*access provider*, il *caching provider* o, in ultima analisi, anche l'*hosting provider*.

La legge sul cyberbullismo, in sostanza, ha escluso dal novero dei “gestori del sito internet”, e quindi dall'ambito di applicazione del provvedimento e dagli obblighi di rimozione del contenuto lesivo, gli *access provider* (cioè i *provider* che forniscono

¹ In http://www.sviluppoeconomico.gov.it/images/stories/documenti/codice_cyberbullismo_8%-20gennaio_2013.pdf.

² Morelli C., *Cyberbullismo: provider fuori dal raggio d'azione della legge*, in *Altalex* del 23 maggio 2017, <http://www.altalex.com/documents/news/2017/05/23/cyberbullismo>.

connessione ad Internet, come Vodafone o Telecom Italia), nonché i *cache provider*, cioè i *provider* che memorizzano temporaneamente siti web, e i motori di ricerca.

Rientrano, invece, nella definizione di “gestori del sito internet” tutti i fornitori di contenuti su Internet.

Secondo l’Ufficio Studi della Camera, che ha approntato due documenti nel corso del lungo iter di approvazione della legge (si tratta delle Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo – A.C. 3139 e abb. – Schede di lettura del 24 giugno 2015³ e del Dossier n. 315/1 – Elementi per l’esame in Assemblea – Seconda edizione 12 settembre 2016), la disposizione farebbe in modo di escludere una responsabilità delle tipologie di *provider* sopra richiamate per i contenuti memorizzati, in coerenza con il principio di non responsabilità affermato dagli artt. 15 e 16 del citato decreto legislativo⁴.

La ricostruzione operata, però, non convince per una pluralità di motivi: la prima è di ordine strettamente sistematico, in quanto la legge sul cyberbullismo introduce precise tipologie di soggetti, come si evince chiaramente dalle definizioni dell’art. 2, comma 2.

Si tratta, anzi, della prima norma italiana – e, probabilmente, europea – che stabilisce con precisione la categoria di soggetti ai quali inviare la richiesta di “*notice and action*”⁵.

Il responsabile è, dunque, un soggetto ben individuato, che ha una relazione certa con la violazione, e non una semplice connessione derivante, ad esempio, da un contratto di accesso ad internet; ne consegue che nel fuoco della norma si devono ricomprendere solo coloro che hanno un rapporto contenutistico con il file lesivo dell’identità del minore.

La novità normativa, pertanto, consente di circoscrivere con sufficiente precisione, quanto alle condotte che non hanno a che fare con la titolarità dei dati personali, i soggetti che sono destinatari degli obblighi, e costituisce un netto miglioramento delle interpretazioni astruse operate degli artt. 14, 15 e 16 della norma sul commercio

³ In <http://www.documenti.camera.it/leg17/dossier/pdf/gi0384.pdf>.

⁴ In <http://www.documenti.camera.it/leg17/dossier/pdf/gi0384.pdf>.

⁵ In <http://www.brunosaetta.it/internet/il-regolamento-agcom-e-la-direttiva-europea-notice-and-action.html>.

elettronico, in materia – ad esempio – di intervento dell'autorità per le garanzie nelle comunicazioni, in tema di diritto d'autore.

Alcune difficoltà possono sorgere, invece, in relazione all'individuazione del *webmaster* nei *social network*, nonché alla regolamentazione della richiesta di rimozione, ed obblighi conseguenti, in base alla disciplina presente e futura relativa al trattamento dei dati personali.

Da questo punto di vista, la disposizione ha prestato il fianco a diverse critiche sul ruolo dei soggetti obbligati ad adempiere e sulla figura del titolare del trattamento dei dati personali, mutuata dall'art. 4 del D.Lgs. n. 196/2003.

Difatti, l'individuazione di quest'ultimo non risulta così pacifica, specie laddove i dati siano raccolti da un soggetto, ma di fatto trattati da altri.

Quid iuris, poi, qualora il titolare non sia raggiungibile, ad esempio perché in uno Stato extra-Ue, ove non sia prevista clausola di reciprocità in ordine alla Direttiva 95/46/UE? Stesse perplessità suscita il riferimento al gestore del sito e ancor più del *social media*, strumenti questi ultimi notoriamente sottostanti alla giurisdizione estera.

Il riferimento all'art. 167 del D.Lgs. 196/2003, del resto, nasce già, per così dire, vecchio, non tenendo in considerazione i diversi illeciti previsti dal Reg. EU 27 aprile 2016, 2016/679 (“GDPR”) – già in vigore dal maggio 2016 ed operativo dal prossimo 25 maggio – che manda in soffitta il vecchio T.U. Privacy.

Tra l'altro, il Regolamento europeo stabilisce norme precise in tema di diritto all'oblio anche in relazione ai minori.

Il diritto all'oblio rientra nel diritto alla protezione dei dati personali, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, ove si afferma che “ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano”.

È il nuovo regolamento europeo a dettare la disciplina.

L'oblio non abbraccia solo le ipotesi di mera eliminazione dei dati, ma un definitivo dovere di astenersi, da parte del titolare, da ogni e qualsivoglia interessamento nei confronti di una persona, a maggior ragione se tale persona sia minore di età.

Un'attenzione maggiore al tessuto normativo di impatto avrebbe, forse, potuto evitare tale aporia⁶.

⁶ Bassoli E., *L'oggetto della disciplina*, in *Contrasto al cyberbullismo: una legge utile?*

Ulteriori dubbi sorgono in relazione al ruolo da attribuire ai soggetti privati incaricati di rimuovere i contenuti ed alla possibile funzione “censoria” che questi soggetti potrebbero essere chiamati ad esercitare sui contenuti in rete.

La norma potrebbe incoraggiare richieste di rimozione ritenute pericolose per la libertà di espressione in rete, ma soprattutto per gli stessi intermediari della comunicazione, che in tale quadro normativo diventerebbero gli sceriffi della rete, con tutte le conseguenze del caso, comprese le responsabilità collegate.

È per questo motivo, peraltro, che nella regolamentazione della disciplina del commercio elettronico, sottostante alla direttiva n. 31 del 2000, la Commissione Europea incoraggiò la collaborazione tra le parti al fine di giungere celermente alla rimozione dei contenuti illeciti.

Il tema è stato al centro di aspri dibattiti, anche nella regolamentazione del cyberbullismo, in quanto le organizzazioni per la difesa dei diritti hanno espresso il timore di scarso controllo sulla trasparenza di tali accordi nonché per la difficoltà di controllare le policy aziendali delle multinazionali che attuano procedure di rimozione.

Il giudizio sull’illiceità dei contenuti, infatti, a monte della rimozione, lasciato in balia di un dialogo tra il titolare dei diritti e un terzo alla contesa, cioè il provider, ha delle evidenti ricadute sui diritti dei cittadini⁷.

Si ripropongono sul cyberbullismo gli stessi dubbi che hanno accompagnato l’affermazione del diritto all’oblio, ossia il diritto dell’individuo ad essere dimenticato ed a salvaguardare il riserbo imposto dal tempo ad una notizia già resa di dominio pubblico.

Al riguardo, una politica “cauta” da parte dei motori di ricerca e la fissazione di diversi paletti da parte dell’Autorità Garante per la protezione dei dati personali, soprattutto in tema di interesse pubblico alla notizia, sembrano aver garantito un certo equilibrio tra le richieste indiscriminate di cancellazione e la tutela della personalità di chi richiede la rimozione.

Va ricordato che il Garante per la protezione dei dati personali assume un ruolo centrale nella nuova procedura di rimozione dei contenuti idonei ad essere sussunti nell’ampia definizione di “cyberbullismo”, per cui è lecito attendersi – come già

⁷ Bistolfi C., *Strumenti di tutela contro il cyberbullismo negli ordinamenti contemporanei e nelle policies dei social network*, in <http://www.tesi.eprints.luiss.it/13056/2/bistolfi-camilla-sintesi-2014.pdf>

avvenuto nel caso del diritto all'oblio – un ruolo particolarmente attivo di quest'ultima Istituzione nella definizione di linee guida per la detta rimozione.

Peraltro – come visto dianzi – ai sensi dell'art.2, comma 2, della legge in esame, “*qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile non abbia comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro quarantotto ore non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media*”, l'interessato può rivolgere analoga richiesta – mediante segnalazione o reclamo – proprio al Garante per la protezione dei dati personali, il quale, entro quarantotto ore dal ricevimento della richiesta, provvede ai sensi degli articoli 143 e 144 del citato decreto legislativo 30 giugno 2003, n. 196.

Del resto, l'Autorità è ben conscia del ruolo che la legge n. 71/2017 le attribuisce, e ciò risulta tanto più evidente dalle parole del Presidente Soro⁸: “l'Autorità si impegna a svolgere l'importante funzione di garanzia assegnatale dalla legge, nella consapevolezza sia delle oggettive difficoltà tecniche sia della necessità di risorse adeguate ai nuovi compiti”.

Certo è che nel settore dei social network il tema del “Giudice della verità” privato sembra riproporsi.

Ed in effetti la scoperta, nel maggio 2017, da parte dell'autorevole quotidiano britannico “The Guardian” dei c.d. “*facebook files*”, ovvero delle regole, che ai più sono risultate incomprensibili, che il *social network* adotta in occasione dell'inserimento (e rimozione) dei contenuti sulla piattaforma, ha dato in qualche modo corpo a questi timori⁹.

A tal proposito, le *Human rights guidelines for Internet Service Providers per la self-regulation*, redatte dal Consiglio d'Europa e basate sull'art. 10 della Convenzione Europea dei Diritti dell'Uomo, relativo alla libertà di espressione, sottolineano proprio questo pericolo¹⁰.

⁸ Relazione 2016 - Discorso del Presidente Antonello Soro, in <http://194.242.234.211/documents/10160/0/Relazione+2016+-+Discorso+del+Presidente+Antonello+Soro>.

⁹ “Facebook Files”, Guardian pubblica le “regole” del social network, in <http://www.notizie.tiscali.it/esteri/articoli/facebook/files-guardian-pubblica-regole-social-network-00001/>.

¹⁰ Consiglio d'Europa in cooperazione con la European Internet Service Providers Association (EuroISPA), H/Inf (2008) 9.

All'interno di queste linee guida si trovano una serie di disposizioni relative ai servizi di accesso, nella fornitura dei quali il provider è tenuto a garantire che gli utenti abbiano a disposizione informazioni sui potenziali rischi per i loro diritti, la loro sicurezza e la loro privacy *on-line*.

Il Consiglio d'Europa ammonisce che impedire l'accesso dell'utente al suo account costituisce una limitazione del suo diritto di accesso e di libertà di espressione/informazione. Pertanto, la disattivazione del profilo può essere disposta solo dalle forze dell'ordine nazionali o decisa per motivi legittimi e strettamente necessari, come una violazione degli obblighi contrattuali o di abuso intenzionale, mentre tutto ciò che riguarda i provvedimenti giuridici dipende dalle disposizioni del diritto dello stato.

Da questo punto di vista, va salutata con estremo favore la limitazione della tutela prevista dalla legge n. 71 a favore dei soli soggetti minori.

L'estensione indiscriminata a tutti i soggetti, ancorché maggiorenni, della possibilità di richiedere la rimozione (e conseguente obbligo per i gestori dei siti) operata dalla seconda lettura della legge alla Camera (poi eliminata) avrebbe determinato una vera e propria minaccia alla libertà di espressione in rete, data l'enorme platea di soggetti interessati ad eventuali rimozioni¹¹.

Da questo punto di vista sarebbe stato praticamente impossibile, in caso di allargamento a soggetti maggiori di età, distinguere – ad esempio, in caso di diffamazione – le richieste strumentali da quelle meritevoli di tutela.

In casi come questi il ricorso all'Autorità giudiziaria e le norme esistenti appaiono essere l'unico modo di apporre un filtro a richieste che possono compromettere la libertà di espressione in rete, mentre all'opposto una rapida definizione della questione, in caso di soggetti minorenni, sembra essere la strada migliore al fine di proteggere i diritti del minore.

È per questo, peraltro, che la presenza di codici di auto-regolamentazione, prevista in origine nella disposizione sul cyberbullismo, ha lasciato spazio alla c.d. co-regolamentazione, secondo quanto previsto dall'art. 3, comma 3, della legge n.71.

¹¹ Meazza L.N., *Cyberbullismo e bullismo, proposta di legge approvata alla Camera*, in *Giurisprudenza Penale Web*, 2016, 9.

3. Il Piano di azione integrato

La legge n. 71/2017 prevede una complessa fase esecutiva della strategia di prevenzione del cyberbullismo attraverso l'attivazione di un tavolo tecnico e l'adozione di un piano di azione integrato nonché una relazione annuale sugli esiti delle attività svolte dal tavolo stesso.

E', infatti, prevista la pronta adozione di un decreto con il quale viene istituito, presso la Presidenza del Consiglio dei Ministri, il tavolo tecnico per la prevenzione ed il contrasto al cyberbullismo, formato da rappresentanti dei Ministeri dell'Interno, dell'Istruzione, del Lavoro, dello Sviluppo Economico e Sociale, della Giustizia, della Salute, della Conferenza Unificata, dell'Autorità per le garanzie nelle comunicazioni, del Garante per l'infanzia e l'adolescenza, del Comitato di applicazione del codice di autoregolamentazione media e minori nonché del Garante per la protezione dei dati personali.

La composizione del Tavolo ricomprende anche rappresentanti di associazioni con comprovata esperienza nella promozione dei diritti dei minori e degli adolescenti e nelle tematiche di genere, degli operatori che forniscono servizi di social networking e degli altri operatori della rete internet, una rappresentanza delle associazioni studentesche e dei genitori, nonché una rappresentanza delle associazioni attive nel contrasto del bullismo e del cyberbullismo.

