Dipartimento di Scienze Politiche

Cattedra di Diritto dell'informazione e della comunicazione (c.p.)

STRUMENTI DI TUTELA CONTRO IL CYBERBULLISMO NEGLI ORDINAMENTI CONTEMPORANEI E NELLE POLICIES DEI SOCIAL NETWORK

RELATORE

CHIAR.MO PROF.
Pietro Santo Leopoldo Falletta

CANDIDATO

Camilla Bistolfi
MATR. 620722

CORRELATORE

PROF. Michele Sorice

ANNO ACCADEMICO 2013/2014

Indice

Introduzione

Il 20 aprile del 1999, gli Stati Uniti furono sconvolti dal massacro della *Columbine High School*, nel quale persero la vita 12 studenti e un professore, per mano di due adolescenti che frequentavano quell'istituto. La tragedia sollevò numerosi dibattiti, non solo riguardanti la vendita e la reperibilità di armi da fuoco negli stati americani, ma anche e soprattutto relativi al fenomeno del bullismo. Infatti, i due studenti confessarono di aver perpetrato i delitti per vendicarsi delle prepotenze subite dai bulli della scuola.

Solo otto giorni dopo, il Canada venne scosso dalla sparatoria tenutasi nella *W. R. Myers High School* ad Alberta, dove un quattordicenne tolse la vita ad uno studente e ne ferì gravemente un altro. Il ragazzo si rivelò essere vittima di atti di bullismo da molto tempo e, come raccontò la sua famiglia, ebbe un crollo subito dopo gli eventi della *Columbine High School*, che lo spinsero all'insano gesto.

Quel 28 aprile, racconta l'insegnante canadese Bill Belsey[1], era iniziato come tanti, ma cambiò la sua vita per sempre. Infatti, sconvolto dai fatti, diede immediatamente vita al sito www.bullying.org per aiutare le giovani vittime del bullismo. Il motto della pagina web, "*Where you are NOT alone*" sottolinea ancora oggi l'attività di supporto e di sostegno che si concretizza, tra l'altro, nella creazione di una vera e propria community in cui si possono condividere storie ed esperienze.

Tradizionalmente 3il bullismo viene considerato come un atto o una serie di comportamenti prepotenti, perpetrati da bambini e ragazzi nei confronti dei loro coetanei[2]. Oggi, però, questo fenomeno ha assunto nuove forme e si è diffuso attraverso la rete, che costituisce uno dei principali e più potenti strumenti intimidatori nelle mani dei bulli. E' stato lo stesso Bill Belsey, nel 2005, a coniare il termine cyberbullismo, intendendo con esso l'uso delle nuove tecnologie che ha come fine quello di supportare un comportamento deliberatamente e ripetutamente ostile nei confronti di altri individui. Ciò, ovviamente, può avvenire attraverso SMS

[1] B. Belsey, *Cyberbullying: an emerging threat to the "always on" generation,* in www.cyberbullying.ca.

[2] S. Pisciotta, *Lessico oggi. Orientarsi nel mondo che cambia*, Rubbettino, Catanzaro 2003.

o e-mail, persino con l'uso degli MMS, ma assume caratteri decisamente più gravi qualora avvenga sulla rete, nei blog, nei forum, su siti internet o nei social network. Infatti, è molto diverso subire delle prepotenze in privato (ad esempio via chat), piuttosto che esserne vittima pubblicamente, soprattutto considerando che il web è accessibile da chiunque in qualunque momento. La varietà di strumenti pone, quindi, di fronte ad una delle questioni relative ad internet più spinose degli ultimi vent'anni, cioè quella del corretto bilanciamento tra libertà di manifestazione del pensiero e gli altri diritti della personalità, quali l'onore, la reputazione e l'identità personale. Infatti, il cyberbullo non si limita alla pubblicazione di pettegolezzi e di bugie, ma attacca direttamente la vittima con materiali diffamanti ed umilianti. Addirittura, spesso si assiste alla creazione di un vero e proprio sito web (o di un blog) contenente informazioni umilianti e imbarazzanti per chi viene preso di mira, oppure vengono creati sondaggi che lo offendono deliberatamente. Queste caratteristiche hanno reso il bullismo elettronico un tipo di *hate speech*, poiché l'intento è mettere in ridicolo, screditare e convincere chi legge ad odiare ed insultare a sua volta la vittima. Spesso, infatti, le molestie non si limitano ad affermazioni ingiuriose relative alla persona e al suo aspetto, ma vengono perpetrate dando origine a una diffamazione che verte sulle qualità del soggetto (età, sesso, razza, religione, orientamento sessuale, handicap). E' il caso, ad esempio, del video apparso su YouTube e girato a Grosseto mentre una ragazza di colore veniva assalita da un gruppo di coetanei (vedi *infra* pag. 155). Ancora, la discriminazione può vertere sugli handicap, come nella celebre vicenda che ha visto l'associazione Vividown ricorrere in giudizio contro Google (vedi *infra* pag. 159).

Il fenomeno del cyberbullismo, in realtà, non è limitato ai rapporti tra minori. Infatti, molto spesso viene perpetrato anche da adulti a discapito di altri adulti, ma in questo caso si tende ad identificarlo, nella maggioranza degli stati, come *cyberstalking*, includendo in esso anche il furto di identità, le molestie e le minacce tra soggetti *over* 18. Inoltre, il cyberbullismo non va confuso con il *cyberbaiting*, una versione di bullismo in cui gli studenti tormentano i loro insegnanti catturandone la reazione con un cellulare e inserendo il video o la foto online per umiliarli di fronte a tutti.

Secondo il Rapporto Norton Online Family del 2011[3], a livello globale, un insegnante su cinque ha sperimentato personalmente *cyberbaiting* o conosce un altro insegnante che ne è stato vittima.

Tornando al cyberbullismo, non è un caso se, qualche tempo dopo aver coniato questo nuovo termine, Bill Belsey creò il primo sito al mondo dedicato al bullismo elettronico, www.cyberbulling.org.

Vista l'attualità del tema, l'opera cinematografica intitolata *Disconnect*[4] presenta, in uno dei suoi tre episodi, la vicenda di un ragazzo che viene adescato su Facebook da due compagni di scuola. Questi, dopo aver creato un falso profilo, fingono di essere una ragazza infatuata del giovane e gli chiedono di inviare una foto succinta in chat privata. L'immagine viene poi inoltrata dai due cyberbulli ai numeri di telefono di tutta la scuola, il che spinge la vittima a tentare il suicidio, impiccandosi nella sua camera da letto per la vergogna di essere diventata lo zimbello di tutta la scuola.

Sfortunatamente, la pellicola è un *exemplum* di quanto avviene nella realtà. Infatti, già nel 2004 da una ricerca della iSafe American[5] risultava che 42% dei ragazzi intervistati era stato vittima di bullismo online e, ad oggi, sono sempre più numerosi i casi di suicidio tra i giovanissimi. Nel 2013, in provincia di Padova e a Lutterworth, a distanza di qualche giorno l'una dall'altra, due quattordicenni si sono tolte la vita dopo essere state a lungo oggetto di scherno su Ask.fm (vedi *infra* pag. 178 e 181). Sempre nel 2013, Rebecca Sedwick, a soli 12 anni, ha conosciuto la stessa sorte in Florida, mentre un anno prima, in Australia, Amanda Todd si toglieva la vita a seguito degli insulti ricevuti su Facebook (vedi *infra* pag. 185). Non è un caso se, a seguito di questi tragici eventi, sono nati decine e decine di siti, tra cui www.cyber-bullying-facts.com, www.cyberbullyingprevention.com, stopcyberbullying.org che offrono tecniche di prevenzione e metodi di sostegno alle famiglie e alle vittime del bullismo in rete.

[3] it.norton.com/cybercrimereport.

[4] *Disconnect*, regia di Henry Alex Rubin, 2103.

[5] iSafe America, 2004 Survey of students nationwide, *Cyber Bullying: statistics and tips,* in www.isafe.org.

In realtà, già nel settembre del 2010 il fenomeno era divenuto oggetto di dibattito e di studio, quando il diciottenne Tyler Clementi si era lanciato dal ponte George Washinghton. Il 19 settembre, infatti, il suo compagno di stanza, Dharun Ravi con la complicità di un altro studente della Rutgers University, Molly Wei, aveva usato una webcam per visualizzare, senza il consenso di Clementi, il bacio tra la vittima e un altro ragazzo. Due giorni dopo, Ravi aveva esortato amici e *followers* di Twitter a guardare attraverso la sua webcam il secondo appuntamento tra Clementi e il suo partner, anche se la visione non si verificò mai.

Nonostante l'indubbio ruolo nel suicidio di Tyler, i suoi due compagni sono stati incriminati solo per la questione riguardante la violazione della privacy commessa con l'uso della webcam. La morte di Clementi, quindi, ha portato all'attenzione nazionale e internazionale non soltanto le difficoltà che affrontano i giovani LGBT, ma soprattutto il problema del cyberbullismo. Nel novembre del 2010, infatti, in risposta al suicidio di Clementi e ad altri incidenti simili, i rappresentanti dell'Assemblea Generale del New Jersey (Valerie Vainieri Huttle e Mary Pat Angelini) introdussero con un accordo bipartisan l' "*Anti-bullying Bill of Rights*", che ottenne 71 voti favorevoli ed 1 solo voto contrario nell'Assemblea e l'intero consenso del Senato.

Chiaramente, a spingere Clementi e molti suoi coetanei al suicidio deve essere stato un insieme di altri fattori aggiuntivi, che precedono o vanno di pari passo con le prepotenze sul web, contribuendo alla decisione di togliersi la vita. Ciò che è certo, però, è che il cyberbullismo ha delle conseguenze gravi sulle vittime e può assumere un ruolo di centralità nel loro senso di inadeguatezza, tanto che sul sito www.cyber-bullying-facts.com vengono elencati i cd. "*warning signs*", che consentono di capire se un ragazzo è vittima di prepotenze elettroniche e tra essi vengono citati stati d'animo quali la scarsa autostima, l'ansia, la paura e la depressione, spesso accompagnati da una devianza dalla normale routine, come la tendenza ad isolarsi e ad ottenere voti più bassi a scuola[6].

[6] S. Hinduja, J. W. Patchin, *Cyberbullying: An exploratory analysis of factors related to offending and victimization*, Deviant Behavior, 2008 (129–156) e S. Hinduja, J. W. Patchin, *Offline consequences of online victimization: school violence and delinquency*, Journal of School Violence, 2007 (89–112).

I direttori del *Cyberbullying Research Center*, Sameer Hinduja e Justin W. Patchin hanno iniziato a studiare il fenomeno sin dal 2002, per poi fondare, tre anni dopo, il sito www.cyberbullying.us con lo scopo di promuovere la loro ricerca a supporto delle vittime e dei familiari. Nell'articolo intitolato "*Bullying, cyberbullying and suicide*"[7], i due studiosi spiegano come l'esperienza del bullismo sia un fattore collegabile all'intenzione suicida. Infatti, l'essere bersagli del bullismo elettronico contribuisce alla depressione e ad una ridotta autostima, facendo maturare nella vittima disperazione e solitudine, che sono precursori di pensieri e comportamenti suicidi.

Per evitare di cadere nella trappola dei cyberbulli, il sito www.cyberbullyingprevention.com propone addirittura il download di un pacchetto gratuito di prevenzione in cui vengono illustrati "*the who, what, where, why and how's of cyber-bullying*", seguiti da una spiegazione rivolta agli adulti basata, da un lato, sulle "*technology solutions*" (software antivirus e *antispyware* gratuiti, *firewall*, impostazioni di Windows per filtrare i contenuti internet, *kid-save web browser* e norme basilari di sicurezza sul web) e dall'altro sulle "*social solutions*" (5 regole della *Cyber-etiquette* da insegnare ai bambini e 5 trucchi nell'uso di internet).

