

XVII legislatura

CYBERBULLISMO

NOTE SULL'A.S. N. 1261-C

gennaio 2017
n. 439



servizio studi del Senato

ufficio ricerche sulle questioni
istituzionali, sulla giustizia e sulla
cultura



SERVIZIO STUDI
TEL. 066706-2451
studi1@senato.it

I dossier del Servizio studi sono destinati alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. I testi e i contenuti normativi ufficiali sono solo quelli risultanti dagli atti parlamentari. Il Senato della Repubblica declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

XVII legislatura

CYBERBULLISMO

NOTE SULL'A.S. N. 1261-C

gennaio 2017
n. 439

a cura di: Luca Borsi

ha collaborato: Simone Bonanni

Classificazione Teseo: Minori; Violenze e minacce; *Internet*

Cyberbullismo: cenni introduttivi, pag. 5 - Alcuni dati sulla dimensione del fenomeno, pag. 9 - Il disegno di legge A.S. n. 1261-C, pag. 15.

CYBERBULLISMO: CENNI INTRODUTTIVI

Il bullismo informatico - o *cyberbullismo* - è una forma di maltrattamento (*to bull* in inglese significa: usare prepotenza, maltrattare, intimidire, intimorire) perpetrato su soggetti minorenni utilizzando le tecnologie dell'informazione e della comunicazione.

Messo in atto da una o più persone (bulli) nei confronti di altro individuo percepito come più debole (vittima), vi è insita la reiterazione di un atteggiamento e di una condotta di sopraffazione, esercitando un condizionamento psicologico lesivo, mediante contenuti (parole o immagini) immessi su *social network*, *blog*, *email*, *sms*, ecc., quanto costituisca una rete virtuale di comunicazioni.

Ancorché sia sovente estensione e prosecuzione del bullismo 'tradizionale', il *cyberbullismo* assume connotati propri di fluidità e pervasività. Rilevano qui: la capacità di permeare le percezioni e la psicologia e la vita quotidiana dei giovanissimi, le cui attività di socializzazione avvengono sul *web* con altrettanta 'realtà' che fuori di esso; la sua natura 'virale', in grado di superare ogni confine e distanza nonché di raggiungere un grande numero di osservatori e testimoni; la sequenzialità dei messaggi, talché può sfumare fin quasi a dissolversi la individuabilità della deliberazione e della intenzionalità del messaggio nocivo; la possibile assunzione di una personalità in rete altra da sé, con conseguente affievolimento del senso del lecito e di remore etiche. Ed il controllo degli adulti è reso vieppiù difficoltoso dal divario generazionale in termini di alfabetizzazione digitale.

Nel *cyberbullismo* il grande numero, se non potenziale illimitatezza, del pubblico esponenziale di contatti, così come l'anonimato e la distanza da un luogo fisico (spesso la scuola) senza rischio di essere individuati e contrastati, rendono possibile un 'effetto slavina' dell'intimidazione e del discredito.

L'espressione "bullismo" ha fatto ingresso nel linguaggio delle leggi nel 2012 (l'articolo 50 del decreto-legge n. 5 del 2012 prevede, entro norme per l'autonomia scolastica, che un decreto del ministro dell'istruzione,

dell'università e della ricerca emanasse linee guide per la definizione, fra l'altro, di un organico di rete territoriale tra istituzioni scolastiche, finalizzato anche al contrasto dei fenomeni di "bullismo").

Successivamente la "prevenzione ed il contrasto di ogni forma di discriminazione e di bullismo, anche informatico" sono stati posti dalla legge n. 107 del 2015 (recante riforma del sistema nazionale di istruzione e formazione nonché delega per il riordino delle disposizioni legislative vigenti) tra gli obiettivi di potenziamento dell'offerta formativa (articolo 1, comma 7, lettera l)).

Una definizione normativa di *cyberbullismo* non è finora presente nell'ordinamento.

Esso 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 sede giurisprudenziale (civile di risarcimento per fatto illecito ex articolo 2043 del codice civile, e penale) sono stati determinati pertanto alcuni profili.

Per quanto riguarda l'imputabilità, vige il principio generale (posto che i bulli maggiorenni sono soggetti alla disciplina ordinaria) sancito dall'articolo 98 del codice penale, che prevede l'imputabilità del minorenne con più di 14 anni al momento del fatto, del quale sia riconosciuta la capacità di intendere e di volere. L'imputabilità del minore con età inferiore a 14 anni è invece esclusa dall'articolo 97 del codice penale (tuttavia, ove egli sia ritenuto pericoloso, tenuto specialmente conto della gravità del fatto e delle condizioni morali della famiglia in cui il minore è vissuto, il giudice minorile ne ordina il ricovero in riformatorio giudiziario o lo pone in libertà vigilata: art. 224 c.p.).

Gli atti di bullismo, ove connotati da particolare gravità, possono giustificare misure cautelari.

Per quanto riguarda la titolarità del diritto di querela, essa è in capo al minore se ultraquattordicenne (il minore infraquattordicenne ne è privo), e convive con l'autonomo analogo diritto in capo all'esercente la potestà genitoriale. Ove vi sia diversità di orientamento, prevale la volontà orientata all'esercizio del diritto di querela.