La legge specifica che il sopra citato Tavolo è istituito senza nuovi o maggiori oneri a carico della finanza pubblica e che ai soggetti che partecipano ai lavori non è corrisposto alcun compenso, indennità, gettone di presenza, rimborso spese o emolumento comunque denominato.

Si osserva come nel testo approvato alla Camera, poi espunto al Senato, veniva specificato che il tavolo era formato da *“esperti dotati di specifiche competenze in campo psicologico, pedagogico e delle comunicazioni sociali telematiche, nominati dalla Presidenza del Consiglio dei ministri”*. In realtà, il riferimento alle competenze psicologiche e pedagogiche è certamente strategico nella prevenzione e contrasto al cyberbullismo, e si può auspicare che, in fase attuativa, venga recuperato con l'attivazione di convenzioni con Università, centri di ricerca e ordini professionali di psicologi, pur nella consapevolezza che tali convenzioni non potranno che essere a titolo gratuito, viste le limitazioni di budget o, meglio, la sua assenza.

Il sopra citato Tavolo, coordinato dal Ministero dell'Istruzione, Università e Ricerca, ha il cruciale compito, entro sessanta giorni dall'insediamento, di adottare un piano di azione integrato per il contrasto e la prevenzione al cyberbullismo, nel rispetto delle direttive europee in materia e nell'ambito del programma pluriennale dell'Unione Europea, di cui alla decisione 1351/2008/CE del Parlamento Europeo e del Consiglio del 16 dicembre 2008.

Il sopra citato piano di azione deve prevedere iniziative di informazione e di prevenzione del cyberbullismo rivolte ai cittadini, con il coinvolgimento dei servizi sociali presenti sul territorio in sinergia con le scuole.

Nell'ambito del sopra citato Piano, la Presidenza del Consiglio dei Ministri, in collaborazione con il Ministero dell'Istruzione, dell'Università e della Ricerca e con l'autorità per le garanzie nelle comunicazioni, predispone, nei limiti delle – scarsissime – risorse indicate all'art. 4, settimo comma, periodiche campagne informative di prevenzione e sensibilizzazione sul fenomeno in esame, avvalendosi dei principali media, nonché degli organi di comunicazione e di stampa e di soggetti privati.

Il profilo della comunicazione è strategico nella prevenzione e contrasto del cyberbullismo; si auspica la promozione di contesti ed il coinvolgimento diretto dei ragazzi in queste attività, al fine di una maggiore efficacia e resa.

La legge prevede, altresì, che il tavolo sopracitato deve realizzare un sistema di raccolta di dati finalizzato al monitoraggio dell'evoluzione dei fenomeni e, anche avvalendosi della collaborazione con la Polizia Postale e delle Comunicazioni e con altre Forze di Polizia, al controllo dei contenuti per la tutela dei minori.

La mancanza di dati validati e certi in materia di cyberbullismo costituisce, infatti, una grave carenza di sistema del nostro paese; senza dati e informazioni diventa molto difficile interpretare ed avere una visione del fenomeno, così da adottare strumenti efficaci di prevenzione e contrasto.

I dati dovrebbero essere pubblicati on-line in forma aggregata al fine di favorire il riutilizzo delle informazioni per finalità di ricerca. Si segnala, al riguardo, come l'art. 6 della legge in commento preveda, altresì, la pubblicazione in formato aperto della relazione annuale resa dalla polizia postale al tavolo tecnico sugli esiti delle misure di contrasto al fenomeno in esame.

Inoltre, la legge prevede che tale piano di azione sia integrato da un codice di coregolamentazione per la prevenzione e il contrasto del cyberbullismo¹², cui devono attenersi gli operatori che forniscono servizi di social networking e gli altri operatori della rete internet.

Attraverso il predetto codice è istituito un comitato di monitoraggio al quale è assegnato il compito di identificare procedure e formati standard per l'istanza di cui all'art. 2, comma 1, nonché di aggiornare periodicamente, sulla base delle evoluzioni tecnologiche e dei dati raccolti dal tavolo tecnico di cui all'art. 3, comma 1, la tipologia dei soggetti ai quali è possibile inoltrare la medesima istanza secondo modalità disciplinate con il decreto del Presidente del Consiglio dei Ministri di cui al medesimo art. 3, comma 1, della L. n. 71/2017.

La legge prevede, altresì, l'obbligo del Ministero dell'Istruzione, dell'Università e della Ricerca di trasmettere alle Camere, entro il 31 dicembre di ogni anno, una relazione sugli esiti delle attività svolte dal citato Tavolo tecnico.

Siffatta previsione costituisce un importante obbligo di rendicontazione nell'ottica di *accountability*. Si evidenzia, tuttavia, come non sia stata prevista, purtroppo, la pubblicazione della summenzionata relazione on-line – e in un formato aperto – al fine di garantire la massima trasparenza e condivisione.

¹² Si segnala che nel 2014, da parte del Ministero per lo Sviluppo Economico, è stata presentata la proposta di adozione di un Codice di Autoregolamentazione per la prevenzione ed il contrasto del fenomeno del cyberbullismo ed è stata anche promossa una consultazione pubblica on-line; il percorso di elaborazione del codice, tuttavia, non ha prodotto alcun testo definitivo.

4. Le linee di orientamento in ambito scolastico

Uno dei punti di forza della nuova legge è costituito dal profilo della prevenzione nell'ambito scolastico.

L'art. 4, rubricato "Linee di orientamento per la prevenzione e il contrasto in ambito scolastico" conferma e rafforza, al riguardo, la strategia ed il lavoro svolto dal Ministero dell'Istruzione, dell'Università e della Ricerca.

Al fine di rendere più efficace la prevenzione ed il contrasto al cyberbullismo su tutto il territorio nazionale, è prevista – tra l'altro – l'adozione da parte del Ministero dell'Istruzione, dell'Università e della Ricerca di specifiche linee di orientamento, l'individuazione, in ogni istituto scolastico, di un referente con il compito di coordinare le iniziative nonché la promozione del ruolo attivo degli studenti e la loro educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche.

Il testo si muove nel solco del lavoro svolto dal Miur, che già nel 2015 ha adottato specifiche linee guida in materia¹³, strumento prezioso per accompagnare le scuole, le famiglie e i ragazzi nel complesso percorso di prevenzione e contrasto del bullismo e cyberbullismo.

La legge in commento specifica gli elementi essenziali delle nuove linee di orientamento per il triennio 2017-2019 conformemente a quanto previsto dalla legge 13 luglio 2015 n. 107 (c.d. "La Buona Scuola") che, all'art. 1, comma 7, lettera D), tra gli obiettivi formativi prioritari individua proprio la prevenzione ed il contrasto di ogni forma di discriminazione e bullismo, anche informatico.

Inoltre, al fine di meglio comprendere il contesto delle sopra citate linee guida, giova ricordare che il Ministero dell'Istruzione, dell'Università e della Ricerca ha adottato e presentato, in data 16 ottobre 2016, il *Piano nazionale per prevenire e combattere il bullismo e cyberbullismo in classe*¹⁴.

Tale piano prevede dieci azioni mirate tra le quali: l'istituzione della giornata nazionale in materia di bullismo e cyberbullismo del 7 febbraio 2017 in coincidenza

¹³ Ministero dell'Istruzione, dell'Università e della Ricerca, *Linee di orientamento per azioni di prevenzione e contrasto al bullismo e al cyberbullismo* (13 aprile 2015), consultabile al link: http://www.istruzione.it/allegati/2015/2015_04_13_16_39_29.pdf.

¹⁴ Ministero dell'Istruzione, dell'Università e della Ricerca, *Piano nazionale per la prevenzione del bullismo e cyber-bullismo a scuola*, anno 2016, consultabile al link: http://www.istruzione.it/allegati/2016/Piano_azioni_definitivo.pdf.

con la giornata europea della sicurezza in rete indetta dalla Commissione Europea (*Safer Internet Day*); la promozione di una campagna nazionale “*Il nodo Blu contro il bullismo*”; il rafforzamento della formazione dei docenti e delle attività in collaborazione con la Polizia di Stato, con Save the Children e con Telefono Azzurro; il progetto “*Generazioni connesse*” ed il progetto “*Verso una scuola amica*” finalizzato ad attivare prassi educative sull’art. 29 (diritto all’educazione) della Convenzione sui diritti dell’infanzia e dell’adolescenza.

Peraltro, la prevenzione del bullismo e del cyberbullismo costituisce una delle linee prioritarie delle attività previste nell’ambito del *Piano Nazionale di Formazione dei docenti*, presentato il 3 ottobre 2016, che prevede il coinvolgimento di circa sedicimila docenti, delle scuole di ogni ordine e grado, in attività di formazione, con “lezioni” ad hoc per favorire l’acquisizione di competenze psico-pedagogiche e sociali in materia.

Ciò posto, una delle novità più interessanti della legge n. 71/2017 è costituita dalla previsione, presso ogni scuola, di un referente in materia di cyberbullismo.

L’art. 4, comma 3, prevede, infatti, che ogni istituto scolastico, nell’ambito della propria autonomia, debba individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo.

Alla luce della complessità e delicatezza dei compiti del referente, risulta imprescindibile per tale figura una formazione ed un aggiornamento interdisciplinare che ricomprenda materie come il diritto, l’informatica, la pedagogia, la psicologia e l’educazione all’uso consapevole di internet.

Il sopra citato referente, infatti, dovrà costituire il motore attivo delle iniziative in materia di cyberbullismo e non potrà non avere delle capacità relazionali, di ascolto e di assertività.

La previsione di un referente costituisce – senza alcun dubbio – un presidio importante nella prevenzione e contrasto del cyberbullismo, ma tali attività richiedono inevitabilmente risorse.

Al riguardo, l’art. 4, comma 4, prevede che “*gli uffici scolastici regionali promuovono la pubblicazione di bandi per il finanziamento di progetti di particolare interesse elaborati da reti di scuole, in collaborazione con i servizi minorili dell’Amministrazione della giustizia, le prefetture - Uffici territoriali del Governo,*

gli enti locali, i servizi territoriali, le Forze di polizia nonché associazioni ed enti, per promuovere sul territorio azioni integrate di contrasto del cyberbullismo e l'educazione alla legalità al fine di favorire nei ragazzi comportamenti di salvaguardia e di contrasto”.

In altri termini, la legge invita gli uffici scolastici ad agevolare e valorizzare, in questo complesso percorso, il coinvolgimento di ogni altra istituzione competente, ente o associazione, operante a livello nazionale o territoriale, nell'ambito delle attività di formazione e sensibilizzazione.

In particolare, la previsione del ruolo delle associazioni, nel rispetto del principio di sussidiarietà, è da ritenersi fondamentale, anche al fine di non disperdere un patrimonio informativo e professionale ed alla luce delle implicazioni sociali del fenomeno del cyberbullismo.

Infine, merita menzione il comma 5 dell'articolo in commento, che richiama l'attenzione sull'obbligo delle istituzioni scolastiche – conformemente a quanto previsto dalla lettera *h*) del comma 7 dell'art. 1 della legge 13 luglio 2015, n. 107 – di promuovere, nell'ambito della propria autonomia e delle risorse disponibili a legislazione vigente, l'educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche, quale elemento trasversale alle diverse discipline curriculari, anche mediante la realizzazione di apposite attività progettuali aventi carattere di continuità tra i diversi gradi di istruzione o di progetti elaborati da reti di scuole in collaborazione con enti locali, servizi territoriali, organi di polizia, associazioni ed enti.

5. L’informativa alle famiglie

L’art. 5 della legge n. 71/2017, rubricato “*Informativa alle famiglie, sanzioni in ambito scolastico e progetti di sostegno e di recupero*” prevede che, salvo che il fatto costituisca reato, il dirigente che venga a conoscenza di atti di cyberbullismo debba informarne tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti ed attivare adeguate azioni di carattere educativo.

Sul punto, è opportuno sottolineare che la previsione in esame non costituisce una novità ed infatti è espressamente specificato che tale azione debba essere attuata in applicazione della normativa vigente e dei regolamenti degli istituti scolastici.

Quanto alle citate azioni di carattere educativo, si osserva che le stesse dovrebbero avere natura preventiva, così da anticipare – e, nei limiti del possibile, scongiurare – il verificarsi del fenomeno in esame.

Parimenti, si segnala che se non sono stabiliti canali specifici per la segnalazione degli episodi di cyberbullismo, si rischia di non registrarne alcuna; pertanto, sarebbe opportuno uniformare le procedure a livello nazionale attraverso le linee guida Miur.

Ciò posto, è d’uopo evidenziare che la presente procedura non trova applicazione nell’ipotesi in cui il dirigente scolastico venga a conoscenza di reati perseguibili d’ufficio; in tal caso, infatti, incombe su quest’ultimo l’obbligo di denuncia, conformemente a quanto disposto dall’art. 331 c.p.p.

Infine, è doveroso sottolineare che la norma in commento, al secondo comma, richiede di integrare i regolamenti delle istituzioni scolastiche ed il patto educativo di corresponsabilità (di cui all’articolo 5 bis del decreto n. 249 del 1998) con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.

6. Le risorse

L'art. 6 della legge in esame, rubricato "*Rifinanziamento del fondo di cui all'articolo 12 della legge 18 marzo 2008, n. 48*", prevede l'obbligo della Polizia Postale e delle Comunicazioni di relazionare con cadenza annuale al tavolo tecnico di cui all'art. 3, comma 1, sugli esiti delle misure di contrasto al fenomeno del cyberbullismo.