Oltre ai siti più tecnici, come quello ideato da S. Hinduja e J. Patchin, ve ne sono moltissimi altri che si rivolgono in primis ai giovani e alle loro famiglie, come nel caso di stopcyberbullying.org. Al suo interno, infatti, sono presenti moltissime sezioni, che vanno dalla definizione del problema a piccoli test autovalutativi rivolti ai bambini e ai ragazzi per capire se sono o meno cyberbulli. Un altro aspetto interessante che indica la complessità del fenomeno, è proprio l'individuazione di diverse tipologie di "cyberbullo" che si riassumono in quattro diversi atteggiamenti:

1. il cd. "*vengeful angel*" che non si vede come un bullo, bensì come giustiziere, per proteggersi o proteggere altri (spesso amici) da colui che sta bersagliando, così da vendicarsi o dargli una lezione;
2. il "*power-hungry*", spesso vittima di bullismo offline e appagato dall'idea di avere un pubblico di utenti che leggono e partecipano alle sue offese;
3. sul versante opposto si trova la cd. "vendetta dei *nerd*", in cui il bullismo elettronico avviene *one-to-one* e il bullo non confida la sua attività a nessun altro,

[7] S. Hinduja, J. W. Patchin, *Bullying, cyberbullying, and suicide*, Archives of Suicide Research, 2010 (206-221).

avvalendosi delle sue competenze tecnologiche, spesso molto elevate, per prendere di mira la vittima;

4. in ultimo, vi sono le "*mean girls*", gruppetti di bulli che, insieme, si accaniscono su un soggetto per "intrattenersi" e "divertirsi".

In realtà, a queste quattro tipologie se ne aggiunge una quinta, costituita dal "cyberbullo involontario", che si scatena a seguito di provocazioni da parte di altri bulli, senza aver premeditato le risposte, ma reagendo con rabbia e frustrazione.

Entrando nel merito del fenomeno, stopcyberbullying.org precisa l'esistenza di due tipi di bullismo online: gli attacchi diretti (messaggi inviati direttamente alla vittima), che si articolano in dieci diverse varianti:

1. Messaggistica istantanea/SMS:
   - creazione di un nickname (ad es. nelle *chatroom*) molto simile a quello di un altro ragazzo. Il nome di solito ha una lettera di troppo o una in meno. Così facendo, il cyberbullo posta frasi inappropriate rivolte ad altri utenti, passando per la vittima;
   - *text attacks.* Sono vere e proprie guerre che il bullo scatena contro la vittima, inviandole migliaia di messaggi sul cellulare;
   - messaggi di odio;
   - minacce di morte (anche attraverso l'uso di foto e video).
2. Furto della password:
   - può avere come obiettivo quello di far sì che il bullo, rubata la chiave d'accesso, possa chattare con altre persone, spesso offendendole e fingendo di essere la vittima;
   - è usato anche per poter cambiare il profilo della vittima, inclusi i dati anagrafici, postando descrizioni razziste o offensive al fine di attirare attenzioni indesiderate e di offendere le persone;
   - può essere seguito da una modifica della chiave d'accesso, così da impedire alla vittima di collegarsi con il suo account;
   - può essere funzionale all'hackeraggio del computer della vittima.
3. Blog:
   - in alcuni casi viene creato a nome della vittima e vi vengono caricati contenuti offensivi o inappropriati;

- può appartenere al cyberbullo ed essere riconducibile a lui, ma questi lo utilizza per postare affermazioni crudeli e imbarazzanti sulla vittima.

4. Siti web:
   - possono essere creati appositamente per insultare qualcuno ripetutamente;
   - spesso vengono utilizzati per caricare materiale fotografico che ritrae la vittima.
5. Invio di foto tramite e-mail e cellulare:
   - *mass e-mail*. Spesso contiene immagini di nudo o degradanti per la vittima e viene spedita a centinaia di indirizzi di posta elettronica;
   - MMS inviati all'intera rubrica.
6. Sondaggi via internet (le domande sono spesso molto offensive o implicano un giudizio estetico/di valore sulla vittima).
7. Giochi online (il cyberbullo si accanisce durante la sfida, usando un linguaggio osceno e minacciando la vittima. Nei casi di giochi per PC, il computer di quest'ultima viene hackerato).
8. Invio di virus, *spyware* e programmi di *hacking* (ad esempio i *Trojan Horse*, che consentono l'accesso in remoto al computer della vittima).
9. Sottoscrizioni a *newsletter* e e-mail di marketing (il cyberbullo iscrive la mail della vittima agli aggiornamenti di siti porno o di altri portali web).
10. *Impersonation*. Il bullo crea un account fingendosi la vittima e inviando a nome di essa messaggi offensivi, spesso fornendone nome, indirizzo e numero cellulare).

Un secondo modo di esercitare il cyberbullismo online è quello che viene chiamato "*by proxy"*, per "delega" (il cyberbullo si serve di un altro soggetto per tormentare la vittima e spesso il complice ne è inconsapevole). Questa tipologia è la più pericolosa poiché spesso coinvolge gli adulti o soggetti terzi e la cd. *warning wars* ne è un esempio. Infatti, molti ISPs offrono un modo per segnalare un utente che sta dicendo qualcosa di inappropriato, cioè il "*warn button*". Ebbene, i ragazzi spesso lo utilizzano per mettere nei guai la vittima segnalandola moltissime volte, nonostante le sue siano affermazioni del tutto inoffensive, oppure per far sì che il server, ricevuti gli *alert*, la disconnetta, precludendole l'uso della pagina.

Spesso, poi, accade che il cyberbullo faccia sembrare la vittima colpevole, mostrando ai propri genitori o all'ISP che si sta solo difendendo dalle offese che questa gli arreca, così gli adulti o i gestori del sito se la prendono con il soggetto che in realtà riceve gli insulti e le minacce.

Ancor più grave è il caso in cui il bullo inserisce negli *hate groups* i dati personali della vittima (nome, cognome, indirizzo, numero di cellulare, scuola etc…) per far sì che i membri della community facciano il lavoro sporco al suo posto. In alcuni casi, addirittura, il cyberbullo ha inserito le informazioni sulla vittima in siti frequentati da pedofili, istigandoli a contattarla per ottenere prestazioni sessuali.

Insomma, ciò che spaventa del cyberbullismo, sono le abissali differenze rispetto al bullismo tradizionalmente inteso. Infatti, in una generazione di ragazzi "sempre connessi", i bulli possono diffondere i loro messaggi ad un pubblico estremamente esteso e ad una velocità sconosciuta prima dell'avvento di internet. Non meno rischioso è il caso in cui ci sia un furto di identità, per cui il bullo finge di essere la vittima dopo averle rubato la password dell'account. In questi casi è frequente l'invio di messaggi offensivi, ma anche la messa a disposizione di informazioni personali della vittima che incoraggino a contattarla o a deriderla.

Ancora, sempre più diffuso è il cd. *sexting*, cioè la diffusione in rete di foto scattate senza il permesso del soggetto, immortalato nudo o svestito, solitamente in uno spogliatoio o un bagno, con la minaccia di condividere le foto imbarazzanti. Una volta messo in atto il ricatto, le foto possono essere condivise con centinaia di persone nel giro di poche ore, creando siti web, blog, sondaggi e altro. Considerato che si tratta di minori, è chiara la gravità del fenomeno, giacché una volta postati, i contenuti possono essere scaricati, copiati o linkati, rendendo difficoltosa la loro eliminazione dalla rete. Inoltre, con qualche capacità tecnica in più, molti giovani bulli inviano virus, *spyware* o programmi di *hacking* alla vittima, al fine di spiarla o controllarne il computer con accesso remoto.

A ciò si aggiunge il fatto che il cyberbullo può facilmente nascondere la sua identità, mantenendo l'anonimato che la rete permette di ottenere. Diventa, quindi, estremamente difficile rintracciare coloro da cui hanno origine le prepotenze.

Si pone, in tal senso, oltre alla mancanza di controllo degli adulti sulle attività online dei minori, anche l'annosa questione della privacy, che investe nello specifico la

responsabilità degli *Internet Service Providers* di comunicare i dati personali degli utenti al fine di renderli rintracciabili. E, ancora, sempre a proposito dei *providers*, è complicato definire se appartenga o meno a loro il compito di rimuovere quei contenuti che costituiscono veri e propri atti telematici di bullismo.
Un'altra riflessione sorge in relazione alla sovra citata questione delle *warning wars*. Infatti, i prestatori di servizi sono consapevoli dell'abuso che certi giovani utenti fanno del "*warn button*" e, laddove impediscano l'accesso della vittima alla pagina web, diventano complici innocenti del cyberbullo.

L'aspetto interessante del fenomeno risiede proprio nella sua capacità di richiamare i temi più importanti e complessi che sono sorti con l'uso (e abuso) della rete. Come si vedrà nel primo capitolo, il cyberbullismo costituisce un vero e proprio reato in alcuni paesi, mentre in molti altri la regolazione del fenomeno resta incerta e in via di sviluppo. Per questo si è deciso di prendere in esame le fonti statunitensi in materia, che costituiscono senz'altro uno dei pilastri per la lotta al bullismo elettronico e di confrontarle con quanto stabilito e auspicato dalle direttive europee, con un focus sulle sopracitate responsabilità degli ISPs, per capire in che modo essi si comportano e devono comportarsi di fronte a situazioni di cyberbullismo.
Il secondo capitolo analizzerà nel dettaglio le disposizioni esistenti che consentono alle vittime di tutelarsi nei singoli stati, a partire dall'Italia, per poi arrivare sino al Canada, passando attraverso il Regno Unito e la Nuova Zelanda. Un approfondimento sarà, poi, dedicato alla Repubblica di Singapore, che costituisce un esempio orientale virtuoso.
Nel terzo capitolo si vedrà in che modo i social network affrontano le questioni relative al bullismo elettronico, dal momento che oggi essi costituiscono la principale fonte di espressione dei giovani sul web. Non a caso, ciascuna di queste piattaforme fornisce una propria *policy* relativa al cyberbullismo e alle forme di manifestazione del pensiero, che verrà analizzata e rapportata ai principali casi di cronaca.
Infatti, attraverso i vari profili del diritto e grazie alle condizioni d'uso dei social network, si potrà delineare un primo quadro che sarà utile al momento di verificare in che modo i giudici abbiano risolto i diversi casi di bullismo elettronico a partire dalle indagini degli inquirenti, come si vedrà nel secondo approfondimento situato nel

terzo capitolo - preceduto da quello relativo alla piattaforma di *videosharing*, Youtube.

Ciò che si intende dimostrare con questo lavoro è la necessità di un intervento per prevenire e contrastare il fenomeno, che sia coordinato su più fronti: innanzitutto, è auspicabile, da parte degli stati e a livello sovrannazionale, l'adozione di norme giuridiche che favoriscano la regolazione del fenomeno e la tutela delle vittime.
In secondo luogo, a partire da queste disposizioni, è indispensabile che gli Internet Service Providers adottino dei codici che li agevolino nella gestione delle situazioni a rischio. A tal proposito, bisogna capire quali siano le strategie di autoregolamentazione (adottate e adottabili) che consentono di mantenere l'originaria libertà di manifestazione del pensiero sul web.
In terzo luogo, va tenuto in considerazione il fatto che i giovani utenti di internet creano continuamente reti interattive lontano dalla supervisione degli adulti. Infatti, il web è lo strumento perfetto per il bullo, che può raggiungere la sua vittima sempre e ovunque, anche anonimamente. Questo significa che per molti ragazzi, la casa non è più un rifugio dalle prepotenze subite a scuola. Quindi si tratta di agire su altri due livelli, oltreché su quello nazionale/sovrannazionale e dei providers: in primis quello della famiglia, che ha il compito di educare i propri figli al corretto uso della rete e, a seguire, quello della scuola che deve svolgere un'attività di prevenzione e sostegno, fornendo ai ragazzi gli strumenti necessari e le competenze adatte ad arginare il fenomeno e a sapersi difendere legalmente, senza assecondare le prepotenze diventando bulli a loro volta.
Uno scenario del genere, per essere realizzato, necessita di un *frame* normativo solido, di una forte attività statale di promozione scolastica ed extrascolastica e di un comportamento responsabile da parte degli ISPs, perché il cyberbullismo è un affare che riguarda tutti.