Quanto alle puntuali manifestazioni del *cyberbullismo*, vi è un variegato lessico per designarle:

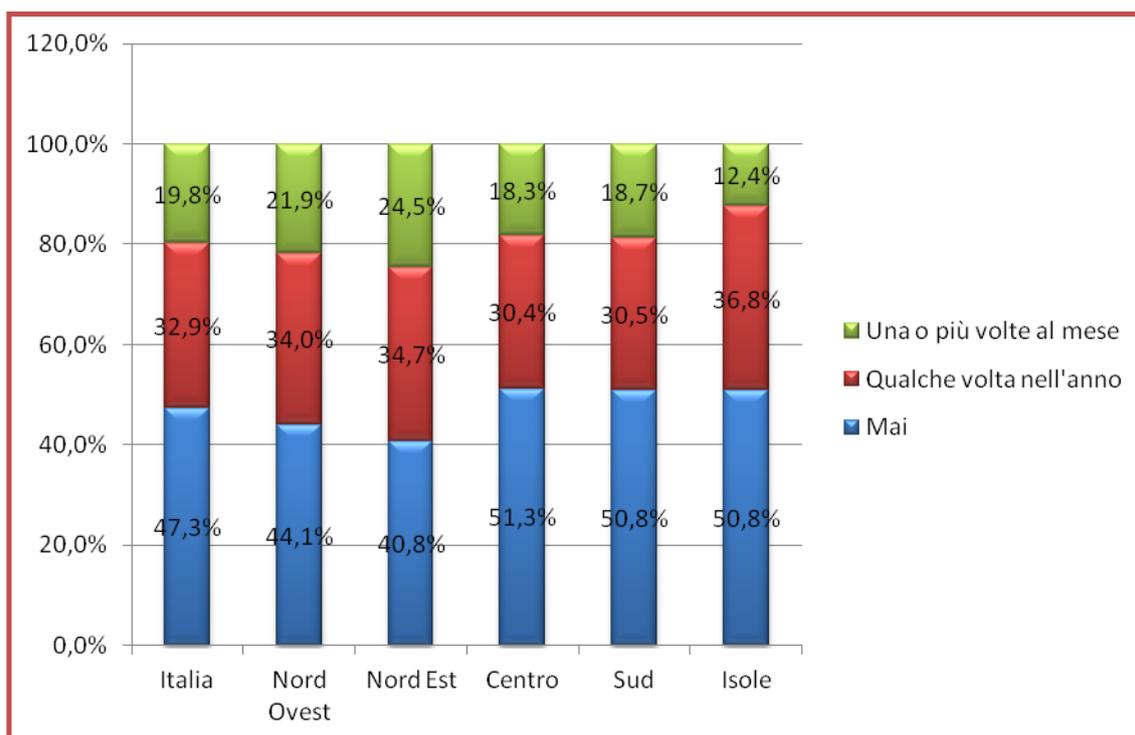
- *cyberstalking* ossia persecuzione per via informatica: molestie e denigrazioni ripetute e minacciose, mirate a incutere paura ed ansia;
- esclusione: escludere deliberatamente una persona da un gruppo *on line* per provocare in essa un sentimento di emarginazione;
- *exposure* ossia rivelazione di informazioni private imbarazzanti su un'altra persona;
- *flaming*: messaggi *on line* violenti e volgari intesi a suscitare (infiammare, testualmente) battaglie verbali in un *forum*;
- *harassment* ossia molestie: spedizione ripetuta di messaggi insultanti mirati a ferire qualcuno; denigrazione: parlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione, via *e-mail*, messaggistica istantanea, gruppi su *social network* ecc.;
- *impersonation* ossia sostituzione di persona: farsi passare per un'altra persona per spedire messaggi o pubblicare testi repressibili;
- *sexting* (dalla fusione di *sex* e *texting*, 'scrivere messaggi'): invio di messaggi, immagini o video a sfondo sessuale o sessualmente espliciti tramite dispositivi informatici;
- *trickery*: ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri le informazioni confidate via mezzi elettronici.

ALCUNI DATI SULLA DIMENSIONE DEL FENOMENO

Una ricerca condotta dall'ISTAT su ["Il bullismo in Italia: comportamenti offensivi e violenti tra i giovanissimi"](#) analizza dati riferiti al 2014.

Evidenza in via preliminare - con riferimento al fenomeno generale del bullismo, non necessariamente in ambiente informatico - come circa il 50% dei ragazzi compresi nella fascia di età tra 11 e 17 anni abbia subito un "episodio offensivo, non rispettoso e/o violento" nel corso 2014; il 19,8% subisce atti di bullismo più volte al mese; di questi, il 9,1% dei ragazzi subisce tali atti settimanalmente.