La relazione – come visto dianzi – è pubblicata in formato di tipo aperto ai sensi dell'articolo 8, comma 3, lettera *a*), del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.

Lo stesso art. 6, al secondo comma, specifica che per le esigenze connesse allo svolgimento delle attività di formazione in ambito scolastico e territoriale, finalizzate alla sicurezza dell'utilizzo della rete internet e alla prevenzione e al contrasto del cyberbullismo, sono stanziati ulteriori risorse pari a 203.000 euro per ciascuno degli anni 2017, 2018 e 2019, in favore del fondo di cui all'articolo 12 della legge 18 marzo 2008, n. 48.

Inoltre, ai sensi dell'art. 3, comma 7, la legge in commento prevede uno stanziamento di 50.000 euro annui per le campagne periodiche di prevenzione e sensibilizzazione predisposte dalla Presidenza del Consiglio dei Ministri.

Tuttavia, in considerazione della dimensione del fenomeno e del numero degli Istituti coinvolti, le risorse stanziati sono oggettivamente esigue.

7. Il procedimento di ammonimento

La legge n. 71/2017 – come noto – ha avuto un iter decisamente tormentato.

Da tale accidentato percorso è stato sostanzialmente risparmiato l'art. 7, arrivato all'approvazione in maniera (quasi) indolore.

La norma prevede che, prima che sia proposta querela o presentata denuncia per taluno dei reati di cui agli artt. 594 (norma, in realtà, abrogata dal D.Lgs. n. 7/2016), 595 e 612 c.p. e all'art. 167 D.Lgs. 196/2003, commessi mediante la rete internet da minori ultraquattordicenni (il riferimento era inevitabile, corrispondendo alla soglia di imputabilità per i soggetti minori), si possa applicare la procedura dell'ammonimento, introdotto dall'art. 8, commi 1 e 2, del decreto legge 23 febbraio 2009, n. 11.

Si ricorda che anche il minore (purché non infraquattordicenne) è titolare del diritto di querela, ai sensi dell'art. 120 del codice penale; diritto che, peraltro, può essere esercitato anche dal genitore, nonostante ogni contraria dichiarazione di volontà, espressa o tacita, del minore stesso.

La procedura di ammonimento, descritta nel citato art. 8, commi 1 e 2, è piuttosto semplice: la persona offesa espone i fatti all'autorità di pubblica sicurezza, avanzando contemporaneamente al Questore richiesta di ammonimento nei confronti dell'autore della condotta. A seguito della richiesta (che deve essere trasmessa "senza ritardo"), il Questore, assunte se necessario informazioni dagli organi investigativi e sentite le persone informate dei fatti, accoglierà la richiesta ove la ritenga fondata, provvedendo ad ammonire oralmente il soggetto nei cui confronti è stato richiesto il provvedimento, invitandolo a tenere una condotta conforme alla legge. Di tale ammonimento (ancorché orale) è redatto un processo verbale, che viene rilasciato in copia sia al richiedente l'ammonimento che al soggetto ammonito. Con riferimento a questa procedura, la legge n. 71/2017, all'art. 7 comma 2, precisa che, ai fini dell'ammonimento, il Questore debba convocare il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale, e che gli effetti dell'ammonimento cessino al compimento della maggiore età.

L'ammonimento, sostanziandosi in un provvedimento amministrativo, è soggetto sia al ricorso gerarchico al Prefetto (entro 30 giorni dalla data di notifica) sia al ricorso

giurisdizionale al Tribunale amministrativo regionale competente (entro il termine di 60 giorni dalla notifica o dalla comunicazione in via amministrativa).

Quanto alla natura ed ai presupposti per l'ammonimento, ci si può rifare a quanto elaborato dalla giurisprudenza in tema di ammonimento "ordinario".

Si tratta di un provvedimento che assolve ad una funzione tipicamente cautelare e preventiva, in quanto preordinato a che gli atti persecutori posti in essere contro la persona non vengano più ripetuti e non cagionino esiti irreparabili¹⁵, e per il quale non occorre la prova del fatto penalmente rilevante ma, nell'ambito di un potere valutativo ampiamente discrezionale, esclusivamente la sussistenza di un quadro indiziario che renda verosimile, secondo massime di esperienza, l'avvenuto compimento delle condotte di reato che legittimano il provvedimento.

Il Consiglio di Stato ha precisato che "in relazione ai rapporti tra l'ammonimento amministrativo e il procedimento penale, va evidenziato che la diversità delle rispettive conseguenze giustifica una differente intensità dell'attività investigativa che si richiede nelle due ipotesi, laddove, ai fini dell'ammonimento non è necessario che si sia raggiunta la prova del reato, bensì è sufficiente che sia fatto riferimento ad elementi dai quali sia possibile desumere, con un sufficiente grado di attendibilità, un comportamento persecutorio che ha ingenerato nella vittima un «perdurante» e «grave» stato di ansia e di paura" e che "il decreto di ammonimento emesso dal Questore non richiede l'acquisizione di prove tali da poter resistere nel giudizio penale, essendo invece sufficiente che siano assunti nel procedimento elementi che consentano all'Autorità emanante il formarsi del convincimento sulla fondatezza dell'istanza"¹⁶.

La natura del provvedimento non esime di per sé dall'osservanza delle formalità partecipative di cui all'art. 7 della L. 241/1990, e dunque dall'avviso di avvio del procedimento. L'eventuale omissione delle formalità partecipative deve pertanto essere supportata da idonea motivazione in ordine alla necessaria celerità del procedimento in relazione al caso concreto senza che possano essere a tal fine sufficienti mere formule di stile¹⁷.

¹⁵ Cons. Stato, sez. III, sent. 4365/2011, dep. il 19 luglio 2011.

¹⁶ Cons. Stato, sez. III, sent. 2599/2015, dep. il 25 maggio 2015.

¹⁷ Tar Liguria, sez. II, sent. 407/2016, dep. il 26 aprile 2016.

Il Consiglio di Stato ha, peraltro, sottolineato di recente come “il Questore, nell’ambito dei suoi poteri discrezionali, può valutare il “se” ed il “quando” emanare il provvedimento di ammonizione: oltre ad essere titolare del potere di emettere o meno la misura, egli può decidere se emanare senza indugio il provvedimento di ammonizione, oppure se le circostanze consentano di avvisare il possibile destinatario dell’atto, con l’avviso di avvio del procedimento, previsto dall’art. 7 della legge n. 241 del 1990”¹⁸.

Gli atti del procedimento, anche prima dell’emanazione del provvedimento, sono suscettibili di accesso, ai sensi – in particolare – dell’art. 10, comma I lett. a) della L. 7 agosto 1990, n.241, che riconosce ai soggetti destinatari della comunicazione di inizio del procedimento il diritto di prendere visione degli atti per poter compiutamente esercitare le proprie facoltà partecipative, e l’eventuale diniego dell’accesso (ai sensi dell’art. 24, comma VI lett. c) della L. 241/1990) può riguardare la sola documentazione effettivamente coperta dal segreto istruttorio o coperta da esigenze investigative, che devono essere specificamente richiamate nel provvedimento di diniego stesso¹⁹.

Lo strumento amministrativo dell’ammonimento è, infine, precluso in caso di precedente instaurazione del procedimento penale, stante sia il dettato letterale della norma che le finalità della stessa²⁰.

Ciò posto, occorre verificare se tali principi siano mutuabili *tout court* all’ammonimento per cyberbullismo.

Come già sottolineato, l’art. 7 comma 2 prevede una modalità specifica, vale a dire la convocazione del minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale “ai fini dell’ammonimento”, convocazione che tra l’altro non pare facoltativa ma obbligatoria.

Occorre naturalmente interpretare cosa abbia inteso il legislatore con l’espressione “ai fini dell’ammonimento”.

Si potrebbe ritenere che questa espressione non possa essere intesa come meramente rafforzativa del disposto dell’art. 8 comma II del D.L. 7/2009, che prevede appunto che il Questore ammonisca oralmente il soggetto nei cui confronti è stato richiesto il

¹⁸ Cons. Stato, sez. III, sent. 2419/2016, dep. il 6 giugno 2016.

¹⁹ Tar Toscana, sez. II, sent. 176/2017, dep. il 1 febbraio 2017.

²⁰ Tar Lombardia, sez. I, sent. 1025/2014, dep. il 23 aprile 2014.

provvedimento, invitandolo a tenere una condotta conforme alla legge e redigendo processo verbale, ma sia un *quid pluris*, una vera e propria modalità partecipativa, prodromica all'emissione del provvedimento (valorizzando, quindi, l'indicazione finalistica della norma).

Se tale opzione interpretativa è valida, allora questa modalità partecipativa espressa, garantendo (e anzi rendendo necessaria) la partecipazione del minore (e del genitore) al procedimento, potrebbe rendere superflua la comunicazione di avvio.

Secondo altra opzione interpretativa (sostenuta nella Relazione del Servizio studi del Senato "Cyberbullismo – Note sull'A.S. n. 1261 – C" n. 439 del gennaio 2017²¹), si ritiene, invece, che la convocazione sia effettuata al fine dell'ammonimento del minore, e dunque non come modalità partecipativa. Questa conclusione (che porrebbe la convocazione esclusivamente all'esito del procedimento) imporrebbe conseguentemente di applicare anche all'ammonimento in materia di cyberbullismo gli stessi principi in tema di partecipazione enucleati per l'ammonimento "ordinario".

7.1. I "reati" presupposti e l'obbligo di denuncia ex art. 331 c.p.p.

Pur comprendendo lo spirito dell'ammonimento verbale e l'importanza di evitare che il minore entri nel circuito penale, la norma appare criticabile nella sua formulazione²².

In primo luogo, il legislatore è incorso in un evidente lapsus, laddove si parla di "reati" con riguardo all'art. 594 del codice penale.

La citata norma, infatti, è stata abrogata (ben prima dell'entrata in vigore della legge in commento) dall'art. 1 del D.Lgs. 15 gennaio 2016, n. 7 (Disposizioni in materia di abrogazione di reati e introduzione di illeciti con sanzioni pecuniarie civili, a norma dell'articolo 2, comma 3, della legge 28 aprile 2014, n. 67) che ha peraltro introdotto delle inedite sanzioni pecuniarie civili, irrogabili dal giudice competente a giudicare sull'azione di risarcimento del danno.

Non può, pertanto, essere proposta querela per il reato di cui all'art. 594 del codice penale, perché questo è stato abrogato.

²¹ In <http://www.senato.it/japp/bgt/showdoc/17/Dossier/1000902/index.html>.

²² La norma, come originariamente approvata dalla Camera dei Deputati, non si limitava a fattispecie di reato, ma consentiva l'ammonimento per tutte le ipotesi di bullismo e cyberbullismo in senso ampio, salvo il limite che i fatti integrassero reati procedibili d'ufficio.

Ci si deve quindi chiedere quale possa essere l'effetto dell'evidente errore in cui è incorso il legislatore.

Esclusa l'ipotesi di una reviviscenza della disciplina penale dell'ingiuria, quale effetto collaterale della norma, rimangono due opzioni interpretative.

La prima è una *interpretatio abrogans*.

Come visto dianzi, la finalità dichiarata dell'introduzione dell'ammonimento è quella di evitare un procedimento penale al minore. Ma se tale è la finalità, allora l'istituto non sarebbe applicabile per una fattispecie che non costituisce più reato, come appunto l'ingiuria. Ne conseguirebbe forse un *unicum* nel nostro ordinamento: una norma che nasce inapplicabile per abrogazione della fattispecie presupposta prima della sua stessa entrata in vigore.

L'altra opzione è quella di interpretare estensivamente la norma, cercando – sia pure a fatica – di coordinare l'introdotta ammonimento con la mutata natura dell'ingiuria.

La condotta costituente ingiuria, infatti, è attualmente disciplinata dall'art. 4, comma 1, lett. a) del già menzionato D.Lgs. 7/2016, il quale prevede la sanzione pecuniaria civile da euro cento a euro ottomila per chi offende l'onore o il decoro di una persona presente, ovvero mediante comunicazione telegrafica, telefonica, informatica o telematica, o con scritti o disegni, diretti alla persona offesa.

Si potrebbe dunque (ma è un esercizio ermeneutico dal difficile approdo) ritenere che l'ammonimento possa essere chiesto anche per tale fattispecie, prima della proposizione dell'azione civile (unico rimedio accessibile dopo l'abrogazione dell'art. 594 c.p.), o addirittura in ogni momento, non essendo possibile proporre una valida querela per una fattispecie abrogata. È certo, però, che tale interpretazione (che avrebbe il pregio di fornire di efficacia la norma, per le frequenti ipotesi di ingiurie, anche reiterate, ma non ancora trasmodanti negli atti persecutori di cui all'art. 612 bis c.p.) si scontra con il dato letterale, laddove si parla di “querela” o “denuncia”, e ci si riferisce chiaramente all'azione penale, senza menzionare in alcun modo l'azione civile, che sarebbe peraltro diretta non già verso il minore, ma verso i genitori (o anche verso l'istituzione scolastica), ex art. 2048 del codice civile.

In secondo luogo, vi è un altro relevantissimo problema riguardo al richiamo operato al delitto di cui all'art. 167 del D.Lgs. 30 giugno 2003, n. 196 (il trattamento

illecito di dati personali) e all'art. 612 c.p., nella sua ipotesi aggravata, entrambe fattispecie delittuose procedibili d'ufficio.

La norma, infatti, prevede la possibilità dell'ammonimento "fino a quando non è [...] presentata denuncia" e, dunque, sembrerebbe che il limite per la richiesta di ammonimento sia costituito dalla presentazione della denuncia all'autorità giudiziaria.