Capitolo 1

Profili normativi: una comparazione tra gli Stati Uniti e l'Europa

1.1 – Gli stati americani e le leggi a tutela delle vittime di cyberbullismo

Insieme ai suoi molteplici vantaggi, internet ha portato alla luce una serie di pericoli relativi alle molestie on-line e al cyberbullismo. Inoltre, dal momento che questo mondo virtuale ha delle conseguenze reali nella vita delle persone, sono emerse non poche sfide per i genitori, le scuole e le istituzioni che tentano di stare al passo con le tecnologie in rapido sviluppo e di fornire adeguate protezioni per i minori. La sfida ancora più grande, poi, è quella di riuscire a bilanciare queste protezioni vitali con il diritto di parola, di espressione e di pensiero[8] che da sempre trova sulla rete il suo terreno più fertile.

Negli Stati Uniti, le disposizioni costituzionali vengono messe duramente alla prova da questo tipo di problematiche, poiché i provvedimenti legislativi che renderebbero internet più sicuro, non devono erodere la libertà di espressione garantita dal Primo Emendamento, secondo cui: «Il Congresso non promulgherà leggi […] che limitino la libertà di parola, o di stampa […]».

Così, mentre la *Youth Risk Behavior Survey Surveillance*, nel 2011, aveva rilevato che il 16% degli studenti delle scuole superiori erano stati vittime di bullismo elettronico nel corso dell'anno precedente, ad oggi ancora non esiste una legge federale che valga in particolare per il cyberbullismo. In alcuni casi, quando il bullismo online è basato su razza, colore, origine etnica, sesso, disabilità o religione, esso si sovrappone con le molestie e la discriminazione, quindi le scuole sono legalmente obbligate ad affrontarlo.

Per quanto riguarda i singoli stati, ciascuno ha intrapreso strade diverse per tutelare i minori dal fenomeno, richiedendo collaborazione sia alle scuole che ai distretti.

Per la precisione, il cyberbullismo e i comportamenti correlati possono essere disciplinati in una sola legge o possono essere regolati in più disposizioni.

[8] A. V. King, *Constitutionality of cyberbullying laws: keeping the online playground safe for both teens and free speech*, in www.vanderbiltlawreview.org.

Vista la complessità della materia, il governo statunitense ha dato vita al sito www.stopbullying.gov che consente di visualizzare tutte le *policies* dei singoli stati (aggiornati a febbraio 2014).

Secondo il resoconto del *Cyberbullying Research Center*[9] solo sette stati hanno leggi sul bullismo che contengono il termine "cyberbullismo" e lo considerano un crimine, mentre gli altri fanno semplicemente riferimento a "molestie"/"bullismo elettronico" senza alcuna previsione penale.

Il primo dei sette casi è quello dell'Arkansas, dove dal luglio 2011 è entrata in vigore la "*Cyberbullying crime law*" (*Act 905 of the Regular Session*), *«an act to establish the crime of cyberbullying»*[10] che lo identifica come un reato di classe B. Ciò comporta la previsione di una condanna cui può conseguire una pena detentiva fino a 90 giorni e una multa fino a $1.000 a seconda dell'età e della classe frequentata dallo studente colpevole.

In riferimento a quelli che vengono definiti comportamenti "*off-campus*", la legge vieta il bullismo compiuto con «un atto elettronico che provoca la sostanziale interruzione del regolare funzionamento della scuola o dell'ambiente educativo»[11]. Quindi le disposizioni si applicano «ad un atto elettronico che può essere nato o meno all'interno della scuola o con equipaggiamento scolastico, se esso è diretto specificatamente a studenti o personale della scuola e maliziosamente destinato a scopo di turbare la scuola ed ha una elevata probabilità di successo a tale scopo»[12].

Anche in Louisiana è previsto che chi commette il reato di cyberbullismo potrà essere «multato per non più di cinquecento dollari, arrestato per non più di sei mesi o sottoposto ad entrambe le sanzioni. Tuttavia, quando l'autore del reato è minore di 17 anni, la materia è disciplinata esclusivamente dalla sezione "*Families in Need of Services"* del *Children's Code*»[13].

---

[9] S. Hinduja, J. W. Patchin, *State cyberbullying laws*, 2014 in cyberbullying.us.

[10] Senate Bill 214, *Act 905 of the regular session*, in www.arkleg.state.ar.us.

[11] *6-18-514 Antybullying policies*, in www.arkdisabilityrights.org.

[12] Ibid.

[13] *Burrell (HB 1259) Act No. 989*, in www.legis.la.gov.

Parallelamente, *l'House Bill 1259*, dà ai genitori della vittima la possibilità di presentare una relazione all'ufficio di giustizia minorile. Dall'agosto 2010, inoltre, questa carta fornisce un codice di condotta rivolto agli studenti di tutte le scuole che si accompagna alle previsioni dei *Revised Statutes 14:40.7* e *17:416.13*. Questi, infatti, fanno riferimento alle codotte "*off-campus*", identificandole come perpetrate sia dentro che fuori dalla scuola, ma con l'intento di avere un effetto sulla vittima mentre essa è nel territorio scolastico.

In Missouri, i *Senate Bills nos. 818&795* identificano il reato di cyberbullismo come un crimine di classe A (pena massima: un anno di carcere o una multa di 1.000 dollari) «a meno che sia commesso da una persona che abbia 21 anni o più nei confronti di un minore di diciassette anni o che il colpevole abbia già commesso il reato di molestie. In tali casi, si considera è un crimine di classe D»[14].

In Nevada, con il *Revised Statute 338* ai punti dal 121 al 139 viene definito il cyberbullismo e si richiede al Dipartimento di Stato responsabile dell'istruzione che sviluppi politiche volte a contrastare il fenomeno. Queste devono essere diffuse a studenti, genitori e collaboratori scolastici e devono contenere norme per l'uso etico di internet. Nello specifico, con il *Revised Statue* del 2013, nella sezione §392,915, in determinate circostanze il cyberbullismo viene considerato un reato e ad esso sono applicabili persino le sanzioni penali previste per lo *stalking* (cfr. *Nev. Rev. Stat. Ann. §200,575*) e per le molestie (cfr. *Nev. Rev. Stat. Ann. §200,571*).

Nel North Carolina il *Senate Bill 707* con le modifiche degli *amends 14-458,1*, aggiunge come illecito punibile il cyberbullismo, il quale si applica a comportamenti diretti verso i minori o anche verso i genitori di un minore. E' previsto, inoltre, che esso sia punito come «un reato di classe 1 se l'imputato è maggiore di 18 anni al momento in cui il reato è stato commesso. Se l'imputato ha un'età inferiore, viene punito come un reato di classe 2»[15]. Nel primo caso, il colpevole sconterà da 1 a 120 giorni di «*active, intermediate, or community punishment*»[16], mentre nel secondo, da 1 a 60 giorni.

[14] *Senate Bills nos. 818&795* in www.senate.mo.gov.

[15] Senate Bill 707, amends 14-458,1.

[16] Ibid.

In Tennessee, invece, il *Senate Bill 113* prevede fino a un anno di carcere e una multa 2.500 dollari.

Nello stato di Washinghton, il *Senate Bill 5288* del 2007 ha modificato il *Code of Washinghton §28A.300.285*, aggiungendo il cyberbullismo al *Bullying Act*. Inoltre, ha previsto che entro agosto del 2011 tutte le scuole adottassero una politica per farvi fronte e che esse designassero una persona nel distretto scolastico che fosse responsabile della ricezione e del trattamento dei reclami di bullismo e che fungesse anche da mediatore tra le diverse agenzie statali.

Queste previsioni si accompagnano, ad oggi, a quelle del *WA. Rev. Code. Ann. §9.61.260*, che prevede la possibilità di sanzionare penalmente i cyberbulli applicando la *Cyberstalking Law*[17] nella quale sono previsti fino a novanta giorni di carcere e fino a 1000 dollari di multa nel caso si tratti di *misdemeanor*, oppure fino a cinque anni di detenzione e fino a 10000 dollari di risarcimento nel caso vi siano le aggravanti di cui al comma 3 del *Revised Code of Washinghton §9.61.260*.

Nonostante i considerevoli progressi in materia, molti dei principali stati americani nominano il cyberbullismo all'interno delle leggi sul bullismo tradizionale precedentemente adottate, ma non hanno ancora provveduto a determinarne le conseguenze penali. E' il caso, ad esempio, dello stato di Washington che, fermo restando quanto descritto sopra, nel *Revised Code of Washington*, al titolo 28A, capitolo 28A.300, sezione 285 precisa che «l'associazione dei dirigenti scolastici dello stato di Washington, con l'assistenza dell'ufficio del sovrintendente della pubblica istruzione, convoca un comitato consultivo per sviluppare un modello di politica che vieta gli atti di molestie, intimidazioni o bullismo che vengono svolte tramite mezzi elettronici da un studente mentre è a scuola e durante la giornata scolastica». Inoltre è previsto che questa politica disponga l'adozione di materiali destinati a educare i genitori e gli studenti circa la gravità del cyberbullismo, presentando le opzioni disponibili se uno studente è vittima di bullismo elettronico tra cui la denuncia delle minacce alla polizia locale, il coinvolgimento della scuola o la segnalazione al provider di servizi internet[18].

[17] Revised Code of Washinghton §9.61.260, Cyberstalking.

[18] cit. *Title 28a RCW - Common school provisions* in apps.leg.wa.gov.

L'House of Representatives Bill n. 699 (cd. School *Safety "Jeffrey Johnson Stand Up for All Students Act"*) ha introdotto nella sezione §1006.147 dello statuto della Florida la necessità per i distretti scolastici di rendere chiare le conseguenze del cyberbullismo.

Nello stato di New York, la Commissioner's Regulation 100.2 e le *Education Laws 2801 e 2801-a*, hanno imposto che ciascun consiglio di istruzione adotti e applichi un codice di condotta, che preveda provvedimenti disciplinari da adottare in caso di questioni che coinvolgano l'uso della forza fisica o le molestie elettroniche e non.

Di recente, poi, è stata proposta una legge che introduce sanzioni penali per il cyberbullismo (non ancora approvata) sulla base della *N.Y. Penal Law §240.30*, in cui una persona si considera colpevole di molestie di secondo grado quando «comunica per telefono, per telegrafo, per posta o con altri mezzi elettronici […] e/o commette il reato di molestie in primo grado ed è stata precedentemente condannata per questo».

Nel District of Columbia, il cyberbullismo non compare in nessuna legge ma, pur non esistendo alcuno statuto, grazie al *D.C. Code* può essere perseguito con la legge sullo *stalking* (*Ann. §22-404*).

Parallelamente, lo stato della California nell'*Education code - Title 1, Conference 32265* dispone che ci siano almeno due conferenze regionali annuali affinché vengano ridotti i crimini scolastici, tra cui la prevenzione del bullismo, anche quando commesso tramite mezzi elettronici.

Inoltre, l'*Assembly Bill 746*, approvato nel luglio 2011 per emendare la sezione 32261 dell'*Education Code*, ha stabilito che «il bullismo commesso per mezzo di un atto elettronico […], è un terreno su cui basare la sospensione o l'espulsione» dello studente che ne è artefice.

Nel codice penale californiano[19] le molestie, gli atti intimidatori e quelli di bullismo vengono puniti con pene amministrative in quanto interferiscono con l'esercizio dei diritti garantiti dalla Costituzione. Tuttavia, queste disposizioni si applicano solo ai casi di "*hate crime*", cioè «quegli atti criminali commessi, in tutto o in parte, a causa

[19] *Section 422.6-422.865* of Penal Code of California in www.leginfo.ca.gov.

di uno o più delle seguenti caratteristiche della vittima: disabilità, sesso, nazionalità, razza o etnia, religione e orientamento sessuale […]»[20].