Ragazzi e adolescenti di 11-17 anni per frequenza in cui hanno subito comportamenti offensivi nel corso degli ultimi 12 mesi, per ripartizione territoriale. Anno 2014 (per 100 ragazzi e adolescenti di 11-17 anni della stessa ripartizione territoriale)



Nel 2014, in Italia, il 52,7% di ragazzi appartenenti alla fascia di età compresa tra 11 e 17 anni sono stati interessati da episodi di bullismo, più o meno frequenti. Considerando che la popolazione residente della stessa fascia di età è pari a circa 4 milioni, quasi 2,2 milioni di ragazzi, su tutto il territorio nazionale, sarebbero stati interessati da tali episodi.

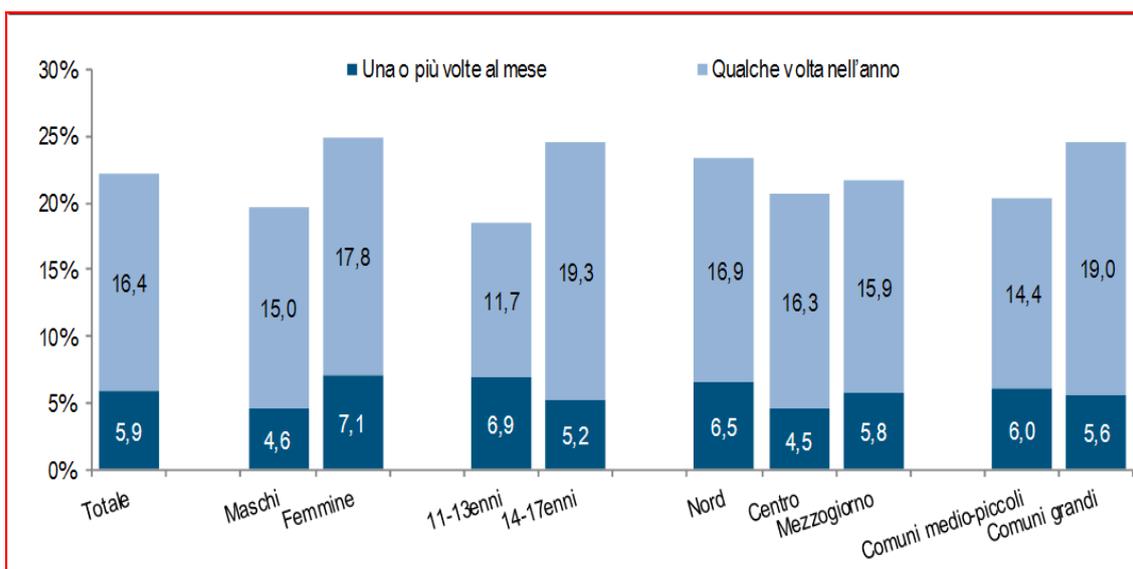
Riguardo alle dimensioni del fenomeno del *cyberbullismo*, la medesima indagine ISTAT informa che "tra i ragazzi utilizzatori di cellulare e/o Internet, il 5,9% denuncia di avere subito ripetutamente azioni vessatorie tramite *sms*, *e-mail*, *chat* o sui *social network*. Le ragazze sono più di frequente vittime di *cyberbullismo* (7,1% contro il 4,6% dei ragazzi)".

Inoltre, durante l'anno 2014, circa il 22% delle vittime di bullismo ha dichiarato di aver subito un atto offensivo veicolato attraverso la rete; le azioni ripetute (più volte al mese) riguardano il 5,9% dei ragazzi vittime di *cyberbullismo*.

Tali percentuali sono da riferirsi non al complesso dei ragazzi compresi nella fascia di età 11-17 anni ma all'insieme dei giovani utenti che accedono ad internet tramite PC, cellulari, *tablet* ecc. (si tratta del 90% circa dei giovani nella fascia di età considerata).

Si registra un maggior rischio tra i più giovani: secondo il report ISTAT, "circa il 7% degli 11-13enni dichiara di essere stato vittima una o più volte al mese di prepotenze tramite cellulare o Internet mentre la quota scende al 5,2% se la vittima ha un'età compresa tra 14 e 17 anni". Il grafico che segue illustra i dati principali del report ISTAT più volte richiamato.

Ragazzi e adolescenti di 11-17 anni per frequenza con cui hanno subito, tramite internet o telefono cellulare, comportamenti offensivi, non rispettosi e/o violenti, per sesso, per classe di età e per ripartizione territoriale e dimensione demografica del comune di residenza. Anno 2014 (per 100 ragazzi e adolescenti di 11-17 anni con le stesse caratteristiche che usano Internet e/o il telefono cellulare)



Fonte: ISTAT, *Il bullismo in Italia: comportamenti offensivi e violenti tra i giovanissimi* - Anno 2014