L'estensione dell'ammonimento a un delitto procedibile d'ufficio diverge significativamente da quanto previsto dall'art. 8 del D.L. 11/2009, che è invece applicabile – non a caso – solo alle fattispecie perseguibili a querela, e pone dei problemi di non poco momento.

Il legislatore, infatti, non pare avvedersi dell'esistenza dell'art. 331 del codice di procedura penale, che prevede l'obbligo (penalmente sanzionato dagli artt. 361 e ss. del codice penale) per i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, abbiano notizia di reato perseguibile di ufficio, di farne denuncia per iscritto, senza ritardo.

Ora, non vi è dubbio che l'autorità di pubblica sicurezza cui la richiesta di ammonimento debba essere presentata rivesta la qualifica di pubblico ufficiale o incaricato di pubblico servizio, e che riceva la richiesta proprio nell'esercizio o a causa delle funzioni o del servizio.

Ne consegue che, trattandosi appunto di un reato (e anzi di un delitto) perseguibile d'ufficio, il soggetto cui è avanzata la richiesta di ammonimento non possa (a pena di sanzione penale) omettere di farne denuncia all'autorità giudiziaria o ad un ufficiale di polizia giudiziaria, ai sensi del secondo comma dell'art. 331 c.p.p. Il che vanificherebbe, in radice, la finalità stessa dello strumento, che è appunto quella di prevenire, mediante l'ammonimento, l'ingresso del minore nel circuito penale.

È vero che, per giurisprudenza costante in materia, ai fini dell'ammonimento non è necessario che si sia raggiunta la prova del reato, bensì è sufficiente che sia fatto riferimento ad elementi dai quali sia possibile desumere, con un sufficiente grado di attendibilità, un comportamento corrispondente alla fattispecie in questione, ma è altrettanto vero che la sussistenza di questi elementi renderebbe comunque applicabile l'art. 331 c.p.p.

Il legislatore, per dare effettività all'istituto, anche con riguardo alle fattispecie procedibili d'ufficio richiamate, avrebbe dovuto prevedere una deroga espressa all'art. 331 c.p.p., ma purtroppo ciò non è avvenuto.

I reati (commessi – si ricordi – mediante la rete Internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne) per cui è possibile con certezza l'ammonimento sono, dunque, solamente quelli di diffamazione (art. 595 c.p.) e minacce (art. 612 c.p.).

Anche per le minacce, peraltro, laddove queste siano qualificabili come aggravante ai sensi del secondo comma dell'art. 612 c.p., si procederebbe d'ufficio, con gli stessi profili problematici testé esaminati in tema di obbligo di denuncia.

Sembra, infine, restare fuori dall'ambito dell'ammonimento il delitto di atti persecutori di cui all'art. 612 bis c.p., anche se commesso per via telematica, non essendovi alcun richiamo nell'art. 7 della legge n. 71/2017. Si applica, pertanto, la disciplina "ordinaria", di cui all'art. 8 del D.L. 11/2009, la quale però è esperibile – non a caso – solo per le fattispecie perseguibili a querela, e dunque non per gli atti persecutori in danno di minori, che sono sempre perseguibili d'ufficio²³.

7.2. Le conseguenze dell'ammonimento e l'efficacia dell'istituto

Si sono già espresse forti perplessità sulla tecnica normativa e sui reati presupposti. Rimane da esaminare quali siano gli effetti dell'ammonimento che, secondo la norma, cesserebbero al compimento della maggiore età.

Gli effetti dell'ammonimento "ordinario" – al di là del generale potere deterrente – sono previsti dai commi 3 e 4 del più volte richiamato art. 8 del D.L. 11/2009, e consistono in una circostanza aggravante per il delitto di cui all'art. 612 bis c.p. e nella procedibilità d'ufficio per tutte le fattispecie, qualora il fatto sia commesso da soggetto già ammonito.

Ma tali effetti non sono applicabili all'ammonimento speciale, e difatti non sono neanche richiamati dall'art. 7.

Rimane, dunque, il mero effetto di deterrenza, senza alcuna sanzione, perfino per le ipotesi di reiterazione delle condotte dopo l'ammonimento. In ciò concorda la relazione del Servizio studi del Senato "Cyberbullismo – Note sull'A.S. n. 1261 – C"

²³ Anceschi A., *Illeciti penali nei rapporti di famiglia e responsabilità civili*, Maggioli, 2012, pag. 96.

n. 439 del gennaio 2017²⁴, che afferma come “la disposizione non prevede misure conseguenti alla violazione delle prescrizioni impartite con l’ammonimento”.

E sarà certamente da valutare l’efficacia concreta di tale effetto deterrente e responsabilizzante, che per essere davvero tale dovrà essere gestito (da personale specializzato) in maniera coerente rispetto alla minore età dei soggetti coinvolti, rischiando in caso contrario di sortire effetti controproducenti.

²⁴ Sul punto, v. *supra*, § 7., nota n.21, in questo stesso capitolo.

CAPITOLO III

Le fattispecie di reato

SOMMARIO: 1. Premessa - 2. La sostituzione di persona - 3. L'ingiuria - 4. La diffamazione come manifestazione del cyberbullismo - 5. Cyberbullismo e reati in materia di pedopornografia - 6. Cyberbullismo e atti persecutori - 7. L'accesso abusivo a sistema informatico - 8. Trattamento illecito di dati personali e cyberbullismo.

1. Premessa

In più occasioni si è assistito, nel corso degli ultimi anni, a richieste provenienti dagli ambienti più disparati e finalizzate ad introdurre, nel nostro ordinamento, speciali norme penali incriminatrici che disciplinassero e sanzionassero penalmente quelle ipotesi che vanno ricomprese entro il concetto – molto ampio in verità – di cyberbullismo.

Ed anche il tortuoso iter della legge ha visto un carsico apparire e scomparire di sanzioni penali, in particolare con il “tentativo” di modifica (non ben meditata, come si vedrà dopo), dell'art. 612 bis c.p. in tema di atti persecutori.

La legge 29 maggio 2017, n. 71, non prevede alcuna specifica sanzione penale o modifica a norme penali incriminatrici, avendo preferito puntare la sua attenzione, come visto dianzi, sulla prevenzione e sulla responsabilizzazione piuttosto che sulla repressione.

Ciò nonostante, appare utile compiere una pur sommaria analisi, sulla base della vigente definizione di cyberbullismo contemplata dal secondo comma dell'art. 1 della L. 71/2017, secondo la quale cyberbullismo è *“qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un*

gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo". Si comprende, quindi, in quali enormi difficoltà sarebbe potuto incorrere il Legislatore nel confezionare una norma penale incriminatrice tale da ricomprendere – nel rispetto del principio di legalità (art. 25 Cost.) – tutti quei comportamenti che, astrattamente sarebbero idonei ad essere ricompresi entro l'accezione di cyberbullismo legislativamente tratteggiata.

Anche nella relazione del Servizio studi del Senato "Cyberbullismo – note sull'A.S. n. 1261 – C" n. 439 del gennaio 2017¹, si sottolinea che la nozione di cyberbullismo *"si scompone nelle condotte riconducibili a fattispecie di reato punite dal codice penale o da leggi speciali, come ad esempio molestie (articolo 660 del codice penale), minaccia (art. 612 c.p.), stalking (art. 612-bis c.p.), estorsione (art. 629 c.p.), diffamazione (art. 595 c.p.), sostituzione di persona (art. 494 c.p.), furto d'identità digitale (art. 640-ter c.p.), trattamento illecito di dati (articolo 167 del decreto legislativo n. 196 del 2003, codice della privacy) - fattispecie per alcune delle quali l'utilizzo dello strumento informatico si configura come aggravante"*. In realtà questa elencazione è parziale, non includendo alcune tra le forme più devastanti di cyberbullismo che possono consistere, ad esempio, nella diffusione di immagini pedo-pornografiche.

La stessa promotrice della legge, la Senatrice Ferrara, nella discussione del 31 gennaio 2017, ha evidenziato che *"i reati ci sono già e contemplano l'on-line, dallo stalking alla diffamazione, dal furto d'identità fino alla morte come conseguenza di altro reato. Lo dimostrano le condanne esemplari comunicate dal tribunale per i minorenni di Torino per il caso di Carolina Picchio: fino a ventisette mesi di messa alla prova per i ragazzi accusati, all'epoca dei fatti minorenni come la loro vittima. Una pena alternativa al carcere, ma certamente non una vacanza"*.

Occorre naturalmente tener conto delle regole in tema di imputabilità (trattandosi, anche, di soggetti minori): saranno dunque imputabili, ai sensi dell'art. 98 c.p., soltanto i minorenni che, nel momento in cui hanno commesso il fatto, abbiano compiuto i quattordici anni, e dei quali sia riconosciuta la capacità di intendere e di volere. I minori al di sotto dei quattordici anni non saranno invece imputabili, ai sensi dell'art. 97 c.p., ma potrà trovare applicazione l'art. 224 del codice penale.

¹ Sul punto, v. *supra*, capitolo II, § 7., nota n. 21.

Il fatto che si tratti di reati anche commessi da minori non soltanto radica la competenza del Tribunale per i minorenni, ma consente anche l'utilizzo degli istituti tipici di tale processo, in particolare la sentenza di non luogo a procedere per irrilevanza del fatto di cui all'art. 27 del D.P.R. 22 settembre 1988 n. 488 e la sospensione con messa alla prova di cui all'art. 28 del medesimo D.P.R.

Con riguardo a quest'ultimo istituto, può essere particolarmente utile l'applicazione di quanto previsto dal comma II dell'art. 28, in tema di prescrizioni dirette a riparare le conseguenze del reato ed a promuovere la conciliazione del minore con la persona offesa dal reato.

2. La sostituzione di persona

La sostituzione di persona, come dianzi rilevato, è uno dei reati più frequenti in tema di condotte di cyberbullismo e può essere integrato dal “furto d’identità” richiamato dall’art. 1 della L. 71/2017: impersonare un’altra persona, infatti, è uno dei modi più insidiosi per porre in essere delle condotte che possono avere un devastante impatto sui minori.

Il delitto è previsto dall’art. 494 c.p., che punisce, con la reclusione fino ad un anno, chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all’altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici.

Venendo all’analisi della fattispecie, si tratta di un delitto procedibile d’ufficio, caratterizzato dal dolo specifico (il fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno) che non richiede, quindi, che l’agente punti ad un guadagno patrimoniale, ma semplicemente ad un’utilità o ad un danno per la persona offesa².

Oggetto della tutela penale è l’interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali.

La norma, pur non avendo subito alcuno specifico “adattamento” all’ecosistema telematico, è ritenuta (in maniera corretta) applicabile – a volte con interpretazione estensiva – ai fatti commessi in rete, al punto che la Suprema Corte ha affermato, proprio con riguardo all’art. 494 c.p., che *“i profondi e, per certi versi, rivoluzionari cambiamenti che l’evoluzione tecnologica ha prodotto attraverso l’affermarsi delle nuove tecnologie informatiche, che, grazie alla nota rete telematica internet, consentono una diffusione di informazioni e possibilità di comunicazione diretta tra gli utenti pressoché illimitate, hanno dispiegato i loro effetti (e non poteva essere altrimenti, in considerazione dell’intima connessione esistente tra società e diritto) anche in materia penale, ponendo molteplici problemi, tra i quali di non poco momento appaiono quelli sottesi ad un’attività di interpretazione estensiva che, in*

² Sansobrinò F., *Creazione di un falso account, abusivo utilizzo dell’immagine di una terza persona e delitto di sostituzione di persona*, in *Diritto Penale Contemporaneo*, in <http://www.penalecontemporaneo.it/d/3269-creazione-di-un-falso-account-abusivo-utilizzo-dell-immagine-di-una-terza-persona-e-delitto-di-sost>.

*assenza di organici interventi legislativi, consenta di adeguare l'ambito di operatività delle tradizionali fattispecie di reato, come quella di cui all'art. 494, c.p., alle nuove forme di aggressione per via telematica dei beni giuridici oggetto di protezione, senza violare i principi della tassatività della fattispecie legale e del divieto di interpretazione analogica delle norme penali*³.

La Cassazione ha, infatti, avuto modo di chiarire – da tempo risalente – che integra il reato di sostituzione di persona la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, allacciando rapporti con altri utenti e così inducendo in errore sia il gestore del sito sia gli utenti, al fine di arrecare un danno consistente nella subdola inclusione della persona offesa in una corrispondenza idonea a ledere l'immagine o la dignità⁴.

Il reato in questione sussiste anche qualora si partecipi ad aste on-line con l'uso di uno pseudonimo. La Suprema Corte argomenta che *“la partecipazione ad aste on-line con l'uso di uno pseudonimo presuppone necessariamente che a tale pseudonimo corrisponda una reale identità, accertabile on-line da parte di tutti i soggetti con i quali vengono concluse compravendite. E ciò, evidentemente, al fine di consentire la tutela delle controparti contrattuali nei confronti di eventuali inadempimenti”*⁵.

Particolarmente interessante, poi, è la già citata sentenza 18826/2013, nella quale si ritiene sussistente il delitto di sostituzione di persona per un'ipotesi purtroppo tristemente frequente nelle condotte di cyberbullismo: l'inserimento in una “chat” di incontri personali del numero di utenza cellulare di un'altra persona, all'insaputa di quest'ultima.

La vittima aveva di conseguenza ricevuto, anche in ore notturne, molteplici chiamate, sms e mms provenienti da vari utenti della chat, anche a sfondo erotico e pornografico.