Insomma, non vi sono rimedi legali contro il cyberbullismo commesso per cause non rientranti in quelle sovra citate, ma non si esclude che le vittime possano cercare altri rimedi giuridici. Ciò accade anche in Oregon (cfr. *Or. Rev. Stat. Ann. §339,364*, 2009) dove «le vittime possono chiedere un risarcimento ai sensi di altre leggi […]» per cui lo statuto «non può essere interpretato per evitare che una vittima di molestie, intimidazioni o bullismo o una vittima di cyberbullismo chieda un risarcimento garantito in qualsiasi altra legge disponibile, sia civile che penale».

Non vi è, quindi, in molti casi, una esplicita previsione di reato, ma per tutelare le vittime dal fenomeno, esso si può sovrapporre di volta in volta a crimini informatici piuttosto che relativi alla diffamazione o all'*hate speech.*

1.1.1 – Disposizioni federali e corretto bilanciamento tra tutela dei minori e free speech

Terminata la panoramica relativa ai singoli stati, è bene passare al livello federale, dove un disegno di legge, il *Megan Meier Cyberbullying Prevention Act,* fu presentato al Congresso dopo il tragico suicidio di una ragazza del Missouri di soli 13 anni, Megan Meier. La ragazza aveva stretto amicizia e veniva corteggiata on-line su MySpace da un ragazzo di nome Josh Evans, che poi la respinse in modo crudele, offendendola ripetutamente e spingendo la giovane a decidere di impiccarsi nella sua camera da letto nell'ottobre del 2006.

Quello di Josh Evans si è poi rivelato essere un profilo creato da una vicina di casa e madre di un amico di Megan. La donna, insieme ad alcuni complici del quartiere, aveva creato l'account di MySpace con il solo scopo di ingannare la vittima. Dal momento che non vi era nessuna legge contro il cyberbullismo, il crimine fu giudicato in base al *Computer Fraud and Abuse Act*, una legge contro la pirateria informatica, applicabile alla fattispecie poiché la donna aveva usato un computer protetto per ottenere informazioni che umiliassero la vittima.

[20] *Section 422.55-422.57* of Penal Code of California in www.leginfo.ca.gov.

In seguito alla vicenda, nell'aprile del 2009, la rappresentante dello stato della California, Linda Sanchez, ha proposto il "*Megan Meier Cyberbullying Prevention Act*" (*HR 1966* proposto nell'aprile 2009) con lo scopo di modificare il titolo 18 dello *United States Code* introducendovi il fenomeno del cyberbullismo. Esso, infatti, ha l'intento di dar vita alla sezione 881, rivolta a «chi trasmette in commercio interstatale o estero qualsiasi comunicazione, con l'intento di costringere, intimidire, molestare o causare sostanziale stress emotivo ad una persona, usando mezzi elettronici per supportare il comportamento in modo grave, ripetuto ed ostile» prevedendo che il colpevole «sarà multato […], incarcerato non più di due anni, o entrambe le cose». Le disposizioni sarebbero da applicare a quanto avviene all'interno e all'esterno della scuola, non solo se indirizzato ai ragazzi o da essi commesso, ma anche nel caso in cui siano coinvolti gli adulti, tanto come vittime (ad esempio di *cyberbaiting*) quanto come colpevoli.

Tuttavia, il *Cyberbullying Prevention Act* non è ancora stato approvato, nonostante sia co-sponsorizzato da quattordici democratici e un repubblicano ed esso sembri coprire molti casi di cyberbullismo che risultano poco o per nulla tutelati dalle altre disposizioni federali. Infatti, durante la seduta di ascolto dell'*House Judiciary Subcommitee on Crime, Terrorism and Homeland Security*, tenutasi nell'ottobre 2009, entrambi i partiti politici hanno criticato il disegno di legge, ritenendolo una potenziale restrizione al Primo Emendamento.

Il presidente del Comitato, Bobby Scott - del Partito Democratico e membro della Camera dei Rappresentati per lo stato della Virginia - ha espresso la sua preoccupazione per la costituzionalità di questa proposta, sottolineando il potenziale effetto che potrebbe avere sul discorso legittimo e provocatorio. Uno dei repubblicani, Louie Gohmert - membro della Camera dei Rappresentati per lo stato del Texas - ha evidenziato le conseguenze non intenzionali che questa legge, destinata a proteggere gli adolescenti da bullismo online, potrebbe avere, inducendo al perseguimento degli oppositori politici che, ad esempio, avevano postato su un blog frasi offensive, che lo riguardavano. Infatti, nello statuto non vi sarebbero, secondo Gohmert, le condizioni per impedire un tale risultato e, pertanto, esso sarebbe incostituzionale poiché andrebbe a limitare, tra le altre cose, la libera manifestazione del pensiero politico.

Lo *Student Internet Safety Act*[21] (*HR 780*) invece, pur proposto nello stesso anno, ha un approccio più mite alla prevenzione del bullismo elettronico e si avvale soprattutto degli strumenti educativi. Esso, infatti, richiederebbe ai beneficiari dei finanziamenti federali (previsti con l'*Elementary and Secondary Education Act* del 1965) di promuovere la sicurezza nell'uso di internet da parte degli studenti. Tale programma dovrebbe includere la prevenzione del cyberbullismo e un maggiore coinvolgimento dei genitori nel rafforzare l'uso sicuro di internet da parte dei loro figli.

Il disegno di legge, che è passato alla Camera dei Rappresentanti con un forte sostegno bipartisan, attualmente non è ancora stato approvato dal *Committee on Education and Labor*, nonostante gli sia stato sottoposto.

Così, in assenza di leggi che puniscono il crimine di cyberbullismo, le vittime possono solo ricorrere al diritto civile o alle leggi penali che regolano i reati connessi (ad esempio molestie o *cyberstalking*). Dal momento, però, che questi rimedi giuridici non sono progettati per affrontare il problema del bullismo elettronico, essi risultano insufficienti sia per scoraggiare i bulli (prevenzione) sia per proteggere e risarcire le loro vittime (repressione) poiché non costituiscono un mezzo solido di contrasto.

Per quanto riguarda il diritto civile tradizionale statunitense, esso consente di agire per vie legali assimilando il cyberbullismo alla diffamazione.

In realtà, l'unico paese democratico che sta cercando di introdurre una legge sulla cyber-diffamazione è la Corea del Sud. Infatti, la *Korea Communication Commission* ha preso in considerazione una revisione della attuale legge sulle telecomunicazioni in modo da permettere alla polizia di reprimere commenti ingiuriosi senza che la vittima debba segnalarli.

Tornando al diritto costituzionale degli Stati Uniti, i cd. *false statements of fact* costituiscono un'eccezione alla tutela della libertà di parola enunciata nel Primo Emendamento e possono essere previsti anche per il web.

Questa prospettiva si è evoluta nel tempo grazie ad una serie di casi riguardanti la calunnia e la diffamazione che la Corte Suprema si è trovata ad affrontare. In realtà, la norma giuridica in sé è piuttosto complessa, poiché le sue conseguenze dipendono

[21] www.gop.gov.

da chi ha diffamato e da chi è il destinatario dell'offesa. Quindi, si avranno tutele differenti (e maggiori) se il fine è quello di colpire un personaggio pubblico o il governo piuttosto che un soggetto privato offeso riguardo la sua vita privata. Stando così le cose, i punti di partenza fondamentali per costruire un caso di diffamazione sono la maniera e il contesto in cui essa è stata perpetrata.

Il cyberbullismo rientrerebbe nella definizione di "diffamatorio" in quanto danneggia la reputazione di qualcuno tramite una falsa dichiarazione di fronte a terzi. Tuttavia, per avere ragione su una denuncia per diffamazione, la vittima deve dimostrare in primo luogo che l'affermazione è falsa e, in secondo luogo, che ha causato danni materiali alla sua reputazione (cfr. sent. New York Times Co. v Sullivan., *Supreme Court*, 1964).

E' chiaro che, molte giovani vittime di cyberbullismo riscontrano una difficoltà nel provare questo secondo aspetto in quanto, con tutta probabilità, non avranno ancora avuto il tempo di sviluppare una reputazione professionale o personale nella community. Inoltre, poiché una dichiarazione deve essere falsa per essere diffamatoria, un parere non può costituirne la base, perché non può essere provato che sia vero o falso. Ad esempio, se un ragazzo afferma ripetutamente su un social network che un compagno di scuola è "brutto e stupido", si è chiaramente di fronte ad un parere, perché non ci sono strumenti per attestarne la veridicità. Stando così le cose, i giudici non possono fare altro che esaminare la modalità e il contesto della dichiarazione caso per caso, dando esiti diversi di giudizio.

Il professor Eugene Volokh, del dipartimento di legge della UCLA, caratterizza la suddetta analisi di contesto in cinque aree diverse. In primo luogo, le *false statements of fact* possono portare a responsabilità civile se sono «pronunciate con uno stato mentale di sufficiente colpevolezza»[22], cioè se vi è la coscienza e la volontà di fare del male e ferire la vittima (cd. *malice*). La seconda categoria è un sottoinsieme della prima ed è costituita dalle "bugie intenzionali" (false dichiarazioni fatte consapevolmente), il che include la calunnia e la diffamazione (cd. *actual malice*). Questi tipi di dichiarazioni sono punibili perché contengono malizia e si distinguono

[22] E. Volokh, *First Amendment and Related Statutes: Problems, Cases and Policy Arguments*, Foundation Press, 2008.

dalla terza categoria, in cui la falsità delle dichiarazioni risiede nella negligenza di chi le ha pronunciate o scritte.

In ultimo, vi sono le affermazioni che hanno solo una falsa connotazione fattuale dimostrabile. L'esempio utilizzato da Volokh è applicabile perfettamente al cyberbullismo poiché questa quarta categoria si rivolge alle affermazioni tipo: "Joe merita di morire", che spesso viene ritrovata, con nomi diversi e sottoforma di commento o sondaggio, nei social network (ad es.: Ask.fm o Facebook)[23].

Come già detto, nei casi di diffamazione, un personaggio pubblico o il governo americano ricevono maggiore tutela poiché la disciplina nasce per regolare il fenomeno relativamente alla stampa (cfr. sentenza della Corte Suprema nel caso Gertz v. Robert Welch, Inc. del 1974). Invece, il settore più ambiguo resta quello delle false dichiarazioni che coinvolgono i comuni cittadini e che riguardano la loro vita privata, complicando ulteriormente le cose nel caso di bullismo elettronico che coinvolge i minori. Ciò pone la delicata questione di trovare un equilibrio tra la responsabilità oggettiva del diffamatore e la sua libertà di parola garantita dal Primo Emendamento in un contesto con caratteristiche particolarissime, come è la rete. Infatti, oltre agli elevati costi associati alla risoluzione della controversia che rendono difficoltoso per molte giovani vittime far valere i propri diritti, in uno spazio come internet bisogna considerare le peculiarità del mezzo. I contenuti non possono essere rimossi su richiesta, sono sempre disponibili, duplicabili, condivisibili e persino aggiornabili continuamente, cosa che non avviene nel caso di "diffamazione cartacea" o di bullismo nei corridoi della scuola. Infatti, piattaforme social come Facebook, Twitter, Ask.fm e YouTube promuovono l'interattività e la comunicazione, ma negli ultimi anni sono diventati luoghi in cui il bullismo viene esteso oltre i confini della scuola, rendendo la persecuzione perenne.

Comunque, oltre al *false statements of fact,* alla pornografia minorile, all'oscenità e al cd. "*speech owned by others*" (che fa riferimento ai diritti di proprietà intellettuale), vi sono altri due limiti al *free speech*. Innanzi tutto, vi è il cd. *offensive speech*, che si articola anche e soprattutto nelle *fighting words*, cioè espressioni che infliggono intenzionalmente, consapevolmente o incautamente grave stress

[23] Ibid.

emotivo[24]. Tale norma, però, non è mai stata esplicitamente stabilita e sarebbe limitata a soggetti privati, contrariamente al *false statements of fact*. Infatti, la Corte Suprema ha affermato che la satira, anche potenzialmente offensiva, se rivolta ad una figura pubblica è completamente protetta dal Primo Emendamento[25].