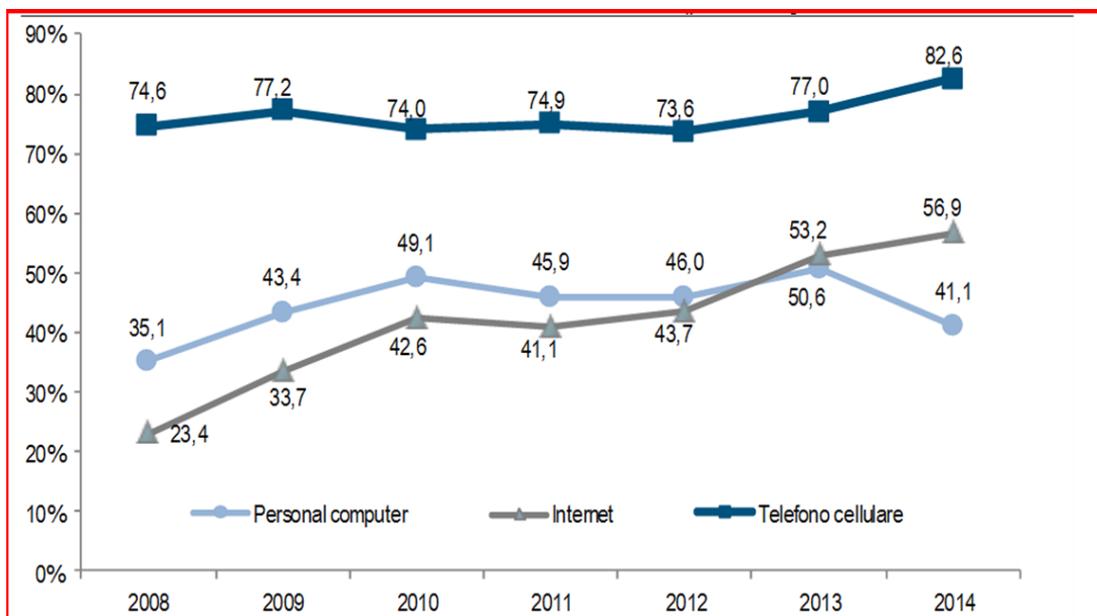
Qui di seguito si riportano alcuni dati desumibili dal *report* ISTAT come rielaborati dal CENSIS (*50° Rapporto sulla situazione sociale del Paese, dicembre 2016*, p. 101).

Vittime di episodi offensivi, non rispettosi, e/o violenti da parte di altri ragazzi tramite internet o telefono cellulare		22,3%
	Femmine	24,9%
	Maschi	19,6%
	11-13enni	18,6%
	14-17enni	24,5%
Vittime assidue (una o più volte al mese)		5,9%
	11-13enni	6,9%
	14-17enni	5,2%
Per area geografica		
	Nord	23,4%
	Centro	20,8%
	Sud	21,7%
Per Comune di residenza¹		
	Comuni medio-piccoli	20,4%
	Comuni grandi	24,6%

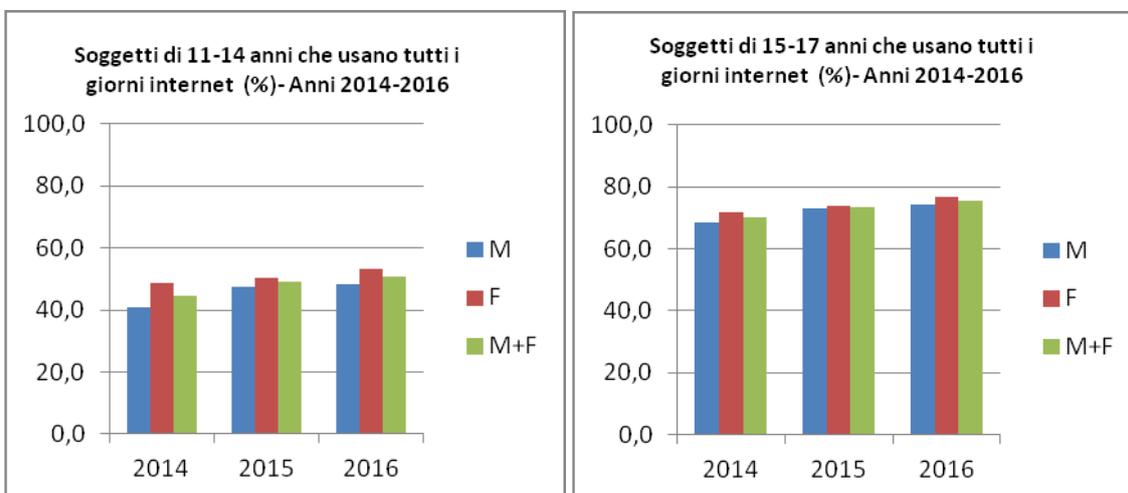
Le percentuali relative ai fenomeni di *cyberbullismo* sono calcolate non sull'insieme dei ragazzi compresi nella fascia di età considerata ma sull'insieme dei ragazzi di quella fascia di età che fanno uso di PC, cellulare, tablet ecc.