La sentenza ritiene che il delitto di cui all'art. 494 c.p. *“ricorre non solo quando si sostituisce illegittimamente la propria all'altrui persona, ma anche quando si attribuisce ad altri un falso nome, un falso stato ovvero una qualità a cui la legge attribuisce effetti giuridici, dovendosi intendere per «nome» non solo il nome di*

³ Cass. Pen., Sez. V, sent. 29 aprile 2013 n.18826.

⁴ Cass. Pen., Sez. V, sent. 46674/2007, dep. il 14 dicembre 2007.

⁵ Cass. Pen., Sez. III, sent. 12479/2012.

battesimo ma anche tutti i contrassegni di identità”, e che la protezione si debba estendere anche al nickname, che “quando, come nel caso concreto, non vi siano dubbi sulla sua riconducibilità ad una persona fisica, assume lo stesso valore dello pseudonimo (in presenza di determinati presupposti, assimilato al nome agli effetti della tutela civilistica del diritto alla identità ai sensi dell’art. 9, c.c.) ovvero di un nome di fantasia, la cui attribuzione, a sé o ad altri, integra pacificamente il delitto di cui all’art. 494, c.p.”.

Da ultimo, il reato è stato ritenuto integrato anche dalla condotta consistente nel creare un profilo su di un social network – utilizzando un’immagine della persona offesa e accompagnando il profilo con una descrizione “tutt’altro che lusinghiera” – e l’usufruire con tale falsa identità dei servizi del sito, consistenti essenzialmente nella possibilità di comunicazione in rete con gli altri iscritti (ovviamente indotti in errore) e di condivisione di contenuti (tra cui la stessa foto della persona offesa)⁶.

In conclusione, l’art. 494 del codice penale ha acquistato per così dire una nuova vita, per diventare tra i reati più facilmente riscontrabili nelle condotte di cyberbullismo, dove è il più delle volte facile dimostrare il dolo specifico, quantomeno come finalità di arrecare a terzi un danno.

⁶ Cass. Pen., Sez. V, sent. 25774/2014, dep. il 16 giugno 2014.

3. L'ingiuria

L'ingiuria era punita dall'art. 594 del codice penale, che sanzionava l'offesa all'onore o al decoro di una persona presente. La sanzione si applicava anche a chi commetteva il fatto mediante comunicazione telegrafica o telefonica, o con scritti o disegni, diretti alla persona offesa.

Non vi era dubbio, in giurisprudenza, che l'ingiuria potesse consumarsi anche attraverso l'utilizzo di comunicazioni elettroniche ed informatiche (che costituiscono mezzi idonei per la propalazione di notizie e comunicazioni⁷) e, dunque, a mezzo chat, messaggio diretto, email, etc.

Le ingiurie "telematiche" quindi (con tutta la varietà dei mezzi consentiti dalla Rete), se perpetrate da un minore imputabile, erano indubbiamente idonee, a seguito di querela, a far avviare un procedimento penale per il delitto di cui all'art. 594 c.p., procedimento che, il più delle volte, si concludeva con una sentenza di non luogo a procedere per irrilevanza del fatto, di cui all'art. 27 del D.P.R. 22 settembre 1988 n. 488, soprattutto per le ipotesi di minore offensività.

La situazione è ora profondamente mutata perché (come già notato a proposito dell'art. 7 della L. 71/2017) l'art. 594 c.p. è stato abrogato – ben prima dell'entrata in vigore della legge in commento – dall'art. 1 del D.Lgs. 15 gennaio 2016, n. 7 (Disposizioni in materia di abrogazione di reati e introduzione di illeciti con sanzioni pecuniarie civili, a norma dell'articolo 2, comma 3, della legge 28 aprile 2014, n. 67, legge che appunto ha delegato il Governo ad abrogare alcuni reati, tra cui l'ingiuria, e ad introdurre delle inedite "sanzioni pecuniarie civili").

Il delitto in esame non è più previsto da nessuna norma penale incriminatrice e la condotta costituente ingiuria è oggi disciplinata dall'art. 4, comma 1, lett. a) del già menzionato D.Lgs. 7/2016, con il quale si è introdotta la "sanzione pecuniaria civile" da euro cento a euro ottomila, per chi offende l'onore o il decoro di una persona presente, ovvero mediante comunicazione telegrafica, telefonica, informatica o telematica, o con scritti o disegni, diretti alla persona offesa. La sanzione è da euro duecento a euro dodicimila se l'offesa consiste nell'attribuzione di un fatto determinato o è commessa in presenza di più persone.

⁷ *Ex multis*, Cass. Pen., Sez. V, sent. 2669/2016.

Il legislatore, nel disegnare la nuova fattispecie soggetta a sanzione civile, ha voluto adeguare la tradizionale nozione di ingiuria, includendovi espressamente l'offesa effettuata mediante comunicazione "informatica o telematica", in conformità peraltro agli approdi giurisprudenziali appena esaminati.

La nuova disciplina prevede poi ulteriori norme (sempre modellate sulle disposizioni penali concernenti l'ingiuria) regolanti le offese reciproche e lo stato d'ira.

L'art. 4, comma 2, infatti, prevede che, se le offese sono reciproche, il giudice può non applicare la sanzione pecuniaria civile ad uno o ad entrambi gli offensori, mentre il comma 3 dispone la non sanzionabilità di chi ha commesso il fatto in stato d'ira determinato da un fatto ingiusto altrui, e subito dopo di esso⁸.

Non vi è dubbio, quindi, che laddove il minore offenda l'onore o il decoro di terzi mediante, ad esempio, Whatsapp, Telegram, Facebook Messenger, Snapchat, messaggio diretto via Twitter o qualunque altro sistema di messaggistica, e non vi sia una pluralità di destinatari, potrà essere integrata la "nuova" fattispecie, non più rientrante nella competenza del Tribunale dei minori (per essere il reato abrogato) ma del Tribunale ordinario civile, non potendo ovviamente il minore rispondere personalmente, ma dovendosi applicare le regole di cui all'art. 2048 del codice civile. In questi casi, dunque, per le ipotesi dolose, potrà essere irrogata l'inedita sanzione pecuniaria civile, da parte del giudice competente a conoscere dell'azione di risarcimento del danno.

La sanzione, peraltro, ha come presupposto indefettibile l'accoglimento della domanda di risarcimento del danno e non pare irrogabile separatamente da esso; inoltre, la somma non deve essere corrisposta al danneggiato, ma recuperata secondo le disposizioni stabilite dalla parte VII del Testo Unico delle disposizioni legislative e regolamentari in materia di spese e giustizia (D.P.R. 30 maggio 2002, n. 115) e versata all'entrata del bilancio dello Stato per essere riassegnata al capitolo di spesa del Ministero dell'Interno riguardante il Fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso, delle richieste estorsive, dell'usura e dei reati intenzionali violenti, per le finalità di cui all'art. 11 della legge 7 luglio 2016, n. 122.

⁸ Gatta G.L., *Depenalizzazione e nuovi illeciti sottoposti a sanzioni pecuniarie civili: una riforma storica*, in *Diritto Penale Contemporaneo*, <http://www.penale.contemporaneo.it/d/4427-depenalizzazione-e-nuovi-illeciti-sottoposti-a-sanzioni-pecuniarie-civili-una-riforma-storica>.

La vittima di un atto rientrante nella nozione di cyberbullismo, di cui all'art. 1 della L. 71/2017, ma qualificabile come ingiuria, non avrà quindi altra alternativa che quella di adire il giudice civile per il risarcimento del danno.

Questa azione, però, presenta svariate difficoltà pratiche, tipiche dell'accertamento delle condotte in Rete.

Tali difficoltà sono legate, in primo luogo, all'individuazione del soggetto responsabile. Si pensi ai messaggi (privati) ricevuti da un profilo facebook non identificabile, o da qualunque altro sistema di chat dove non si sia in grado in concreto di identificare il mittente.

In assenza di ulteriori elementi che possano essere forniti al giudice per l'identificazione dell'offensore, sarà di fatto impossibile risalire all'identità del danneggiante, sia perché (non essendo più reato) non vi è alcuna possibilità di acquisire i dati relativi al traffico telematico, ai sensi dell'art. 132 del Codice della Privacy, in quanto l'emissione del decreto motivato del Pubblico Ministero, prevista dalla norma, presume la finalità di accertamento e repressione dei reati, sia perché oggi i provider statunitensi non offrono alcuna cooperazione per fatti (come l'ingiuria) che, non essendo reato negli U.S.A., non soddisfano il requisito della doppia incriminazione.

Ma quand'anche si conosca l'identità dell'offensore – e molto spesso l'identità del cyberbullo non è affatto celata – è sempre necessario applicare le migliori pratiche di digital forensics per l'acquisizione e la conservazione dei messaggi “incriminati”, in maniera tale da assicurarne la corretta produzione nel successivo giudizio.

È ben vero che il codice di procedura civile non conosce delle regole specifiche per l'acquisizione della prova digitale (contrariamente a quanto accaduto per il diritto processuale penale, a seguito del recepimento della Convenzione di Budapest sul Cybercrime, avvenuta con la L. 18 marzo 2008, n. 48 – “Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento italiano”⁹), ma è altrettanto vero che la volatilità e la facile modificabilità dei documenti informatici non può non essere tenuta in conto, soprattutto quando essi provengono direttamente dalla parte. Vi è da segnalare, peraltro, come la più recente giurisprudenza stia,

⁹ Demarchi P.G., *I nuovi reati informatici*, Giappichelli, 2009.

finalmente, valorizzando il dettato del recente Regolamento Eidas¹⁰, il quale prevede all'art. 46 (rubricato "*Effetti giuridici dei documenti elettronici*") che "a un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica"¹¹.

Da ultimo, rileviamo come ben difficilmente, per le ipotesi di ingiuria, si potrà adire il rimedio di cui all'art. 2 della L. 71/2017 (Tutela della dignità del minore) e cioè l'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, giacché la stessa – per espressa dizione normativa – può riguardare soltanto il dato personale che sia "diffuso nella rete internet" (art. 2, comma 1)¹².

L'uso del termine "diffuso" non può, infatti, intendersi in senso atecnico, tale da ricomprendere qualunque comunicazione effettuata a mezzo Internet, ma deve intendersi come un richiamo al concetto di "diffusione" di cui al D.Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) ed in particolare alla definizione di cui all'art. 4, comma 1, lett. *m*), che individua per diffusione "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

Il concetto in esame non dovrebbe cambiare neanche quando, il 25 maggio 2018, acquisterà piena efficacia il Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR), il quale, pur non fornendo una definizione esplicita come il Codice della Privacy, individua la diffusione come una delle modalità delle comunicazioni di dati personali, distinguendola comunque dalla "trasmissione" (art. 4, comma 1, n. 2), e dunque qualificandola, in ogni caso, come la comunicazione ad una collettività tendenzialmente indeterminata di persone.

¹⁰ Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

¹¹ Sul punto, Trib. Milano, Sez. V, sent. n. 11402/2016, pubbl. il 18/10/2016.

¹² Sul punto, v. *supra*, capitolo II, § 2.

4. La diffamazione come manifestazione del cyberbullismo

Le ipotesi di cyberbullismo che si traducono in “*qualunque forma di diffamazione in danno di minorenni, realizzata per via telematica*” sono già previste e punite in base all’art. 595 c.p.

L’art. 595, primo comma, c.p., infatti, punisce chiunque, comunicando con più persone, offenda l’altrui reputazione. Il terzo comma, inoltre, prevede che il reato in questione sia aggravato qualora l’offesa sia recata con qualsiasi altro (“altro” rispetto al mezzo della stampa) mezzo di pubblicità.

La diffamazione è un reato comune (in quanto può essere commesso da chiunque), di evento (non è sufficiente l’esternazione diffamatoria ma è necessario che “più persone”, ossia almeno due persone diverse, la percepiscano e la comprendano), a forma libera (in quanto può essere realizzato con qualunque mezzo, salva la diversa possibilità di incidere sul bene tutelato a seconda del mezzo utilizzato), punito a titolo di dolo generico (coscienza e volontà di usare espressioni offensive) e il cui bene giuridico tutelato è l’onore e il decoro di una persona.

La persona offesa non deve essere necessariamente una persona fisica, ma può anche essere una collettività di soggetti quali, ad esempio, entità giuridiche, associazioni, enti privi di personalità giuridica quali partiti, fondazioni, comunità religiose, corpi amministrativi e giudiziari, comunità locali e così via.

L’onore, inteso quale bene individuale, della persona – secondo la relazione al progetto preliminare del codice penale – può avere un’accezione “soggettiva” (ed in essa è ricompresa la “*somma dei valori morali che l’individuo attribuisce a se stesso*”) ovvero “oggettiva” (con ciò intendendosi “*la stima o l’opinione che gli altri hanno di noi*”). Il concetto di onore, tuttavia, da una lettura costituzionalmente orientata della previgente norma di cui all’art. 594 c.p. oltre che, ovviamente, dell’art. 595 c.p., può essere individuato nel complesso delle qualità essenziali al valore di ogni persona tra le quali rientrano quelle morali, fisiche, psichiche, intellettuali e così via (Mantovani).

La divulgazione di contenuti potenzialmente lesivi dell’onore o del decoro altrui potrebbe, tuttavia, essere perfettamente lecita (art. 51 c.p. – esercizio di un diritto o adempimento di un dovere) qualora essa integri il corretto esercizio del diritto di manifestare liberamente il proprio pensiero, consacrato nell’art. 21 della

Costituzione. In tal modo, pertanto, non vi sarà diffamazione ma corretto esercizio del diritto di cronaca, ad esempio, qualora le notizie diffuse siano vere (limite della “verità”), l’esposizione dei fatti sia contenuta entro i limiti della correttezza (limite della “continenza”) e vi sia un interesse pubblico alla conoscenza (limite dell’ “interesse pubblico”). Allo stesso modo, inoltre, potrà riconoscersi la liceità della divulgazione di contenuti astrattamente diffamatori qualora sia riconosciuto il corretto utilizzo di altre forme di manifestazione del pensiero quali, ad esempio, la critica o la satira.