In secondo luogo, anche le minacce di violenza dirette ad una persona o ad un gruppo di persone e che hanno l'intento di porre i soggetti a rischio di lesioni o di morte sono generalmente perseguibili - fatta eccezione per casi costituzionalmente protetti, come l'ostracismo sociale e il boicottaggio politicamente motivati. Insomma, potenzialmente il cyberbullismo potrebbe essere tutelato da diverse disposizioni e da diversi limiti posti al *free speech*, ma è ancora del tutto assente una disciplina unitaria che risolva i diversi casi in maniera univoca. Per questo, a livello federale, i maggiori esperti in tema di diritto pongono tre statuti alla base della protezione contro il bullismo elettronico: il Titolo IX degli *Education Amendments* del 1972, il titolo VI del *Civil Rights Act* del 1964 e l'*Americans with Disabilities Act* (ADA). Il Titolo IX viene utilizzato principalmente dalle famiglie quando la scuola ignora volutamente o non indaga adeguatamente sugli episodi di cyberbullismo. L'*Americans with Disabilities Act* è utilizzato come difesa da quegli studenti che hanno una disabilità, sono stati vittima di bullismo elettronico e possono dimostrare che la molestia è protetta da un atto ufficiale delle isituzioni. Infine, il *Civil Rights Act* viene applicato ai casi cyberbullismo quando l'accusa è in grado di dimostrare il fatto che gli attacchi siano basati su razza, religione o sesso, unitamente al fatto che il distretto scolastico era a conoscenza delle molestie e non ha compiuto azioni significative per combatterle.

Prima di agire per vie legali, il genitore può coinvolgere la scuola attraverso la raccolta di un portafoglio di *screenshot* (di post o commenti), dei messaggi, dei file scaricati e ricevuti ecc… Questo passaggio è fondamentale per la costruzione del caso poiché queste informazioni possono essere trasmesse ai dirigenti scolastici e al consiglio scolastico in modo che essi possano risolvere la questione.

Comunque, se a livello scolastico non vi è sufficiente tutela e non viene adottata alcuna risoluzione per tutelare la vittima, si può adire al tribunale grazie ai tre statuti

[24] Ibid.

[25] Cfr. sent. Hustler v. Falwell, 1988.

federali di cui sopra. I diversi tipi di cause civili che i genitori possono intentare sono relative all'invasione della privacy, alla causa del danno fisico o mentale, alla diffamazione o alle minacce che non sono protette dal Primo Emendamento. In ciascuno di questi casi, la famiglia può presentare un'ingiunzione e l'eventuale ordine del tribunale può stabilire che il bullo cessi le molestie. A questo tipo di azione può far seguito un risarcimento che la famiglia del colpevole deve corrispondere a quella della vittima. In Ohio, per esempio, i genitori possono essere citati in giudizio in sede civile, con una multa fino a $15.000.

Passando a ciò che avviene a livello penale, come già sottolineato, negli stati senza leggi che puniscano il cyberbullismo, il pubblico ministero può tentare di perseguire i bulli attraverso norme relative ad alcuni reati connessi, come ad esempio le molestie e lo *stalking*. Tuttavia, questo approccio è possibile solo laddove il caso soddisfi pienamente i requisiti di legge destinati a combattere questi due fenomeni. Infatti, essi hanno caratteristiche diverse rispetto a ciò che avviene online e che comporta indubbi problemi probatori (commenti cancellati, falsi profili, furto della password ecc…).

Diversi stati hanno scelto di affrontare il problema adottando leggi relative al *cyberstalking*, sicuramente più strettamente legate al bullismo delle leggi sullo "*stalking offline*", ma che ancora offrono scarso successo, in quanto tale fenomeno richiede la prova di una "minaccia credibile" di violenza, che potrebbe non essere affatto presente in molti casi di cyberbullismo, spesso basato su prepotenze psicologiche.

Inoltre, diverse leggi federali sono collegate perifericamente al cyberbullismo, ma ancora nessuna di esse risolve adeguatamente il problema a livello penale. Ad esempio, l'*Interstate Communications Act* criminalizza la trasmissione di «qualsiasi minaccia di nuocere ad una persona» attraverso l'*interstate commerce*. Tuttavia, questa previsione è inapplicabile a gran parte dei casi di cyberbullismo, visto che spesso non può essere interpretato come una minaccia di danni fisici, nonostante i suoi contenuti psicologicamente dannosi. Allo stesso modo, il *Telephone Harassment Act* che criminalizza l'uso di comunicazioni anonime nel *District of Columbia*, a livello interstatale o verso l'estero «con l'intento di infastidire, abusare, minacciare o molestare» non riesce a ricomprendere il fenomeno in questione. Anche se questa

legge è stata modificata nel 2006 per includere internet tra le forme di comunicazione, uno dei requisiti fondamentali resta la non identificabilità dell'autore delle comunicazioni, cosa che solo in alcuni casi caratterizza il bullismo elettronico, ma non in tutti (ad esempio materiale video o profili reali da cui vengono perpetrate le offese).

Il *Computer Fraud and Abuse Act*, che criminalizza l'uso non autorizzato del computer, era originariamente destinato a contrastare la pirateria informatica e si potrebbe applicare ad un segmento ristretto di forme di cyberbullismo (ad esempio quando vi è furto di identità o di password), ma non può far ricadere sotto di sé l'intera gamma di reati ad esso connessi.

Sul sito dell'FBI[26], nella sezione "*Law Enforcement Bulletin*" vi è un articolo datato 4 giugno 2013 intitolato "*Cyberbullying and Sexting: Law Enforcement Perceptions*". Si tratta della ricerca condotta dai fondatori del *Cyberbullying Research Center*, J. W. Patchin e S. Hinduja - con la collaborazione di J. A. Schafer - attraverso indagini su due campioni distinti. Il primo, ha visto coinvolti gli "*school resource officers*" (SROs) che hanno compilato un sondaggio online sul cyberbullismo e sul *sexting*. Il secondo campione, molto più interessante per le prospettive normative, comprende tre classi di dirigenti delle forze dell'ordine che frequentano l'*FBI National Academy* (FBINA) a Quantico, in Virginia. I ricercatori hanno raccolto i dati provenienti da indagini somministrate a 643 funzionari da tre classi FBINA tra il 2010 e il 2011.

L'80% degli intervistati dell'FBINA ha riconosciuto che cyberbullismo è una questione importante, che richiede il coinvolgimento della polizia, mentre il 10% degli *school resource officers* ha indicato di aver avuto esperienza in indagini su casi cyberbullismo, con una media di due casi durante l'anno scolastico precedente.

Avvalendosi dell'utilizzo di scenari ipotetici (vedi *Table 1*) , tutti gli intervistati hanno valutato la misura in cui l'applicazione di una legge che regola il fenomeno avrebbe potuto svolgere un ruolo significativo, utilizzando una scala da 0 (nessun ruolo significativo) a 10 (ruolo estremamente rilevante). Le situazioni di minaccia di

[26] FBI, *Cyberbullying and Sexting: Law Enforcement Perceptions*, in www.fbi.gov.

danno fisico, di forte umiliazione di fronte ad un pubblico vasto e di cyberbullismo sono state quelle che hanno ottenuto il maggior numero di punti[27]:

Law Enforcement Perceptions Regarding Responsibility in Dealing with Cyberbullying

With 0 being no law enforcement role or responsibility and 10 being a very important or significant role or responsibility, to what degree should law enforcement be involved?	School Resource Officers N=336 Mean	FBI National Academy N=643 Mean
A male student receives an e-mail from an unknown person threatening to kill him at school tomorrow.	9.1	8.6
A female student, Jenny, covertly takes a picture of another female student, Margaret, in her underwear in the girl's locker room and posts it on a website without permission that allows the rest of the student body to rate or judge Margaret's physical appearance.	8.9	7.8
A parent calls to report that her son has a naked image of a female student from his school on his cell phone.	8.3	6.3
A parent calls the police department to report that her son is being cyberbullied by another youth in their neighborhood.	7.8	6.5
A student creates a Facebook Fan Page called "Give Mary a Wedgie Day." Mary is a student at a school in your jurisdiction.	5.8	3.8
A male student reveals another classmate's sexual orientation (without permission) via Twitter to the rest of the student body.	5.7	4.0
A female student receives a text message from another classmate calling her a slut.	4.2	3.4
A student creates a webpage making fun of the school principal.	4.1	2.6
A teacher confiscates a cell phone from a student in class and wants to determine if it contains any information that violates school policy.	2.4	1.4

N=Number of respondents

Table 1

Stando a quanto affermato dagli *school resource officers*, coloro che lavorano all'interno delle scuole sono necessariamente chiamati ad agire al verificarsi di tali situazioni durante il loro mandato, anche se il fenomeno non è considerato specificamente un crimine.

Proprio per la mancanza di previsioni legislative a livello federale, oltre l'ottanta per cento dei partecipanti allo studio ha indicato di aver bisogno di ulteriori informazioni sulla prevenzione e sulle soluzioni da adottare in risposta al cyberbullismo. Inoltre, il 25% degli *school resource officers* e oltre il 40% degli ufficiali dell'FBINA intervistati non hanno saputo indicare se il loro stato possegga o meno una legge

[27] Research by J. W. Patchin, S. Hinduja, A. Schafer, *Cyberbullying and Sexting: Law Enforcement Perceptions*, 2010-2011.

specifica per il fenomeno[28] proprio perché anche a livello statale non vi è, se non in pochissimi casi (vedi *supra* pagg. 14-18), una disciplina giuridica.
In sostanza, come dimostra quanto sin qui affermato, le leggi volte a tutelare gli individui dalle molestie, dallo *stalking* e dalle patologie della comunicazione in genere lasciano comunque un *gap* a livello statale e, soprattutto, federale che deve essere necessariamente colmato da una normativa specifica contro il cyberbullismo.

1.2 – Iniziative paneuropee e obiettivi per il contrasto del cyberbullismo

L'obiettivo del capitolo è quello di procedere ad una descrizione dei profili normativi statunitensi ed europei e sviluppare, progressivamente, una comparazione tra i due contesti. Il primo, come si è visto in precedenza, manca di una disciplina unitaria a livello federale e dispone di normative specifiche solo in alcuni stati, mentre altri restano del tutto estranei alla regolazione del fenomeno. Ora bisogna capire in che modo l'Europa, da intendersi tanto come Unione Europea quanto come Consiglio d'Europa, fa fronte al problema del cyberbullismo a livello sovrannazionale e in che misura influenza le *policies* nazionali, cercando anche di comprendere quanti e quali siano gli accordi stipulati con gli altri organi internazionali.
L'Unione Europea, da sempre attiva nel cercare di promuovere un corretto uso delle nuove tecnologie, ha iniziato sin dal 2002 ad adottare provvedimenti che stimolassero gli stati membri a tenere il passo con le ICT. La cd. "seconda generazione" di direttive europee, infatti, ha portato numerosi cambiamenti in un mercato che, grazie alla prima stagione di direttive (adottate tra il 1988 e il 1996) si era finalmente liberalizzato. A questo proposito, la direttiva "quadro" (2002/21/CE) contiene una disciplina generale per le telecomunicazioni e tiene conto della convergenza tecnologica. La direttiva "autorizzazioni" (2002/20/CE), invece, semplifica l'accesso al mercato, mentre quella sul "servizio universale" (2002/22/CE) garantisce standard minimi di servizi cui gli utenti devono poter accedere. Importantissima, poi, la quarta direttiva, quella relativa all' "accesso" (2002/19/CE), che ribadisce l'apertura della rete, la quale deve poter essere utilizzata

[28] Ibid.

da chiunque, con qualunque mezzo e per esprimere qualsiasi manifestazione del pensiero.