¹ Per “Comuni medio-piccoli” si intendono quelli che hanno una popolazione inferiore ai 50.000 abitanti; nei “Comuni grandi” sono compresi quelli con una popolazione pari o maggiore a 50.000 abitanti e i Comuni periferia dell’area metropolitana

Ragazzi e adolescenti di 11-17 anni che usano tutti i giorni il cellulare, internet e il personal computer. Anni dal 2008 al 2014 (per 100 ragazzi e adolescenti di 11-17 anni)



Secondo quanto riportato nel *report* dell'ISTAT, "la maggior propensione delle ragazze/adolescenti a utilizzare il telefono cellulare e a connettersi a Internet probabilmente le espone di più ai rischi della rete e dei nuovi strumenti di comunicazione". A tale proposito si osserva che l'ISTAT pubblica, negli Annuari Statistici, dati sull'uso di internet per fasce di età e per sesso. I grafici che seguono riepilogano tali dati, riportando la percentuale dei giovani che accedono quotidianamente ad internet, distinti per sesso e con riferimento alle fasce di età 11-14 anni e 15-17 anni, nel triennio 2014-2016.



Fonte: ISTAT, Annuari statistici 2014-2016

Secondo un'indagine presentata commissionata a Skuola.net e all'Università degli studi di Firenze da [Generazioni Connesse](#) (il *Safer Internet Centre* italiano coordinato dal MIUR) e presentata nel febbraio 2016, il 17% dei nati tra il 1996 e il 2010 dichiarano di connettersi ad Internet tra le 5 e le 10 ore al giorno; la stessa percentuale di ragazzi (17%) si dichiara di essere "sempre connessa".

Sul tema del bullismo e del *cyberbullismo* ulteriori dati sono stati forniti dal Censis in occasione della pubblicazione del 50° Rapporto sulla situazione sociale del Paese (dicembre 2016).

Secondo quanto esposto sul sito del Censis, il 52,7% dei ragazzi compresi nella fascia di età tra 11 e 17 anni, nel corso del 2016, ha subito "comportamenti offensivi, non riguardosi o violenti da parte dei coetanei".

Il Censis, inoltre, riporta che il 75,8% dei dirigenti scolastici interpellati (pari a 1.800) si è trovato a gestire più casi di bullismo, il 52,8% di *cyberbullismo*.

Inoltre, "il 51,8% dei dirigenti ha organizzato incontri sulle insidie di internet con i genitori, avvalendosi prevalentemente del supporto delle Forze dell'ordine (69,4%) e di psicologi o operatori delle Asl (49,9%)" (fonte: sito Censis).

Sul medesimo tema, Telefono Azzurro ONLUS ha esposto i dati relativi alle richieste di aiuto gestite nel periodo 1° settembre 2015 – 30 giugno 2016 in uno specifico dossier (*Bersagli senza difese? non lasciamoli soli. Dossier bullismo e cyberbullismo. Anno scolastico 2015-2016*). Sono riconducibili a casi di bullismo e cyberbullismo il 13% (pari a 270 segnalazioni) del totale dei casi gestiti dall'Associazione. Di queste richieste di aiuto, il 10% sono da riferirsi a casi di *cyberbullismo*.

IL DISEGNO DI LEGGE A.S. n. 1261-C
"Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"

Il disegno di legge in commento è stato approvato in prima lettura dal Senato (il 20 maggio 2015), in seconda lettura dalla Camera dei deputati (il 20 settembre 2016). Nuovamente giunge all'esame dell'Assemblea del Senato, dopo la conclusione dell'esame in sede referente presso la Commissione Affari costituzionali (il 25 gennaio 2017).

La *navette* risponde ad una diversità di approccio da parte dei due rami del Parlamento.

Le letture in Senato (quella iniziale; la nuova successiva in sede referente, che ha inteso tornare alla originaria impostazione, ripristinando alcune disposizioni nel testo quale approvato in prima lettura) mirano ad introdurre una disciplina del solo fenomeno del *cyberbullismo* né intendono incidere disposizioni di natura penalistica. La lettura intervenuta presso la Camera dei deputati ha optato per un ampliamento della disciplina al fenomeno del bullismo tutto (del quale il *cyberbullismo* è inteso come una specifica declinazione), insieme incidendo su disposizione del codice penale (relativa allo *stalking*).

Il disegno di legge in esame prospetta un insieme di interventi volti a contrastare il *cyberbullismo*, con azioni a carattere *preventivo* anziché repressivo (con estraneità dunque rispetto al diritto penale).

L'obiettivo è una tutela nei confronti dei minori, siano esse le vittime o gli artefici di episodi di *cyberbullismo*.

Di questo viene (innovativamente) resa dall'**articolo 1, comma 2** una definizione normativa, alla stregua di "*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*".

Secondo tale definizione normativa, la vittima (o le vittime) sono necessariamente minori. Non così il bullo, che può ben essere maggiorenne.

Nella definizione normativa così resa, figura l'espressione "forme di pressione". *Parrebbe suscettibile di approfondimento, se tale dicitura identifichi in modo adeguato le condotte rilevanti*, pur nella specificazione che esse siano "in danno" del minore.

Nella definizione normativa, figura altresì l'espressione "per via telematica". *Invero, altra locuzione - ossia "attraverso strumenti informatici o telematici" - parrebbe doversi dire ricorrente*, là dove le condotte facciano riferimento ad alcuni illeciti (qui caratterizzati dall'uso della via telematica) in gran parte già puniti dall'ordinamento penale come reato.