L’art. 595 c.p. prevede tre diverse circostanze quali possibili aggravanti specifiche del reato in esame. La circostanza aggravante che qui viene in rilievo è quella prevista dal terzo comma del citato articolo, giustificata dalla maggiore diffusività potenziale dei contenuti diffamatori, ossia l’uso della stampa o di “qualsiasi altro mezzo di pubblicità”. La giurisprudenza, al riguardo, ha più volte ribadito¹³ che la diffamazione commessa attraverso la rete Internet sia da considerarsi aggravata ai sensi del terzo comma dell’art. 595 c.p. È chiaro, infatti, che la definizione di “qualsiasi altro mezzo di pubblicità” sia idonea a ricomprendere anche la circostanza che il fatto di diffamazione sia posto in essere attraverso la rete Internet o, comunque, telematicamente.

La diffamazione, diversamente dalla previgente definizione di “ingiuria” (prevista all’art. 594 c.p. prima dell’intervento abrogativo ai sensi dell’art. 1, co. 1, lett. c) del D.Lgs. 15 gennaio 2016 n. 7) prevede che l’offesa all’onore o al decoro di un soggetto sia posta in essere attraverso una “comunicazione con più persone” e non sia, invece, rivolta esclusivamente alla persona offesa “presente”. Il concetto di “più persone”, pertanto, richiama la necessità di verificare il fatto che almeno due soggetti abbiano preso cognizione delle offese all’onore e al decoro della persona offesa.

La diffamazione, sul punto, ha creato fermento giurisprudenziale sulla condivisibile difficoltà di individuare quante persone abbiano effettivamente preso cognizione di un contenuto diffamatorio diffuso attraverso la rete Internet e il momento esatto in cui ciò sia accaduto. Con riferimento alla diffamazione on-line, pertanto, emergono ulteriori problemi interpretativi che riguardano – essenzialmente – in primo luogo profili di giurisdizionalità (nelle ipotesi, ad esempio, in cui i contenuti diffamatori

¹³ *Ex multis*, Cass. Pen., Sez. V, sent. 4741/2000.

risiedano “fisicamente” su un server che si trovi fuori dai confini territoriali dello Stato) e in secondo luogo di competenza per territorio.

Per quanto riguarda i profili connessi alla giurisdizione nel delitto di diffamazione on-line, la giurisprudenza di legittimità ne ha più volte ribadito la sussistenza mediante il richiamo al secondo comma dell’art. 6 c.p., in base al quale il reato si considera commesso nel territorio dello Stato quando su di esso si sia verificata, in tutto o in parte, l’azione o l’omissione, ovvero l’evento che ne sia conseguenza (teoria dell’ubiquità)¹⁴. Considerato che il reato di diffamazione è un reato d’evento, sarà sufficiente a fondare la giurisdizione sia che sul territorio nazionale si sia verificata anche in parte la condotta (ad esempio la condotta di immissione nella rete Internet dei contenuti diffamatori), sia che sul medesimo territorio si sia verificato l’evento (ossia che almeno due soggetti, sul territorio nazionale, abbiano preso cognizione dei contenuti diffamatori)¹⁵.

Per quanto riguarda, invece, i profili relativi alla competenza per territorio a giudicare i reati di diffamazione on-line, la più recente giurisprudenza di legittimità ritiene che la difficoltà connessa alla individuazione del luogo “fisico” in cui il secondo soggetto (il delitto di diffamazione, infatti, si consuma nel momento in cui si verifici l’evento per cui “più persone” percepiscano i contenuti diffamatori e il concetto di “più persone” implica la necessità che almeno due persone percepiscano i contenuti diffamatori on-line) prenda cognizione dei contenuti diffamatori induce a ricorrere – in tutti quei casi in cui non sia effettivamente possibile svolgere tale tipo di indagine – ai criteri suppletivi di collegamento. Si è ribadito, infatti, che *“solo nel caso in cui ciò non sia possibile, la competenza per territorio va determinata in forza del criterio del luogo di domicilio dell’imputato, in applicazione della ulteriore regola suppletiva stabilita dall’art. 9, comma secondo, c.p.p.”*¹⁶.

¹⁴ Cass. Pen., Sez. V, sent. 28739/2017: *“La diffamazione è reato di evento, sicché si consuma nel momento e nel luogo in cui i terzi percepiscono l’espressione ingiuriosa ovvero, nel caso in cui frasi o immagini lesive siano state immesse sul web, nel momento in cui il collegamento viene attivato”*.

¹⁵ *Ex multis*, Cass. Pen., Sez. V, sent. 4741/2000 (cit.).

¹⁶ Cass. Pen., Sez. V, sent. 28739/2017 (cit.): *“Ovviamente non è sempre possibile l’individuazione del secondo soggetto che legge l’articolo diffamatorio (così integrando il requisito della comunicazione con due o più persone) [...] Ne consegue che, procedendo a cascata, viene in esame il primo dei momenti di collegamento suppletivi, sopra richiamato. Quindi, se è individuabile il luogo in cui è avvenuta una parte dell’azione (l’ultima individuabile), è in quel luogo che si determina la competenza territoriale per il giudizio [...] Solo nel caso in cui ciò non sia possibile, la competenza per territorio va determinata in forza del criterio del luogo di domicilio dell’imputato, in applicazione della ulteriore regola suppletiva stabilita dall’art. 9, comma secondo, c.p.p.”*.

Altri profili problematici riguardano la possibilità di applicare alle ipotesi di diffamazione on-line le norme specificatamente previste per la stampa e, ancora, la possibilità di estendere ai provider la responsabilità penale prevista per il soggetto agente del delitto di diffamazione.

Il primo, tra gli ultimi profili richiamati, è rilevante nel senso che le conseguenze dell'equiparazione tra web e stampa possono condurre ad ipotesi di estensione (analogica in *malam partem* e, perciò, vietate) della disciplina speciale della stampa a fattispecie non espressamente disciplinate.

La vigente legge sulla stampa (L. 8 febbraio 1948, n. 47) prevede nell'art. 13, ad esempio, un'aggravante particolare per le ipotesi di diffamazione a mezzo stampa "consistente nell'attribuzione di un fatto determinato" che rende applicabile a tale ipotesi di diffamazione la pena detentiva fino a sei anni di reclusione. Secondo la più recente giurisprudenza di legittimità, la norma in questione (art. 13 L. 47/1948) non è applicabile a tutti i casi di diffamazione commessa on-line in quanto, in ossequio alla recente giurisprudenza delle Sezioni Unite¹⁷, deve tenersi ben distinta l'area dell'informazione di tipo professionale, veicolata per il tramite di una testata giornalistica on-line, dal vasto ed eterogeneo ambito della diffusione di notizie ed informazioni da parte di singoli soggetti in modo spontaneo¹⁸.

Altre ipotesi in cui si è statuita la inapplicabilità al web delle norme che facciano espresso richiamo al concetto di "stampa" possono rinvenirsi a proposito della configurabilità del soggetto del "direttore responsabile" ex art. 57 c.p. per le testate on-line¹⁹, o di applicabilità della disciplina prevista per la "stampa clandestina" dall'art. 16 della L. 47/1948²⁰. In tutte tali ipotesi si è ribadito che l'estensione anche ai contenuti diffusi via Internet del concetto di "stampa" costituisce interpretazione analogica in "malam partem" non consentita ai sensi dell'art. 25, comma secondo, della Costituzione.

Tuttavia, come già accennato, recentemente le Sezioni Unite penali (con la sentenza n. 31022/2015) hanno statuito la necessità di richiamare un concetto di stampa

¹⁷ Cass. Pen., SS.UU., sent. 31022/2015.

¹⁸ Cass. Pen., Sez. V, sent. 4873/2017.

¹⁹ Cass. Pen., Sez. V, sent. 54177/2016.

²⁰ Cass. Pen., sent. 23230/2012.

“costituzionalmente orientato” (e limitato solo ad alcune ipotesi²¹) partendo dalla considerazione secondo cui *“il giornale telematico, sia se riproduzione di quello cartaceo, sia se unica e autonoma fonte di informazione professionale, soggiace alla normativa sulla stampa, perché ontologicamente e funzionalmente è assimilabile alla pubblicazione cartacea”*.

Ultimo tra i profili più rilevanti in tema di diffamazione on-line – che può comunque svolgere un ruolo di interesse per la persona offesa dei reati in questione – è quello relativo alla responsabilità dei provider. La questione, infatti, si muove tra le ipotesi in cui il prestatore dei servizi della società dell’informazione (rientrano in tale *genus* sia il concetto di Internet Service Provider che i fornitori, genericamente intesi, dei servizi di hosting, caching o mere-conduit) possa essere ritenuto in qualche modo responsabile dei contenuti diffusi on-line da altri ai sensi della disciplina di cui al D.Lgs. 70/2003 (che recepisce in Italia la direttiva europea 2000/31/CE – ossia la “Direttiva sul commercio elettronico”) e quella in cui possa ritenersi fondata la sua responsabilità ai sensi dell’art. 110 c.p., o, ancora, ai sensi dell’art. 40, cpv., c.p. Quest’ultima possibilità (ossia la possibilità, nel caso di specie, di ritenere il provider soggetto ad un obbligo giuridico di impedire l’evento-diffamazione) resta, comunque, esclusa in radice se si considera che non sussiste un obbligo generalizzato di controllo.

Possono aversi, invece, ipotesi in cui la responsabilità venga estesa al gestore del sito internet ai sensi dell’art. 110 c.p. (concorso di persone nel reato)²².

Infine, per quanto riguarda la condizione di procedibilità per il reato di diffamazione a danno di minorenni, occorre evidenziare che il genitore mantiene la legittimazione all’esercizio del diritto di querela sia nell’ipotesi in cui il figlio minorenni sia dissenziente (la volontà contraria del minore alla proposizione della querela è, in tal

²¹ Cass. Pen., SS.UU., sent. 31022/2015: *“Prima, però, di esporre le ragioni che inducono a legittimare, nel rispetto del principio di legalità, una interpretazione evolutiva e costituzionalmente orientata del termine “stampa”, è necessario chiarire che l’esito di tale operazione ermeneutica non può riguardare tutti in blocco i nuovi mezzi, informatici e telematici, di manifestazione del pensiero (forum, blog, newsletter, newsgroup, mailing list, pagine Facebook), a prescindere dalle caratteristiche specifiche di ciascuno di essi, ma deve rimanere circoscritto a quei soli casi che, per i profili strutturale e finalistico che li comotano, sono riconducibili, come meglio si preciserà in seguito, nel concetto di “stampa” inteso in senso più ampio. Ed invero, deve tenersi ben distinta, ai fini che qui interessano, l’area dell’informazione di tipo professionale, veicolata per il tramite di una testata giornalistica on-line, dal vasto ed eterogeneo ambito della diffusione di notizie ed informazioni da parte di singoli soggetti in modo spontaneo”*.

²² Sul punto, v. Cass. Pen., sent. 54946/2016.

caso, *tamquam non esset*) sia nell'eventualità in cui il minore non sia venuto a conoscenza, per qualsiasi motivo, della condotta delittuosa in suo danno²³.

²³ Sul punto, v. Cass. Pen., Sez. V, sent. 23010/2013, che risulta essere, tra l'altro, l'unica sentenza in cui la Cassazione adoperi il termine "cyberbullismo".

5. Cyberbullismo e reati in materia di pedopornografia

Uno dei comportamenti più comuni rientranti nel concetto di cyberbullismo è l'impiego di immagini a sfondo sessuale – siano esse autoprodotte dalla vittima minorenni ovvero realizzate da altri – per finalità di estorsione nei confronti della stessa vittima.

In tali particolari ipotesi, sono configurabili diverse fattispecie criminose: dalla detenzione o realizzazione di immagini pedo-pornografiche al reato di estorsione.

Negli ultimi anni, l'evoluzione della tecnologia mobile unita ad una riduzione dei costi di produzione di dispositivi quali smartphone e tablet ha comportato una diffusione massiva di tali strumenti, che sono abitualmente in uso anche ai minorenni, tanto da indurre, talvolta, gli istituti scolastici a regolamentarne l'utilizzo durante le ore di lezione²⁴.

Tali dispositivi sono dotati, nella quasi totalità dei casi, di sistemi di ripresa audiovisiva. Se poi si pensa alla riduzione dei costi anche sul versante delle connessioni dati da parte degli operatori telefonici, si comprende facilmente quali siano i numeri della condivisione e pubblicazione di contenuti on-line: ogni minuto vengono condivisi centinaia di migliaia di contenuti audiovisivi.

La condivisione di immagini, audio e video – fino a qualche anno fa proibitiva a causa dei costi delle connessioni dati – rappresenta oggi la funzione principale dei dispositivi mobile (in grado di soppiantare, quanto a durata e mole di dati, anche la tradizionale comunicazione telefonica).

È agevolmente intuibile, pertanto, quale sia il livello di espansione anche del fenomeno del c.d. sexting, ossia la condivisione di messaggi contenenti testi o contenuti audiovisivi sessualmente espliciti.

La diffusione del fenomeno è tanto massiccia da aver indotto talune software house a rilasciare applicazioni per dispositivi mobile (c.d. “App”) la cui funzione è proprio quella di “potersi scambiare materiali hot via internet”.

Nell'epoca della condivisione globale il sesso diventa uno dei protagonisti principali.