Dello stesso anno è anche la direttiva in materia di privacy (58/2002/CE), un argomento che l'Unione ha molto a cuore, trattandosi di un diritto che riguarda sia la comunicazione telematica che i dati personali, due elementi fortemente in gioco quando si parla di internet.

Più di recente, il legislatore comunitario è intervenuto per modificare questo tipo di provvedimenti, dando vita a due direttive che hanno precisato e ridefinito il contesto normativo delle ICT. In primo luogo, la direttiva 2009/140/CE che modifica le direttive 19, 20 e 21 del 2002 e, congiuntamente, la direttiva 2009/136/CE, la quale invece rielabora le direttive 22 e 58 del 2002. L'obiettivo di questi due provvedimenti è quello di ribadire la cd. "neutralità tecnologica", un principio fondamentale che riguarda in primis la non discriminazione nella disponibilità dei servizi sulle diverse piattaforme e in secondo luogo si collega al concetto di "neutralità della rete". Con questa espressione si intende l'assenza di limitazioni/discriminazioni nell'accesso alle reti e nel traffico dei dati, ma soprattutto l'impossibilità di applicare limitazioni/discriminazioni ai dati immessi dagli utenti nel web, che nasce come uno strumento libero e neutrale rispetto ai contenuti che vi vengono inseriti.

Ovviamente, si tratta di un argomento delicato, poiché chiama in causa la libera manifestazione del pensiero che è alla base della Carta dei Diritti Fondamentali dell'UE (allegata al Trattato di Lisbona del 2009), in cui, nell'articolo 11 viene sancita la libertà di manifestazione del pensiero e d'informazione e stabilito che: «Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera». Allo stesso modo e con espressioni molto simili, il Consiglio d'Europa nella Convenzione Europea dei Diritti dell'Uomo pone all'articolo 10 la libertà di espressione, precisando, però, un punto importante: «L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, […] alla difesa dell'ordine e alla

prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui […]».

Quindi, a differenza dell'Unione Europea, il Consiglio d'Europa si sofferma anche sui rischi connessi alla libera manifestazione del pensiero, il che è essenziale in un contesto come quello di internet, in cui i contenuti sono disponibili sempre ed ovunque, con la possibilità per chiunque di accedervi. Questo aspetto, ovviamente, complica le cose nel momento in cui bisogna decidere quali diritti privilegiare, se quelli della persona umana (dignità, onore, reputazione, uguaglianza ecc…) oppure mantenere un ambiente aperto e privo di limitazioni.

Negli Stati Uniti, come si è visto in precedenza, la priorità viene data al *free speech*, che, limitato solo in alcuni casi (pornografia minorile, *fighting words*, oscenità ecc…), mantiene la sua sacralità fino al punto di considerare incostituzionali quelle leggi che, a tutela delle vittime minorenni del cyberbullismo, potrebbero andare ad inficiare sulle previsioni del Primo Emendamento.

Dal punto di vista europeo, invece, a quanto risulta dalle disposizioni sovra citate, sembra si opti per una maggior protezione dell'individuo come persona, facendola prevalere sulla possibilità di esercitare i diritti di libera manifestazione del pensiero.

Per esempio, tornando alla Carta dei Diritti Fondamentali, l'art. 24, che tutela i "Diritti del bambino", stabilisce che: «i bambini hanno diritto alla protezione e alle cure necessarie per il loro benessere».

Si attiva, quindi, un doppio profilo: da una parte la tutela dell'infanzia e dell'adolescenza, dall'altra, grazie alle disposizioni di cui sopra, la necessità di garantire la libera espressione, che però può includere la libertà di comunicare e di ricevere contenuti offensivi e violenti non adatti per queste particolari fasce di età. Nel caso del cyberbullismo, inoltre, queste manifestazioni del pensiero possono ledere la dignità umana oltre che risultare diffamanti o verbalmente violente e, per questo, richiedono il dovere di rispettare e proteggere coloro che sono più vulnerabili.

Quindi, tornando alla neutralità della rete intesa anche come libertà di espressione, bisogna evidentemente adottare una regolamentazione che rispetti l'apertura del web in modo ragionevole, ma che sia anche in grado di far fronte ai delicati problemi che esso pone quando si tratta di tutelare i minori.

A tal proposito, il 20 novembre del 2012, durante una seduta plenaria del Parlamento europeo, è stata adottata una risoluzione non legislativa dal titolo "*Protecting children in the digital world*". La relatrice italiana, Silvia Costa, ha sottolineato come i bambini sulla rete corrano il rischio di violenza, frode e offese alla propria dignità o altrui (è questo il caso del cyberbullismo) senza che i loro genitori se ne accorgano. Per questo, gli Stati membri dell'UE dovrebbero intensificare i loro sforzi, attraverso la legge, la cooperazione o la condivisione di buone pratiche, per combattere i contenuti illeciti o dannosi e garantire che le risorse online possano essere utilizzate con meno rischi.

Il testo della risoluzione propone un'educazione ai nuovi media digitali non solo per i bambini, ma anche per i genitori e gli insegnanti, da includere nei programmi educativi, affiancando ad essa la lotta contro i contenuti illegali e nocivi da parte dei soggetti istituzionali e dei fornitori di servizi internet. Questi, infatti, dovrebbero intensificare il coordinamento a livello europeo, in modo da facilitare la segnalazione di illeciti e da poter collaborare con le forze di giustizia, compresa la Polizia postale. Inoltre, si sottolinea la necessità di aumentare la cooperazione con i paesi terzi, in modo che i contenuti nocivi ospitati sul loro territorio possano essere rimossi rapidamente[29].

Proprio in occasione di questa seduta, la relatrice ha affermato: «Abbiamo cercato di soppesare i diritti fondamentali dei minori nel mondo digitale - i diritti di accesso, di istruzione e di protezione - e di proteggere i loro diritti come "cittadini digitali", attraverso una nuova forma di *governance* e in modo da sviluppare i loro interessi in quanto persone e cittadini europei»[30].

Questo tipo di interventi, pur fondamentali nell'adozione di strategie di prevenzione e repressione del cyberbullismo, in realtà però non sono specificamente indirizzati ad esso.

Al contrario, un enorme passo in avanti è stato fatto grazie alla Commissione Europea che ha scandito le sue azioni in diverse tappe.

[29] European Parliament resolution of 20 November 2012, *Protecting children in the digital world*, Procedure 2012/2068(INI).

[30] *Video recording of debate*, in www.europarl.europa.eu.

Innanzi tutto, il "*Daphne III Funding Programme*" adottato nel 2007 con una decisione del Parlamento europeo e del Consiglio che lo hanno istituito come parte del programma generale "*Fundamental Rights and Justice*"[31]. Questo progetto, nato nel 2000 e riproposto nel 2004 per una seconda edizione, ha tra i suoi obiettivi quello di contribuire alla protezione dei bambini e dei giovani contro tutte le forme di violenza attraverso l'adozione di misure preventive e fornendo sostegno alle vittime.
Successivamente, durante il *Safer Internet Day*[32] del 2009 (10 febbraio), la Commissione ha iniziato la campagna contro il cyberbullismo con la partecipazione di tutti gli stati membri e anche di Islanda e Norvegia.
Secondo quanto scritto nel comunicato stampa[33] rilasciato in occasione dell'evento, il fenomeno si caratterizza per ripetute molestie verbali o psicologiche, effettuata da un individuo o un gruppo, contro terzi. Esso può assumere molte forme tra cui la derisione, gli insulti, le minacce, i pettegolezzi, i commenti sgradevoli o le calunnie. Oltre ai social network e ai forum, i servizi interattivi on-line (e-mail, chat, messaggistica istantanea) e i telefoni cellulari hanno dato ai cyberbulli nuove opportunità per abusare delle loro vittime. Per di più, in aggiunta alla gravità intrinseca del fenomeno, i social network oltrepassano le frontiere statali, rendendo più difficile l'applicazione di misure nazionali per affrontare problema, per questo la Commissione ritiene necessaria un'azione paneuropea.
Così, per farvi fronte in modo efficace, nel comunicato stampa si parla dell'importanza di condividere le buone strategie che si stanno sviluppando in diversi paesi europei e di realizzare rimedi comuni.
In questo senso, proprio nell'ambito del programma *Daphne III* e a seguito di quanto dichiarato conferenza stampa del febbraio 2009, dal 1 febbraio 2013 ha preso vita il progetto *Delete cyberbullying*[34], attivo fino a giugno 2014. All'interno del sito, nella

[31] Decision No. 779/2007/EC of the European Parliament and of the Council of 20 June 2007 «establishing for the period 2007-2013 a specific programme to prevent and combat violence against children, young people and women and to protect victims and groups at risk (Daphne III programme) as part of the General Programme Fundamental Rights and Justice». (Document 32007D0779 in eur-lex.europa.eu).

[32] Parte del Safer Internet Programme (IP/08/1899) della Commissione Europea.

[33] Comunicato stampa della Commissione Europea del 10/02/2009, *Commission Européenne - MEMO/09/58*, in europa.eu.

[34] Vedi sito deletecyberbullying.eu.

sezione "*About the project*", si legge che il cyberbullismo consiste nell'uso di internet e delle tecnologie correlate per danneggiare altre persone, in modo intenzionale, ripetuto e ostile[35].

Poco dopo vengono posti gli obiettivi del progetto che, attraverso la collaborazione dei partner internazionali, vuole contribuire allo sviluppo di un approccio comune alla prevenzione dei rischi, alle informazioni e alle linee guida per insegnanti, genitori, bambini e altre parti interessate[36].

Inoltre, sempre nell'ambito del progetto, viene affermata la necessità di riconoscere il cyberbullismo come un pericolo reale e sostanziale, in grado di provocare danni immediati e significativi.

In secondo luogo, la Commissione auspica uno scambio di buone pratiche nelle scuole e nelle famiglie per l'individuazione, il controllo e la prevenzione del bullismo online.

Non a caso, il coordinatore del progetto è la *Confederation of Family Organisations in the European Union* (COFACE)[37] che si occupa di mettere in relazione l'attività di otto partner di diversi paesi europei[38] che condividono lo stesso interesse, cioè la sensibilizzazione e lo sviluppo di strumenti sia per prevenire le molestie, che per aiutare le vittime.

In terzo luogo, il progetto *#DeleteCyberbullying* ha lo scopo di dar vita a raccomandazioni specifiche per le *policies* da adottare a livello sovrannazionale e nei singoli Stati membri. Per questo, la European *Conference on Cyberbullying*, organizzata a Madrid da COFACE il 28 maggio del 2013, ha visto la partecipazione di oltre 80 esperti del settore, provenienti da tutta Europa.

Nel corso dell'evento è stata sottolineata la necessità di riunire una grande varietà di *stakeholders* (famiglie, giovani, ONG, scuole, forze dell'ordine e industria) poiché il

[35] «Cyberbullying is the use of the Internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner», in deletecyberbullying.eu.

[36] «The project through the cooperation of the international partners contribute to developing a common approach to risk-prevention, information and guidelines to families, parents, children and other relevant stakeholders», in deletecyberbullying.eu.

[37] Vedi sito www.coface-eu.org.

[38] ASGECO-Confederación e Isadora Duncan (Spagna), BeatBullying (Regno Unito), CWSP-Center for Women's Studies and Policies (Bulgaria), Gezinsbond (Belgio), KMOP (Grecia), Väestöliitto (Finlandia), Kék Vonal (Ungheria).

bullismo elettronico non è dovuto solo alla tecnologia, ma anche all'educazione e ai comportamenti di attori molto diversi che necessitano di essere regolamentati o indirizzati[39].

In ultimo, vi è l'utile sviluppo di materiale online che incoraggi la partecipazione dei bambini e dei giovani, in modo che essi siano la parte attiva e non solo la ragione del cambiamento[40].

Considerato tutto ciò, i partner, al termine del progetto, esamineranno le ricerche, gli studi e i risultati delle indagini per stabilire il quadro della situazione relativa al cyberbullismo in Europa. Una volta stabiliti i rischi, le forme, i sintomi e l'impatto del fenomeno, verranno preparate raccomandazioni politiche relative a programmi scolastici, norme in materia di tutela dei minori, ISPs, intervento delle forze dell'ordine ecc… sia a livello nazionale che europeo, in modo da fornire delle soluzioni solide al problema.