In particolare, in relazione al reato di *stalking* (articolo 612-*bis* c.p., "Atti persecutori"), è attualmente previsto un aumento di pena quando il fatto è commesso "attraverso strumenti informatici o telematici". L'aggravante "telematica", introdotta nel 2013, si inserisce in un filone di interventi volti a codificare l'estensione dell'applicabilità di fattispecie penali alle condotte commesse attraverso l'uso della rete, affiancando così l'opera della giurisprudenza.

Su altra materia, l'addestramento a fini di terrorismo di cui all'art. 570-*quinquies* c.p., modificato dal decreto-legge n. 7 del 2015, punisce con una aggravante il reato commesso "attraverso strumenti informatici o telematici".

In generale, tale locuzione ricorre in riferimento a più reati previsti dal codice penale.

Ancora l'**articolo 1** reca, al **comma 3**, una definizione normativa, concernente il "gestore del sito internet".

Tale è inteso "*il prestatore di servizi della società d'informazione, diverso da quello degli articoli 14, 15 e 16 del decreto legislativo n. 70/2003, che sulla rete Internet cura la gestione dei contenuti di un sito*".

Richiamato è qui il decreto legislativo n. 70 del 2003 (che ha recepito nell'ordinamento italiano la direttiva 2000/31/CE). Esso definisce "servizi della società d'informazione" le attività economiche svolte *on line*, (nonché qualsiasi servizio prestato normalmente dietro retribuzione a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi).

Gli articoli 14, 15 e 16 del decreto legislativo n. 70 del 2003, richiamati dalla disposizione del disegno di legge, fanno riferimento a tipologie particolari di prestatori di servizi della società d'informazione.

Si tratta dei *provider* che provvedono a: la mera trasmissione di dati sulla rete (attività di *mere conduit*: articolo 14); la memorizzazione

temporanea di dati (attività di *caching*: articolo 15); la memorizzazione di più lungo periodo delle informazioni (attività di *hosting*: articolo 16).

Per le attività di *mere conduit* (articolo 14), secondo la normativa europea così recepita il prestatore è comunque non responsabile, a meno che non dia origine o modifichi la trasmissione o non ne selezioni il destinatario.

Per le attività di *caching* (articolo 15), il prestatore non è responsabile se non modifichi le informazioni e se agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione. Ad ogni modo l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore impedisca o ponga fine alle violazioni commesse.

Per le attività di *hosting* (articolo 16), il prestatore non è responsabile se non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita (e per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione) e se, non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore impedisca o ponga fine alle violazioni commesse.

Dunque si profilano esclusi dalla definizione di "gestore" (e dall'ambito di applicazione del provvedimento) gli *access provider* (ossia i *provider* che forniscono connessione ad Internet: ad esempio Vodafone o Telecom Italia) nonché i *cache provider* (i *provider* che memorizzano temporaneamente siti web). Rientrano invece nella definizione di "gestori" tutti i fornitori di contenuti su Internet.

Per quanto riguarda i motori di ricerca (ad esempio Google), parrebbe doversi valutare se essi si rivelino meri *hosting provider* (per i quali varrebbero le previsioni sopra ricordate del decreto legislativo n. 70 del 2003 di recepimento) ovvero vi si realizzi una gestione *dei contenuti*.

Secondo quanto introdotto nel corso dell'esame del disegno di legge presso la Camera dei deputati, la gestione (non solo del sito, com'era originariamente previsto nel testo licenziato dal Senato in prima lettura, ma) dei contenuti importerebbe inclusione nella nozione di "gestore" ai sensi della disciplina qui introdotta.

Si tratta di materia invero assai tecnica e complessa, ed in divenire giurisprudenziale. Può ricordarsi per questo riguardo la sentenza della Corte di giustizia dell'Unione europea del maggio 2014 nella causa C-131/12 (cd. "causa Google Spain"), la quale ha affermato che il gestore di un motore di ricerca sia responsabile, ai sensi della normativa europea in

materia di tutela della *privacy*, del trattamento da esso effettuato dei dati personali che appaiono su pagine web pubblicate da terzi.

Rimane, ad ogni modo, che la previsione del disegno di legge debba risultare conforme alla normativa europea.

L'**articolo 2** istituisce una specifica *procedura dinanzi al Garante per la protezione dei dati personali*, che consenta a ciascun minore ultraquattordicenne o ai genitori della vittima minorenni di ottenere una tutela rafforzata.

Tale tutela è volta all'adozione di provvedimenti inibitori e prescrittivi (oscuramento, rimozione o blocco dei dati personali diffusi su *Internet* o *social network*) che garantiscano la dignità del minore oggetto di atti di cyberbullismo.

Permane la conservazione dei dati originali, nella forma della "URL", vale a dire una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in *Internet*.

La tutela è attivabile anche quando la diffusione non concreti un "trattamento illecito di dati" previsto dall'art. 167 del Codice della *privacy* (decreto legislativo n. 196 del 2003) o da altre norme incriminatrici.