²⁴ Anche il Garante per la protezione dei dati personali, nel corso della sua relazione sull'attività del 2016, tenutasi a Roma il 6 giugno 2017, ha ribadito l'attenzione dell'Autorità per i temi come la privacy a scuola tanto da dedicarvi un documento informativo sul corretto uso delle nuove forme di comunicazione e condivisione in internet.

Tuttavia, qualora i contenuti “sessualmente espliciti” abbiano ad oggetto soggetti infra-diciottenni, è ben possibile che le condotte assumano una rilevanza anche di tipo penale.

Di recente, la Corte di Cassazione²⁵ ha affrontato proprio gli aspetti del sexting: una minorenni autoproduceva alcune fotografie che la ritraevano in pose sessualmente esplicite e le inviava – di propria iniziativa, senza esservi sollecitata – ad alcuni conoscenti, dei quali tutti, tranne uno, ricondividevano le stesse immagini. Il ragazzo che non condivideva ulteriormente le immagini veniva accusato del reato di detenzione di materiale pedopornografico (ai sensi dell’art. 600 quater c.p.) mentre gli altri di diffusione di materiale pedopornografico (ai sensi dell’art. 600 ter, comma quarto, c.p.). Il Tribunale per i minorenni di Arezzo pronunciava sentenza di non doversi procedere nei confronti di tutti gli imputati per insussistenza del fatto in quanto nel caso in esame mancava uno degli elementi costitutivi del delitto oggetto di imputazione, ossia la necessaria alterità tra colui che produce il materiale e il minore offeso. Avverso tale sentenza proponeva ricorso il Procuratore della Repubblica in relazione ai capi d’imputazione riguardanti i ragazzi che avevano ulteriormente condiviso le immagini pedo-pornografiche, ma la Cassazione rigettava il ricorso condividendo l’impostazione del Tribunale per i minorenni.

Il quarto comma dell’art. 600 ter c.p., infatti, punisce colui che, al di fuori delle ipotesi di commercio, distribuzione, divulgazione, diffusione o pubblicizzazione, offra o ceda ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma del medesimo articolo. Tale ultima disposizione (art. 600 ter c.p.) punisce chiunque “*utilizzando minori di anni diciotto [...] produce materiale pornografico*”. Ed è proprio il concetto di “utilizzazione” che richiede la diversità tra l’autore delle produzioni pornografiche e il minore oggetto delle medesime.

Per cui, in sostanza, una diversa interpretazione che ammettesse la possibilità di estendere la punibilità anche alle ipotesi in cui il soggetto “utilizzatore del minore” e il minore stesso coincidano, si tradurrebbe in una analogia in *malam partem*.

Alle medesime conclusioni si giungerebbe anche nei casi in cui il minore oggetto delle rappresentazioni di natura pedopornografica revocasse, in seguito, il proprio “consenso” alla detenzione o ulteriore condivisione degli oggetti.

²⁵ Cass. Pen., sent. 11675/2016, consultabile al link: <http://www.penalecontemporaneo.it/upload/1463148722cass-pen.11675-16.pdf>

6. Cyberbullismo e atti persecutori

Il delitto di atti persecutori è stato introdotto nel nostro codice penale, all'art. 612 bis, dal D.L. 23 febbraio 2009, n. 11, convertito con la legge 23 aprile 20089, n. 38.

La nuova fattispecie delittuosa appariva necessaria a sanzionare compiutamente il cosiddetto "stalking", posto che prima della sua entrata in vigore le stesse condotte – nelle ipotesi in cui non si trattasse di fatti di lesioni o comunque di violenza e minacce – erano sanzionate ai sensi dell'art. 660 c.p.²⁶. Tuttavia è criticata, da più parti, la clausola di riserva ("salvo che il fatto non costituisca più grave reato") in quanto il reato in questione appare difficilmente inquadrabile in un qualche rapporto di specialità rispetto ad altre norme penali incriminatrici.

Il fatto tipico del reato di atti persecutori (reato di evento), inoltre, richiede, da un lato, che via sia una reiterazione delle condotte di minaccia o molestia e, dall'altro, che tali condotte abbiano l'effetto, sulla persona offesa, di cagionare un perdurante e grave stato di ansia o di paura ovvero di ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona alla medesima legata da relazione affettiva ovvero da costringere la stessa persona offesa ad alterare le proprie abitudini di vita.

Si tratta, in sostanza, di un reato necessariamente abituale²⁷ in cui, cioè, il fatto tipico esige una reiterazione di comportamenti e i successivi eventi (*"cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita"*) debbono essere causalmente riconducibili alla condotta dell'agente.

In particolare, quanto alla reiterazione, si sottolinea che sono state ritenute sufficienti ad integrare il reato de quo anche solo due condotte²⁸.

Così come il delitto di diffamazione, anche il reato di "atti persecutori" (o, come comunemente chiamato dagli organi di stampa, "stalking") prevede, al secondo comma dell'art. 612 bis, un'aggravante speciale per l'ipotesi in cui il fatto sia commesso "attraverso strumenti informatici o telematici".

²⁶ Sul punto, v. Cass. Pen., Sez. I, sent. 23262/2016.

²⁷ Sul punto, v. Cass. Pen., Sez. VII, ord. 41572/2016.

²⁸ *Ex multis*, Cass. Pen., Sez. V, sent. 48690/2014.

Si tratta di un'aggravante speciale ad effetto comune, ossia una circostanza riferibile al reato di atti persecutori che comporta un aumento della pena fino ad un terzo (ai sensi dell'art. 64 c.p.) e che rende possibile – nel caso di unica aggravante – l'applicazione della reclusione da 8 mesi a 6 anni e 8 mesi.

Tuttavia, riprendendo gli elementi della vigente definizione di cyberbullismo, potranno essere in essa ricomprese tutte le ipotesi in cui taluno, con condotte reiterate, minacci o molesti per via telematica un soggetto minore in modo da cagionarne un perdurante e grave stato di ansia o di paura ovvero da ingenerare nello stesso un fondato timore per l'incolumità sua o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso minore ad alterare le proprie abitudini di vita²⁹.

Poiché gli atti persecutori si caratterizzano per la sussistenza di una serie di condotte, la consumazione del reato si perfeziona con l'ultima di dette condotte e, di conseguenza, la competenza si radica nel luogo in cui si realizza la condotta stessa. In queste ipotesi, infatti, opera la regola suppletiva di cui all'art. 9, comma 1, c.p.p., secondo cui è competente *“il giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione”*, e non la disposizione di cui all'art. 8, comma 3, c.p.p., che, con riferimento ai reati permanenti, individua la competenza territoriale in capo al *“giudice del luogo in cui ha avuto inizio la consumazione”*.

Considerando quel che qui ci interessa – vale a dire l'ipotesi in cui il soggetto agente commette il fatto tipico mediante lo “strumento telematico” – occorre chiedersi se sia necessario, per la possibilità di ritenere integrata l'aggravante di cui al secondo comma dell'art. 612 bis c.p. (relativa, appunto, all'uso degli “strumenti informatici o telematici”), che tutte le condotte, nella loro abitualità, si debbano caratterizzare per l'uso degli “strumenti informatici o telematici”.

Da un'interpretazione letterale della norma parrebbe preferibile – ad integrare l'aggravante in questione – la necessità di individuare quantomeno due differenti ipotesi di minaccia o molestia attraverso l'uso di “strumenti informatici o telematici”,

²⁹ Cass. Pen., Sez. V, sent. 18819/2013: *“per ravvisare il delitto de quo non si richiede l'accertamento di uno stato patologico, ma è sufficiente che gli atti ritenuti persecutori - e nella specie costituiti da minacce e insulti alla persona offesa, inviati con messaggi telefonici o via Internet o, comunque, espressi nel corso di incontri imposti - abbiano un effetto destabilizzante della serenità e dell'equilibrio psicologico della vittima, considerato che la fattispecie incriminatrice di cui all'art. 612 bis cod. pen. non costituisce una duplicazione del reato di lesioni (art. 582 cod. pen.) , il cui evento è configurabile sia come malattia fisica che come malattia mentale e psicologica”*.

posto che il secondo comma fa riferimento al “fatto” tipico del reato di cui al primo comma.

Questa ipotesi di cyberbullismo, oltretutto – considerata la minore età della persona offesa – ai sensi al quarto comma dell’art. 612 bis c.p. è perseguibile d’ufficio e richiama, in tal modo, ben due circostanze aggravanti: la prima è un’aggravante speciale ad effetto speciale (prevista dal terzo comma dell’art. 612 bis c.p.), la seconda un’aggravante speciale ad effetto comune (prevista dal secondo comma del menzionato art. 612 bis).

In sostanza, per le ipotesi di cyberbullismo così delineate, sarà possibile – ai sensi dell’art. 63, comma terzo, c.p. – giungere ad un’applicazione della pena detentiva che varia da 1 a 10 anni di reclusione.

7. L'accesso abusivo a sistema informatico

L'accesso abusivo a sistema informatico è uno dei reati introdotti dalla L. 23 dicembre 1993 n. 547 (Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica) ed è tra le fattispecie più frequenti (assieme alla sostituzione di persona) in tema di cyberbullismo.

Prendere il controllo dei sistemi informatici della vittima è, infatti, uno dei primi passi per ridicolizzarlo, per pubblicare “post” a suo nome, per comprometterne l'immagine tra i compagni, o semplicemente per dimostrare di essere tecnicamente più preparati: è una delle attività che spesso vengono compiute con molta leggerezza e che, giunti all'epilogo giudiziario, impegnano i tribunali dei minori.

Si tratta di un reato dalla portata particolarmente invasiva, dato che oramai la nostra intera vita, le nostre comunicazioni, il nostro patrimonio di informazioni, immagini e video, è contenuto nei dispositivi elettronici personali.

E ciò è tanto vero che una notissima sentenza della Corte Suprema degli Stati Uniti (Riley vs California) ironizza – ma non troppo – sul fatto che il proverbiale marziano che arrivasse sulla Terra considererebbe lo smartphone come un componente importante dell'anatomia umana³⁰, e questo è vero soprattutto per i giovani e i giovanissimi, per i quali lo smartphone è un indispensabile completamento dell'interazione sociale quotidiana.

Non è questa la sede per una disamina completa di tutti gli aspetti dell'accesso abusivo (che ha impegnato molto la dottrina e la giurisprudenza, con diverse importanti pronunce della Cassazione, anche a Sezioni Unite³¹), per cui ci limiteremo a tratteggiare i profili della fattispecie più rilevanti per il fenomeno oggetto della presente trattazione.

La fattispecie prevista dall'art. 615 ter del codice penale punisce, a querela della persona offesa (quantomeno per le fattispecie non aggravate), con la reclusione fino a tre anni “*chiunque abusivamente si introduce in un sistema informatico o telematico*”

³⁰ U.S. Supreme Court, Riley vs California, 25 giugno 2014, al link: <http://www.scotusblog.com/case-files/cases/riley-v-california/>.

³¹ Da ultimo, Cass. Pen., SS.UU., 18 maggio 2017.

protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo”.

Si tratta chiaramente di un delitto di mera condotta (quantomeno per le fattispecie non aggravate), a dolo generico, integrato da due condotte alternative (l'introdursi in un sistema protetto da misure di sicurezza o il mantenersi contro la volontà espressa o tacita del titolare dello *ius excludendi*), che si perfeziona con la violazione del domicilio informatico – e, quindi, con la introduzione nel relativo sistema – senza la necessità che si verifichi una effettiva lesione del diritto alla riservatezza dei dati³². Trattandosi di un delitto a dolo generico, non occorre alcuna specifica finalità (quale quella di altrui danno o profitto), ma è sufficiente semplicemente la coscienza e volontà di introdursi (o mantenersi) in un sistema protetto da misure di sicurezza.

La norma tutela il domicilio informatico, e non si limita a preservare soltanto i contenuti personalissimi presenti nel sistema, ma tende a salvaguardare da qualunque tipo di intrusione, che possa avere ricadute anche solo economico-patrimoniali.

La Suprema Corte, fin da tempo risalente, ha adottato una definizione lata di “sistema informatico”³³ e, successivamente, la Convenzione Europea di Budapest del 23 novembre 2001 (recepita – come noto – con la L. 48/2008), all'art. 1 ha definito quale sistema informatico «qualsiasi apparecchiature o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati».

Di recente, la Cassazione ha precisato che “un dispositivo elettronico assurge al rango di sistema informatico o telematico se si caratterizza per l'installazione di un software che ne sovrintende il funzionamento, per la capacità di utilizzare periferiche o dispositivi esterni, per l'interconnessione con altri apparecchi e per la molteplicità dei dati oggetto di trattamento”³⁴ e che “per evitare vuoti di tutela e per ampliare la

³² Cass. Pen., Sez. V, sent. 11689 del 6 febbraio 2007.

³³ La definizione “tradizionale” è quella enucleata da Cass. Pen., Sez. VI, n. 3067 del 4 ottobre 1999, secondo cui il “sistema informatico” deve intendersi come un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche parziale) di tecnologie informatiche sono caratterizzate, per mezzo di un'attività di “codificazione” e “decodificazione”, dalla “registrazione” o “memorizzazione” tramite impulsi elettronici, su supporti adeguati, di “dati”, cioè, di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni costituite da un insieme più o meno vasto di informazioni organizzate secondo una logica che consente loro di esprimere un particolare significato per l'utente.

³⁴ Cass. Pen., SS.UU., sent. 17325 del 26 marzo 2015.

sfera di protezione offerta ai sistemi informatici e telematici, è opportuno accogliere la nozione più ampia possibile di computer o unità di elaborazione di informazioni”.