Intanto, nel febbraio 2013, 385 membri del Parlamento Europeo avevano già firmato una dichiarazione scritta[41] che chiedeva la creazione di una giornata contro il bullismo e le violenze scolastiche, con l'obiettivo di contribuire alla sensibilizzazione e proteggere i bambini dalle prepotenze fisiche e psicologiche, incluso in cyberbullismo.

Più di recente, invece, durante l'ottava edizione dello *European Forum on the Rights of the Child*[42] organizzato dalla Commissione Europea, sono state affrontate le tematiche relative alla necessità di integrare le *policies* riguardanti la protezione dei minori per fornire delle linee guida all'Unione Europea. Infatti, nella seconda giornata, una delle quattro sessioni di lavoro ha riguardato proprio il cyberbullismo, visto che la *European Union Agenda for the Rights of the Child* annovera tra i suoi obiettivi quello di concentrarsi sulle azioni per proteggere bambini dalla violenza sia

[39] Press release, *Cyberbullying is not only about technology but about behavior*, European Conference on Cyberbullying, Madrid, 28 maggio 2013, in coface-eu.org.

[40] Comunicato stampa della Commissione Europea del 10/02/2009, *Commission Européenne - MEMO/09/58*, in europa.eu.

[41] Written Declaration 0028/2012, *Annex 2 - Written Declaration on establishing a European Day against Bullying and School Violence*, in www.europarl.europa.eu

[42] Bruxelles, 18-19 novembre 2013.

fisica che psicologica, dentro e fuori il contesto scolastico, a prescindere dai mezzi utilizzati per le prepotenze (bullismo/cyberbullismo).

I punti di partenza della sessione sono stati vari: identificare le buone pratiche, gli attori coinvolti nei sistemi di protezione dell'infanzia nonché i meccanismi che favoriscono la loro collaborazione per la prevenzione del fenomeno.

Essa si è svolta facendo riferimento ad un livello ancora superiore, cioè quello dell'Organizzazione delle Nazioni Unite, l'art. 19 della *UN Convention on the Rights of the Child* (UNCRC) prevede che: «Gli Stati membri adottano ogni misura legislativa, amministrativa, sociale ed educativa per tutelare il fanciullo contro ogni forma di violenza, di oltraggio o di brutalità fisiche o mentali […]. Le suddette misure di protezione comporteranno, in caso di necessità, procedure efficaci per la creazione di programmi sociali finalizzati a fornire l'appoggio necessario al fanciullo e a coloro ai quali egli è affidato, nonché per altre forme di prevenzione, e ai fini dell'individuazione, del rapporto, dell'arbitrato, dell'inchiesta, della trattazione e dei seguiti da dare ai casi di maltrattamento del fanciullo di cui sopra; esse dovranno altresì includere, se necessario, procedure di intervento giudiziario»[43].

Inoltre, durante la sessione dello *European Forum*, è stato ricordato che nel *General Comment No. 13,* lo *UN Committee on the Rights of the Child's* aveva inserito tra le "violenze mentali" il bullismo perpetrato anche attraverso le tecnologie dell'informazione e della comunicazione, definendolo, appunto cyberbullismo[44].

Quindi, anche in questo caso, come in quello del progetto *Delete Cyberbullying*, si è posto l'accento sulla necessità di dar vita ad un sistema multidisciplinare e cooperativo, per dar vita ad un quadro giuridico ancora assente nel panorama europeo.

Proteggere i bambini dall'esposizione ai contenuti dannosi del web e consentire loro di gestire i rischi come il cyberbullismo è parte anche della strategia del programma *Better Internet for Kids*, promosso sempre dalla Commissione nell'ambito dell'Agenda Digitale Europea.

---

[43] Convenzione sui Diritti dell'Infanzia, 20 novembre 1989, in www.unicef.it.

[44] «Mental violence: psychological bullying and hazing by adults or other children, including via information and communication technologies (ICTs) such as mobile phones and the Internet (known as "cyberbullying")». CRC/C/CG/13, The *right of the child to freedom from all forms of violence*, 2011.

Questa, infatti, si basa su sette pilastri fondamentali che costituiscono la base di un uso sicuro e responsabile della rete in tutti i paesi membri. Le "*actions*" intraprese nell'ambito dell'Agenda, inoltre, hanno l'obiettivo di proporre misure giuridiche che rafforzino la cooperazione a livello nazionale, comunitario ed extraeuropeo (ad es. la partecipazione della Russia ai *networks* INSAFE e INHOPE) e che permettano ai cittadini di sfruttare pienamente i vantaggi delle tecnologie digitali.

Ai fini dell'argomento trattato, è necessario ricordare che nell'ambito del terzo pilastro (*Trust&Security*), sono state intraprese moltissime azioni, tra cui la n.36, intitolata *Support reporting of illegal content online and awareness campaigns on online safety for children*. Questa ha avuto origine dalle esigenze di arginare il fenomeno della pedopornografia con la condivisione delle *best practices* nazionali e con una cooperazione paneuropea.

Poco dopo, nel maggio 2012, la Commissione ha definito una *European Strategy for a Better Internet for Children*[45], per dare ai bambini le competenze digitali e gli strumenti di cui hanno bisogno per godere del web in modo sicuro. Infatti, tra gli obiettivi principali della strategia vi sono la sensibilizzazione e responsabilizzazione attraverso l'insegnamento di un uso corretto della rete in tutte le scuole dell'UE e la creazione di un ambiente sicuro per i bambini attraverso impostazioni sulla privacy e uso del *parental control*.

Nonostante il cardine principale resti la tutela contro la pedopornografia, la strategia ha il fine di mettere insieme le attività della Commissione europea e degli stati membri con quella degli operatori di telefonia mobile e dei fornitori di servizi di social networking per fornire soluzioni concrete nell'ambito del programma *Safer Internet* e successivamente attraverso programmi come *Connecting Europe Facility*[46] e *Horizon 2020*[47]. Non a caso, nel paragrafo dedicato agli strumenti di report per gli utenti[48], il testo della *European Strategy* indica tra i suoi scopi quello di responsabilizzare i bambini ad affrontare rischi quali il cyberbullismo o il

[45] *Brussels, 2/05/2012, COM(2012) 196 final,* in eur-lex.europa.eu.

[46] Per completare il quadro favorevole agli investimenti per le telecomunicazioni , la Commissione ha proposto la Connecting Europe Facility per fornire finanziamenti di avviamento e assistenza tecnica per le infrastrutture a banda larga e progetti di servizi, 2014-2020, (ec.europa.eu).

[47] *The framework programme for research and innovation*, 2014-2020, in ec.europa.eu.

[48] Par. 2.2.3. *Simple and robust reporting tools for users,* COM(2012) 196 final, in eur-lex.europa.eu.

grooming[49], rendendo disponibili robusti meccanismi sia online che sui dispositivi per la segnalazione dei contenuti e dei contatti potenzialmente nocivi.

Dal momento che si parla di un confronto tra la situazione europea e quella statunitense, è bene ricordare che a livello di cooperazione internazionale è stato adottato nel novembre del 2012 la *EU and US Joint Declaration to Make the Internet Safer for Kids*[50].

Infatti, a seguito dello *EU-US Summit* del 20 novembre 2010, tenutosi a Lisbona con l'obiettivo di affrontare nuove minacce alle reti globali, si è raggiunto un accordo transnazionale tra il vicepresidente della Commissione Europea per l'Agenda Digitale, Neelie Kroes e il segretario statunitense della *Homeland Security*, Janet Napolitano.

Tra gli scopi principali della dichiarazione vi è quello di impegnarsi a contribuire alla cooperazione internazionale nella lotta contro gli abusi online, basata sul lavoro già eseguito dalla *Virtual Global Taskforce* e dall'*Interpol*.

Insomma, per procedere ad una comparazione con gli Stati Uniti, anche all'interno dell'Unione Europea non vi è ancora, dal punto di vista sovrannazionale, un intervento normativo concreto. Sicuramente, come accade oltreoceano, le più tragiche conseguenze di cyberbullismo hanno attirato l'attenzione dei media, delle famiglie, delle scuole e dei providers. Ciò ha comportato una forte esigenza di adottare misure che devono essere prese a ogni livello, sia nazionale che internazionale, ma anche sul fronte scolastico-educativo e su quello della formazione degli insegnanti, assieme alle campagne di sensibilizzazione e di responsabilizzazione dei genitori.

Ciò che appare interessante è il sentire comune che unisce USA ed Europa nella lotta al fenomeno, tanto che, pur non disponendo di specifiche previsioni legislative, si è sentita l'esigenza di procedere ad un'azione congiunta.

[49] «Grooming refers to actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in preparation for sexual activity with the child or exploitation», COM(2012) 196 final, in eur-lex.europa.eu.

[50] Commission Européenne - MEMO/12/881, *Digital Agenda: EU and US sign joint declaration to make the internet safer for kids*, Londra, 20/11/2012, in europa.eu.

Per quanto riguarda il Consiglio d'Europa, nel settembre 2009[51], la sua Assemblea parlamentare ha ricordato la decisione dei capi di stato e di governo (terzo Summit, Varsavia, 2005) di proseguire il lavoro sulla tutela dei bambini nella società dell'informazione, in particolare per quanto riguarda lo sviluppo dell'alfabetizzazione multimediale e la loro protezione contro i contenuti dannosi, anche alla luce di quanto previsto dalla Convenzione di Budapest sul Cybercrimine[52], firmata dagli stati membri ma anche da Stati Uniti, Canada, Giappone e Sud Africa. Quest'ultima, innanzitutto, introduce la cd. "prova elettronica", connotata da fragilità e immaterialità[53] che rende necessaria una maggiore accuratezza e rapidità nella raccolta degli elementi probatori, possibile anche grazie alla collaborazione dei *providers* - da cui il riferimento all'ingiunzione di produrre i dati funzionali all'identificazione degli utenti[54]. In secondo luogo, essa individua i "Reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici"[55], distinguendoli dai "Reati informatici" veri e propri (falsificazione e frode informatica)[56]. In terzo luogo, si occupa di contenuti pedopornografici[57], il che rende, ad oggi, più agevole fronteggiare il *sexting* e la cd. "*revenge porn*" (vedi definizione a pag. 106).

Così, nella raccomandazione n. 1882[58], il Consiglio ha sottolineato la necessità di attuare le misure appropriate per l'uso di internet da parte dei giovani, dal momento che esso può portare anche alla violenza, sia nel mondo virtuale che reale, come nel caso del cyberbullismo e delle molestie[59]. Dunque, mentre la regolamentazione dei

[51] Parliamentary assembly, Recommendation 1882 (2009), *The promotion of Internet and online media services appropriate for minors*, 28 September 2009, in assembly.coe.int.

[52] Consiglio d'Europa, *Convention on Cybercrime*, Budapest, 23 novembre 2001.

[53] Sezione II – Titolo II, *Convention on Cybercrime*, Budapest, 23 novembre 2001.

[54] Sezione II – Titolo III, *Convention on Cybercrime*, Budapest, 23 novembre 2001.

[55] Sezione I – Titolo I, *Convention on Cybercrime*, Budapest, 23 novembre 2001.

[56] Sezione I – Titolo II, *Convention on Cybercrime*, Budapest, 23 novembre 2001.

[57] Sezione I – Titolo III, *Convention on Cybercrime*, Budapest, 23 novembre 2001.

[58] Ibid.

[59] «Certain content on the Internet can have negative effects on children and adolescents. For example, content depicting women and girls as objects, or limiting their depiction to nefarious gender

media tradizionali proibisce o limita i contenuti multimediali nocivi allo sviluppo fisico o morale dei bambini e degli adolescenti, internet pone nuove sfide ai genitori, alle scuole e alle istituzioni. Per questo, il Consiglio d'Europa ritiene che gli stati abbiano la responsabilità di sensibilizzare l'opinione pubblica e di stabilire norme minime che comprendano restrizioni di accesso a contenuti violenti/dannosi, con la collaborazione di scuole, famiglie e fornitori di contenuti o servizi[60].