La richiesta al Garante può essere proposta:

- sia quando non sia possibile identificare il titolare del trattamento (o il gestore del sito o del *social network*);
- sia quando quest'ultimo, richiesto dall'interessato, non abbia provveduto entro 48 ore all'adozione dei provvedimenti inibitori e prescrittivi.

Il Garante, entro 48 ore dalla segnalazione del minore (o del genitore) provvede ai sensi degli articoli 143 e 144 del Codice della *privacy*.

Pertanto, se non invita il titolare ad effettuare il blocco spontaneamente, gli prescrive le misure opportune o necessarie per rendere il trattamento conforme alla legge. In caso di mancato adempimento o anche direttamente, il Garante dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto.

Analoghe misure possono essere adottate quando, in considerazione della natura dei dati o comunque delle modalità del trattamento o degli effetti che esso può determinare, vi sia il concreto rischio di un pregiudizio rilevante per il minore.

L'**articolo 3** prevede al **comma 1** l'istituzione presso la Presidenza del Consiglio dei ministri (con decreto del suo Presidente) di un *tavolo tecnico per la prevenzione e il contrasto del cyberbullismo*, senza oneri per la finanza pubblica.

Il decreto deve essere adottato entro 30 giorni dall'entrata in vigore del provvedimento.

Al tavolo si prevede partecipino rappresentanti dei Ministeri dell'interno, dell'istruzione, del lavoro, della giustizia, dello sviluppo economico, della salute; della Conferenza unificata e dell'ANCI; 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, del Garante per la protezione dei dati personali.

Al tavolo prendono inoltre parte i rappresentanti di associazioni con comprovata esperienza nella promozione dei diritti dei minori e degli adolescenti e nelle tematiche di genere, ed una rappresentanza sia delle associazioni studentesche e dei genitori sia delle associazioni attive nel contrasto del cyberbullismo. Del pari vi partecipano operatori di *social network* e della rete *internet*.

Non è prevista la corresponsione di alcun compenso, indennità, gettone di presenza, rimborso spese o emolumento comunque determinato.

Ai sensi del **comma 2**, il coordinamento del tavolo tecnico è affidato al MIUR.

Il tavolo è chiamato a redigere, entro sessanta giorni dal suo insediamento, un piano di azione integrato per il contrasto e la prevenzione del *cyberbullismo* (nel rispetto delle disposizioni dell'Unione Europea in materia e nell'ambito del programma pluriennale UE: v. decisione 1351/2008/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativa ad un programma comunitario pluriennale per la protezione dei bambini che usano Internet e altre tecnologie di comunicazione) nonché un sistema di raccolta di dati a fini di monitoraggio del fenomeno.

I **commi 3 e 4** disciplinano i contenuti del predetto piano di azione.

Il piano è integrato con il codice di autoregolamentazione per la prevenzione e il contrasto del *cyberbullismo*, rivolto sia agli operatori che forniscono servizi di *social networking*, sia agli altri operatori delle rete *Internet*.

Il codice deve prevedere l'istituzione di un comitato di monitoraggio al quale è assegnato il compito di identificare procedure e formati *standard* per l'oscuramento, la rimozione o il blocco di qualsiasi dato personale del minore diffuso in *Internet* (cfr. articolo 2 *supra*) e di adottare un marchio di qualità da attribuire ai fornitori di servizi di comunicazione elettronica e, in ogni caso, ai produttori di dispositivi elettronici che aderiscono ai progetti elaborati dal tavolo tecnico, in base alle modalità stabilite dal d.P.C.m. da emanare ai sensi del comma 1.

Anche per i soggetti che partecipano ai lavori del comitato di monitoraggio non è prevista la corresponsione di alcun compenso, indennità, gettone di presenza, rimborso spese o emolumento comunque determinato.

Con il piano di azione integrato devono essere inoltre stabilite le iniziative di informazione e di prevenzione del fenomeno del *cyberbullismo* rivolte ai cittadini, con il coinvolgimento delle strutture socio-educative.

Alla Presidenza del Consiglio è affidato il compito di attivare sui principali *media* campagne informative periodiche di prevenzione e sensibilizzazione sui fenomeni indicati (**comma 5**). Obblighi di relazione annuale alle Camere sulle attività svolte dal citato tavolo tecnico sono previsti in capo al MIUR (**comma 6**).

Infine è presente disposizione di copertura finanziaria, con autorizzazione di spesa per 50.000 euro a decorrere dal 2017 (**commi 7 e 8**).

L'**articolo 4** prevede l'adozione da parte del MIUR di *linee di orientamento per la prevenzione e il contrasto del cyberbullismo* nelle scuole (anche avvalendosi della collaborazione della Polizia postale), da aggiornare con cadenza biennale (**comma 1**).

Le linee di orientamento - per il triennio 2017-2019 - devono includere, tra gli obiettivi: la formazione del personale scolastico; la promozione di un ruolo attivo degli studenti (nonché di ex studenti che già abbiano operato entro l'istituto scolastico in attività di *peer education*) nella prevenzione e nel contrasto dei fenomeni nelle scuole; la previsione di misure di sostegno e rieducazione dei minori coinvolti, un sistema di *governance* efficace, diretto dal MIUR (**comma 2**).