Tale nozione ampia certamente ricomprende non solo gli smartphone, ma anche le caselle di posta elettronica³⁵ e gli account social, purché – naturalmente – siano protetti da misure di sicurezza.

Quanto a queste ultime, bisogna sottolineare che è irrilevante che siano facili da superare, o quasi irrisorie (si pensi all’uso di adoperare password semplici, o di non cambiare la password preimpostata nei sistemi), mentre è sufficiente che vi sia una qualsivoglia misura di sicurezza che dimostri la volontà del titolare del sistema di voler riservare l’accesso alle persone autorizzate e di inibire la condivisione del suo spazio informatico con i terzi.

Il luogo di consumazione del reato, dopo varie oscillazioni, è stato individuato in quello nel quale si trova il soggetto che effettua l’introduzione abusiva o vi si mantiene abusivamente.

In altri termini, il luogo de quo si identifica con quello nel quale dalla postazione remota l’agente si interfaccia con l’intero sistema, digita le credenziali di autenticazione e preme il tasto di avvio, restando invece irrilevante il luogo (fisico) dove è situato il server a cui si accede³⁶.

Per esemplificare, il minore che accede al profilo social del compagno, dopo averne carpito (o reperito, con o senza l’utilizzo di specifiche tecniche informatiche) le credenziali di accesso, o accede allo smartphone altrui, protetto da password o pin, commette certamente il delitto in questione, così come commette lo stesso reato qualora si introduca (da remoto), anche solo per gioco o sfida, in un sistema informatico, ad esempio, di un’azienda o di un ente pubblico, e ciò anche se si limiti alla mera introduzione, senza arrecare alcun danno. E infine, qualora non riesca ad introdursi nel sistema, magari perché non ha a disposizione le credenziali corrette, sarà comunque punibile a titolo di tentativo di accesso abusivo.

³⁵ Sul punto, v. Cass. Pen., Sez. V, sent. 13057/2016, che afferma che “*allorché, in un sistema informatico pubblico (che serve, cioè, una Pubblica Amministrazione), siano attivate caselle di posta elettronica - protette da password personalizzate - a nome di uno specifico dipendente, quelle «caselle» rappresentano il domicilio informatico proprio del dipendente, sicché l’accesso abusivo alle stesse, da parte di chiunque (quindi, anche da parte del superiore gerarchico), integra il reato di cui all’art. 615 ter cod. pen.*”.

³⁶ Cass. Pen., SS.UU., sent. 17325 del 26 marzo 2015 (cit).

8. Trattamento illecito di dati personali e cyberbullismo

Il secondo comma dell'art. 1 della L. 71/2017 richiama espressamente – quale comportamento astrattamente idoneo a configurare un'ipotesi di cyberbullismo – il “trattamento illecito di dati personali in danno di minorenni, realizzato per via telematica”.

Il delitto di trattamento illecito di dati personali di cui all'art. 167 del Codice della privacy (D.Lgs. 196/2003) – che si pone in rapporto di continuità normativa rispetto al previgente art. 35 della L. 675/1996 – prevede che *“salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocimento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi”*.

Il secondo comma del medesimo articolo, invece, statuisce che *“salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocimento, con la reclusione da uno a tre anni”*.

I reati in questione sembrerebbero costruiti come reati comuni (dato il richiamo al soggetto attivo come “chiunque”) mentre, in realtà, si tratta di reati che possono essere commessi solamente da chi rivesta la qualifica di titolare, responsabile o incaricato al trattamento dei dati personali ossia da chiunque esegua un trattamento di dati personali in violazione di specifiche norme di legge.

Nel primo comma dell'articolo in questione sono contemplate due differenti fattispecie delittuose: il “trattamento illecito” di dati personali e la “comunicazione o diffusione” illecita di dati personali.

Entrambe le tipologie del primo comma condividono la clausola di riserva (salvo che il fatto costituisca più grave reato), il riferimento al soggetto agente (chiunque) ed il dolo specifico richiesto (al fine di trarne per sé o per altri profitto o di recare ad altri un danno).

La prima ipotesi (del “trattamento illecito”) è punita soltanto se dal fatto deriva il nocumento, mentre la “comunicazione o diffusione” è punita a prescindere dall’effettivo nocumento che pare, pertanto, darsi per presunto.

Per quanto riguarda l’aspetto del “nocumento” richiesto dalla prima fattispecie disciplinata dal primo comma dell’articolo in esame, ci si è interrogati sulla sua natura al fine di comprendere se esso rappresenti un elemento costitutivo del fatto tipico o se rappresenti una condizione oggettiva di punibilità.

Nel primo caso (fatto tipico), infatti, dovrebbe essere oggetto – come tutti gli altri elementi del fatto tipico – del dolo specifico richiesto dalla norma e, inoltre, solo alla sua verifica conseguirebbe la consumazione del reato.

La giurisprudenza di legittimità più risalente ritiene che si tratti di una condizione oggettiva di punibilità (art. 44 c.p.) che comunque non può andare a disegnare una ipotesi di responsabilità oggettiva, posto che la verifica della condizione oggettiva (il nocumento), non facendo parte degli elementi del fatto tipico, non potrebbe in ogni caso essere oggetto dell’elemento psicologico.

Il reato in questione, in sostanza, si perfezionerebbe comunque, a prescindere dalla verifica del nocumento, che condiziona esclusivamente la procedibilità del medesimo reato. Tuttavia, a causa dell’ampio significato che può attribuirsi al concetto di “nocumento” (essendo capace di ricomprendere sia ipotesi incidenti sullo stesso interesse tutelato dalla norma, sia su un bene giuridico diverso³⁷, qual è, ad esempio, l’interesse patrimoniale), risulta complesso verificare se l’elemento condizionante la punibilità riguardi effettivamente il medesimo interesse tutelato dalla norma.

La giurisprudenza di legittimità più recente, pertanto, qualifica l’elemento del “nocumento” non più quale condizione oggettiva di punibilità ma quale elemento costitutivo del reato, *“avuto riguardo alla sua omogeneità rispetto all’interesse leso e alla sua diretta derivazione causale dalla condotta tipica, con conseguente necessità che esso fosse previsto e voluto o, comunque, accettato dall’agente come conseguenza della propria azione, indipendentemente dal fatto che costituisse o si identificasse con il fine dell’azione stessa”* (Sez. III, n. 40103 del 5/02/2015, dep. 6/10/2015, Ciulla, Rv. 264798).

³⁷ Cass. Pen., Sez. V, sent. 11994/2017: *“il nocumento può sussistere anche quando dal trattamento di dati sensibili derivino, per la persona offesa, effetti pregiudizievoli sotto il profilo morale”*.

Per quanto riguarda, invece, il trattamento per fini esclusivamente personali, il reato di trattamento illecito di dati personali non sarebbe configurabile a meno che i dati oggetto del trattamento non siano soggetti a sistematica comunicazione o diffusione³⁸.

³⁸ Cass. Pen., Sez. III, sent. 15221/2017: “*Giova, peraltro, rilevare come secondo la giurisprudenza di questa Corte (v. Sez. 3, n. 29071 del 16/05/2013, dep. 9/07/2013, Boggi e altro, Rv. 256673; Sez. 5, n. 46454 del 22/10/2008, dep. 17/12/2008, Polimeni e altri, Rv. 241966; Sez. 3, n. 5728/05 del 17/11/2004, dep. 15/02/2005, Paciocco, Rv. 230834), il reato di trattamento illecito di dati personali non è integrato se l'utilizzo dei dati avvenga per fini esclusivamente personali, ovvero senza una loro diffusione (definita dalla lett. m dell'art. 4, comma 1, come «il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione») o una loro destinazione ad una comunicazione sistematica*”.

CONCLUSIONI

Telefonate, messaggi, chat su whatsapp, email, post sui social network, diffusione di foto e video...abbiamo visto come la creatività di un cyberbullo possa andare di pari passo con le sue abilità informatiche e consentirgli di invadere, colonizzare telematicamente, detronizzare la sua vittima dentro e fuori dalla rete.

Finché il bullo ha campo, la vittima pare non avere scampo.

E più subisce, più tace, oppure cerca riscatto invertendo i ruoli e bullizzando altri/e, alimentando così questo video-gioco al massacro, nell'impotenza degli adulti e nell'inermità di certe istituzioni, come la scuola, ora in prima linea grazie alla serie di compiti e responsabilità impartite dalla nuova legge.

Sul piano normativo penale, la L. 71/2017 non ha aggiunto alcunché: continuano ad operare le regole usuali a proposito di minacce, diffamazioni, sostituzione di persona, estorsione e violazione norme T.U. Privacy. Continua ad essere competente il Tribunale per i minorenni, ove è vietata la costituzione di parte civile ma all'interno dello strumento della messa alla prova possono essere messe in atto dinamiche di incontro empatico tra autore e vittima del reato.

Tuttavia, la legge n. 71 del 29 maggio 2017, costituisce un fondamentale punto di partenza nel percorso di prevenzione e contrasto del cyberbullismo, finora privo di una normazione unitaria, in Italia come in Europa.

È una legge di diritto mite e partecipativo, che si focalizza sui profili educativi e di prevenzione del cyberbullismo, introducendo sia strumenti di tutela dei ragazzi nel ruolo di vittima (l'istanza di oscuramento) sia strumenti di responsabilizzazione degli stessi nel ruolo attivo di bulli (l'ammonimento).

Non demonizza Internet, straordinario strumento di conoscenza e condivisione dei nostri ragazzi. La pietra angolare del provvedimento è rappresentata, infatti, dall'educazione all'uso consapevole della rete, in un mondo sempre più connesso, complesso e veloce, dove non vi è più alcuna differenza tra on-line ed off-line, al fine di formare nuovi cittadini digitali.

Oggi la consapevolezza di fenomeni riconducibili ad un uso distorto della rete è abbastanza diffusa, ma è auspicabile che, oltre alla campagna informativa, tutti i

soggetti chiamati e responsabilizzati dalle nuove norme prevedano quelle forme di sostegno psicologico che, soprattutto in giovane età, sono indispensabili per scongiurare i pericoli di ricaduta o di *coping*.

BIBLIOGRAFIA

ANCESCHI

Illeciti penali nei rapporti di famiglia e responsabilità civili, Maggioli, 2012

BARONE

Bullismo e cyberbullismo: riflessioni, percorsi di intervento, prospettive, 2016

BASSOLI-RUSSO

Contrasto al cyberbullismo: una legge utile?, in *Il Quotidiano Giuridico*, 2017

BATTAGLIA

Cyberbullismo: il nuovo male oscuro, Gorle Marna, 2016

BERTI-VALORZI-FACCI

Cyberbullismo: guida completa per genitori, ragazzi e insegnanti, Reverdito, 2017

BISTOLFI

Strumenti di tutela contro il cyberbullismo negli ordinamenti contemporanei e nelle policies dei social network, al link: <http://www.tesi.eprints.luiss.it/13056/2/bistolfi-camilla-sintesi-2014.pdf>

DEMARCHI

I nuovi reati informatici, Giappichelli, 2009

DOTTA

Cyberbullismo: cosa prevede la nuova legge, al link: <http://www.webnews.it/2017/05/17/cyberbullismo-legge>

GATTA

Depenalizzazione e nuovi illeciti sottoposti a sanzioni pecuniarie civili: una riforma storica, in *Diritto Penale Contemporaneo*, al link: <http://www.penale.contemporaneo.it/d/4427-depenalizzazione-e-nuovi-illeciti-sottoposti-a-sanzioni-pecuniarie-civili-una-riforma-storica>

KUMPULAINEN

Bullying and psychiatric symptoms among elementary school-age children, in *Child Abuse and Neglect*, 1998

LISI

Ddl Cyberbullismo in cerca d'autore. Atto terzo: buona la prima, si replica a Montecitorio, nella rivista telematica *Huffingtonpost* al link: http://www.huffingtonpost.it/andrea-lisi/ddl-cyberbullismo-in-cerca-dautore-atto-terzo-buona-la-prima-si-replica-a-montecitorio_b_14639392.html

MATTIOLI

Il bullo e la vittima: due facce della stessa medaglia? In *Il Fatto Quotidiano* del 29 gennaio 2016

MEAZZA

Cyberbullismo e bullismo, proposta di legge approvata alla Camera, in *Giurisprudenza Penale Web*, 2016, 9

MORELLI

Cyberbullismo: provider fuori dal raggio d'azione della legge, in *Altalex* del 23 maggio 2017, <http://www.altalex.com/documents/news/2017/05/23/cyberbullismo>

OLWEUS

Bulling at School: What we know, and what we can do, 1996

PERRY-KENNEDY

Conflict and the development of antisocial behavior, in C.U. Shantz, W.W. Hartup, Cambridge Univ. Press, 1992

SANSOBRINO

Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona, in *Diritto Penale Contemporaneo*, al link: [http://www.penalecontemporaneo.it/d/3269-creazione-di-un-falso-account-abusivo-utilizzo-dell-immagine-di-una-terza-persona-e-delitto-di-sost.](http://www.penalecontemporaneo.it/d/3269-creazione-di-un-falso-account-abusivo-utilizzo-dell-immagine-di-una-terza-persona-e-delitto-di-sost)

SCHWARTZ

The aggressive victim of bullying. Emoziona and behavioral disregulation as a pathway to victimization by peers, in J. Juvonen, S. Graham, New York, Guilford Press, 2001

SENISE

L'adolescente "come se", in www.spiveb.it, Riv. della Società Psicoanalitica italiana

ZANETTI-RENATI-BERRONE

Il fenomeno del bullismo, tra prevenzione ed educazione, ED. Magi, 2015

ZICCARDI

L'odio on-line. Violenza verbale e ossessioni in rete, Cortina ed., 2016