Si prevede inoltre l'individuazione in ogni scuola di un docente con funzioni di referente per le iniziative contro il bullismo e il *cyberbullismo*.

Il referente coordina le diverse iniziative di prevenzione e contrasto dei fenomeni, anche collaborando con le Forze di polizia e le associazioni giovanili (o i "centri di aggregazione giovanile") presenti sul territorio (**comma 3**).

Si demanda agli uffici scolastici regionali la promozione della pubblicazione di bandi per il finanziamento di progetti di particolare interesse elaborati da reti scolastiche per azioni integrate di contrasto al *cyberbullismo* e di educazione alla legalità, con il coinvolgimento di un novero di istituzioni pubbliche così come associative private. Nel sito *internet* dei medesimi uffici scolastici regionali devono essere pubblicati i bandi, l'entità dei finanziamenti, i loro beneficiari, i dettagli dei progetti finanziati (**comma 4**).

Alle scuole di ogni ordine e grado è demandata la promozione dell'educazione all'uso consapevole delle rete *Internet* e ai diritti e doveri derivanti dal suo utilizzo (**comma 5**).

Progetti di sostegno dei minori vittime di *cyberbullismo* nonché iniziative rieducative - anche attraverso attività riparatorie o di utilità sociale - dei minori autori degli atti, sono adottati dai servizi territoriali (**comma 6**).

L'**articolo 5** affida al dirigente scolastico il compito di *informare tempestivamente i genitori* (o i tutori) dei minori coinvolti in atti *cyberbullismo* (salvo che il fatto costituisca reato).

Sentite le famiglie e valutata la gravità degli episodi, il dirigente convoca i minori coinvolti, il referente scolastico (di cui all'articolo 4) e i rappresentanti di classe per l'adozione delle misure necessarie (di sostegno e disciplinari).

Viene previsto, infine, l'aggiornamento degli attuali regolamenti scolastici con i necessari riferimenti a *cyberbullismo* e relative sanzioni disciplinari.

L'**articolo 6** prevede misure di sostegno all'attività della *Polizia postale*, cui sono inoltre assegnati obblighi annuali di relazione al tavolo tecnico (di cui all'articolo 3) sui risultati dell'attività di contrasto al *cyberbullismo*.

In particolare, per le attività in ambito scolastico connesse all'uso sicuro di *Internet* e alla prevenzione del *cyberbullismo*, è previsto un finanziamento di 203.000 euro all'anno nel triennio 2017-2019 a favore del Fondo per il contrasto alla pedopornografia su *Internet*, istituito dalla legge 48 del 2008 nello stato di previsione del Ministero dell'interno.

L'**articolo 7** ha per oggetto l'*ammonimento del questore*.

È misura finalizzata sia ad evitare il ricorso alla sanzione penale sia a rendere il minore consapevole del disvalore del proprio atto.

La sua disciplina è mutuata da quella dello *stalking* (articolo 612-*bis* c.p.).

Viene previsto che, fino a quando non sia stata proposta querela o presentata denuncia da parte delle vittime (per ingiuria, diffamazione, minacce - cfr. rispettivamente artt. 594, 595, 612 c.p. - o trattamento illecito di dati personali commessi mediante *Internet*), il questore - assunte se necessario informazioni dagli organi investigativi e sentite le persone informate dei fatti - alla presenza di almeno un genitore (o altro esercente la potestà genitoriale) possa convocare il minorenne ultraquattordicenne

responsabile di atti di *cyberbullismo* nei confronti di altro minorenni, ammonendolo oralmente ed invitandolo a tenere una condotta conforme alla legge.

Dell'ammonimento è redatto processo verbale. L'ammonimento cessa di avere effetto al compimento della maggiore età.

La disposizione non prevede misure conseguenti alla violazione delle prescrizioni impartite con l'ammonimento.

La seconda lettura presso il Senato ha soppresso quanto deliberato dalla Camera dei deputati circa l'introduzione entro l'articolo 612-*bis* del codice penale di una nuova circostanza aggravante del reato di atti persecutori (*stalking*).

Attualmente lo *stalking* commesso per via informatica o telematica è sanzionato con un aumento di pena fino a un terzo (la pena base è la reclusione da 6 mesi a 5 anni).

La modifica introdotta dalla Camera dei deputati prevedeva per lo *stalking* informatico o telematico la reclusione da 1 a 6 anni.

Analoga pena era prevista se il reato fosse commesso con specifiche modalità: con scambio di identità e l'invio di messaggi o divulgazione di testi o di immagini ovvero mediante diffusione di dati sensibili immagini o informazioni private, carpite con l'inganno o con minacce o comunque detenuti o, ancora, mediante realizzazione e diffusione di documenti contenenti la registrazione di fatti di violenza e di minaccia.

Ancora la disposizione introdotta dalla Camera dei deputati prevedeva la confisca obbligatoria dei beni e degli strumenti informatici e telematici utilizzati per la commissione del reato.