Successivamente, infatti, nell'aprile 2011, dopo la conferenza di Strasburgo[61], il Comitato dei ministri ha adottato la *Declaration on Internet Governance Principles*[62], per dare corretta applicazione alla Convenzione Europea dei Diritti dell'Uomo da parte di ciascuno stato membro del Consiglio anche nella realtà online. Ciò avviene nella consapevolezza che internet può aumentare significativamente l'esercizio delle libertà fondamentali, in particolare quella di espressione, spesso andando ad inficiare sulla dignità umana. Pertanto, come si legge nel primo dei principi: «Le disposizioni sulla *governance* di internet devono garantire la tutela di tutti i diritti e le libertà fondamentali e affermare la loro universalità, indivisibilità, interdipendenza e interrelazione, in accordo con le leggi internazionali sui diritti umani. […] Tutti gli attori pubblici e privati dovrebbero riconoscere e difendere i diritti umani e le libertà fondamentali nelle loro operazioni e attività, nonché nella progettazione di nuove tecnologie, servizi e applicazioni. Essi devono essere consapevoli degli sviluppi che portano alla valorizzazione dei diritti e delle libertà fondamentali, così come di quelli che comportano minacce e devono partecipare pienamente agli sforzi volti a riconoscere i diritti emergenti»[63].

---

stereotypes, can lead in certain cases to gender-based violence both in the virtual and the real world, including (cyber-)bullying, harassment, rape, and can even lead to committing massacres in schools», Parliamentary assembly, Recommendation 1882 (2009), *The promotion of Internet and online media services appropriate for minors*, 28 September 2009, in assembly.coe.int.

[60] Parliamentary assembly, Recommendation 1882 (2009), *The promotion of Internet and online media services appropriate for minors*, 28 September 2009, in assembly.coe.int.

[61] Council of Europe conference, 18-19 aprile 2011.

[62] Declaration by the Committee of Ministers on *Internet governance principles*, adopted by the Committee of Ministers on 21 September 2011at the 1121st meeting of the Ministers' Deputies, in wcd.coe.int.

[63] Art. 1: Human rights, democracy and rule of law: «Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law. […] All public

Anche il secondo principio è in linea con quanto detto sin ora in merito ad un'azione articolata su più livelli. Infatti, esso parla proprio di una *governance multi-stakeholders* che conduca allo svilippo di *policies* internazionali riguardanti internet[64], vista la natura globale del mezzo[65].

Ecco perché L'Assemblea accoglie con favore il programma dell'Unione Europea *Safer Internet* e le successive iniziative, ma soprattutto, vi si affianca con la recente campagna *No hate speech movement*[66], un progetto gestito dallo *Youth Department of the Council of Europe* tra il 2012 e il 2014.

Esso mira innanzitutto a combattere il razzismo e la discriminazione online, mobilitando i giovani e le organizzazioni giovanili a riconoscere e agire contro tali violazioni dei diritti umani. Come spiega chiaramente il sito, la campagna non è progettata per limitare la libertà di espressione in rete, ma si pone come obiettivo quello di andare contro l'incitamento all'odio sul web, in tutte le sue forme, comprese quelle che più colpiscono i giovani, come il cyberbullismo.

Inoltre, il Protocollo addizionale alla Convenzione di Budapest sul Cybercrimine si riferisce all'incriminazione di atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici, per far sì che la libertà di espressione non oscuri la lotta agli atti di questo tipo.

Ciò assume una rilevanza considerevole se si considera che molti dei cyberbulli si accaniscono sulle loro vittime per motivi connessi alla discriminazione, tant'è che

---

and private actors should recognise and uphold human rights and fundamental freedoms in their operations and activities, as well as in the design of new technologies, services and applications. They should be aware of developments leading to the enhancement of, as well as threats to, fundamental rights and freedoms, and fully participate in efforts aimed at recognising newly emerging rights», Declaration by the Committee of Ministers on *Internet governance principles*, adopted by the Committee of Ministers on 21 September 2011at the 1121st meeting of the Ministers' Deputies, in wcd.coe.int.

[64] Art. 2: Multi-stakeholder governance: «[…] The development of international Internet-related public policies and Internet governance arrangements should enable full and equal participation of all stakeholders from all countries», Declaration by the Committee of Ministers on *Internet governance principles*, adopted by the Committee of Ministers on 21 September 2011at the 1121st meeting of the Ministers' Deputies, in wcd.coe.int.

[65] Art. 5: Global nature of the internet, Declaration by the Committee of Ministers on *Internet governance principles*, adopted by the Committee of Ministers on 21 September 2011at the 1121st meeting of the Ministers' Deputies, in wcd.coe.int.

[66] nohate.ext.coe.int.

proprio il Protocollo auspica l'armonizzazione del diritto penale degli Stati aderenti e l'aumento della cooperazione internazionale.

Quindi, come accade negli Stati Uniti, anche il Consiglio d'Europa considera il fenomeno una parte integrante dell'*hate speech*, che va combattuto in quanto costituisce una violazione dei diritti umani, ma al tempo stesso va bilanciato con una libertà fondamentale quale quella di espressione e manifestazione del pensiero. Infatti, il Consiglio valuta tutti gli aspetti del fenomeno, in modo da agire proporzionalmente alla motivazione, al contenuto, al tono, al contesto, agli obiettivi e alle conseguenze delle azioni dannose.

Ciò che appare interessante è che, come già evidenziato per USA e UE, anche per il Consiglio la dimensione del web richiede importanti elementi offline come corsi di formazione, seminari, conferenze ed eventi, rivolti ai giovani, alle scuole e alle famiglie. Insomma, si tratta di un'azione multilivello, che chiama in causa sia le istituzioni che i cittadini, con l'obiettivo di fornire alle vittime una maggiore protezione legale e un più forte sistema di prevenzione. Infatti, le campagne nazionali sono attuate con il coinvolgimento attivo di rappresentanti governativi e non nel settore della gioventù, in uno spirito di cogestione.

In proposito, lo schema riportato su nohate.ext.coe.int è estremamente esaustivo:

Targetgroups	Personal and interpersonal sphere	Civil society	Broader social context	Legislative aspect	Political and policy domains
Victims	Empowerment	Methods for inclusion of victims	Social and cultural inclusion	Stronger legal protection	Better minority policies
"Haters"	Alternatives for expression opinion	Other ways of involvement	Stronger social pressure	Consequent legal approach	Less political justification
Activists	Counter arguments and practical tools	Stronger networking	More support and recognition	Legal support for prevention and measures	More political recognition and more support
Public	Awareness	Dynamic civil society involvement	Stronger public opinion against hate speech	Clearer agreement among governments	Less political extremism, more democracy

Le linee guida per le *policies* relative al rapporto tra *hate speech* e libertà di espressione verranno redatte nel corso del 2014, quindi, attualmente, anche il Consiglio d'Europa non è provvisto di norme relative al cyberbullismo che tutelino le vittime del fenomeno.

Lo scenario, dunque, rimane estremamente incerto, soprattutto considerando che molti temono di limitare la natura libera del web, dandogli regole che prevengano e reprimano i reati ad esso connessi. Eppure, come giustamente rilevato sia in ambito americano che europeo, è sempre più complicato assicurare una protezione alle vittime del cyberbullismo se non esistono misure legali da poter intraprendere a tutela dei minori.

Ad oggi, infatti, guardando ad entrambi i continenti si nota come, fatti salvi gli stati americani con apposite leggi e qualche altro raro caso che si affronterà nel secondo capitolo, il cyberbullismo viene regolato da leggi già esistenti che riguardano la libera manifestazione del pensiero, le discriminazioni, il bullismo tradizionale e i diritti umani stabiliti dalle diverse convenzioni.

Approfondimento 1:

Internet Service Providers e *self-regulation*

Nel fenomeno del cyberbullismo gli Internet Service Providers ricoprono un ruolo fondamentale dal momento che essi mettono a disposizione degli utenti, anche quando minorenni, la possibilità di creare un blog, un forum, un account su un social network e persino di costruire un sito. Infatti, è proprio grazie agli spazi offerti e su di essi che il bullo può prendersi gioco della vittima e perseguitarla, sia privatamente (ad es. via *inbox* o *chat*) che pubblicamente (ad es. tramite post in bacheca o su un blog\forum).

Ciò che interessa, dunque, è capire se questi fornitori di servizi siano considerati o meno responsabili delle azioni di cyberbullismo e se, al fine di prevenire ed arginare il fenomeno, sia auspicabile e sufficiente l'autoregolamentazione.

L'orizzonte di riferimento rimane quello occidentale, con la sola esclusione del caso italiano, che verrà trattato nel capitolo successivo (vedi *infra* pag. 50) in modo da comprendere come i providers possono far valere i propri interessi "di impresa" parallelamente all'intento dei governi e delle forze dell'ordine di far rispettare la legge e tutelare i loro cittadini.

Gli Internet Service Providers hanno il merito di offrire servizi che consentono di diffondere informazioni, di dar voce alle minoranze, di esprimersi sulle questioni più disparate, di dar vita a movimenti di protesta, di socializzare ecc... Ma, nonostante ciò, essi nascondono un problema, cioè quello di fornire uno spazio libero in cui, proprio perché vi è questa possibilità di autogestirsi, molto spesso prende corpo il fenomeno del cyberbullismo.

Il primo approccio per prevenire il problema è quello legislativo, grazie al quale i bulli possono essere ritenuti responsabili in sede civile o penale, ma rimane molto difficile applicare i criteri giuridici del "mondo reale" a quello virtuale. Infatti, chiunque può nascondere la propria identità attraverso falsi profili e il materiale bloccato da un provider può essere facilmente postato altrove. Inoltre, la natura virale dei contenuti rende difficile monitorare e tracciare i dati che vengono immessi sulla rete. Queste condizioni rendono decisiva la posizione degli ISPs ed attivano la

possibilità di ricorrere ad un secondo approccio, cioè quello della *self-regulation* in cui essi si devono occupare di sorvegliare i contenuti che gli utenti caricano.

Senza entrare nel merito di quanto dovrebbe essere fatto in altre situazioni (ad es. gruppi d'incitamento all'odio razziale o omofobico), nella prospettiva del cyberbullismo, questo tipo di previsione si rivela al contempo utile e rischiosa.

Nel primo caso, quello vantaggioso, potrebbe infatti essere positiva la possibilità di segnalare il profilo, i gruppi, le pagine, i siti o i blog che prendono di mira la vittima e anche quella di stilare *policies* in cui i providers si impegnino a fronteggiare più attivamente il problema dell'anonimato, oltre che a fornire assistenza attiva nei casi di bullismo elettronico (ad es. con l'attivazione di una e-mail dedicata alle segnalazioni).

Il rischio, però, è quello non solo di far entrare in conflitto due libertà, quella di espressione e quella del web, ma soprattutto risiede nella difficoltà per i providers di poter controllare tutti i contenuti che su di essi vengono immessi, considerando la moltitudine di utenti e di trasmissioni. Inoltre, laddove si dovesse ipotizzare un intervento diretto dell'ISP, il rischio sarebbe quello di un potere di censura del tutto arbitrario.

La sfida, quindi, è nel riuscire a trovare il modo di tutelare il minore insidiato dal cyberbullo e, al tempo stesso, evitare che questa protezione diventi uno strumento per limitare la libertà degli utenti. Chiudere le pagine o i gruppi, oscurare i siti e impedire all'account di accedere al server non possono essere soluzioni da intraprendere sulla base delle sole *policies* degli ISP.

A tal proposito, le *Human rights guidelines for Internet Service Providers*[67] per la *self-regulation*, redatte dal Consiglio d'Europa, si basano proprio sull'art. 10 della Convenzione Europea dei Diritti dell'Uomo, relativo alla libertà di espressione. 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 online. Queste, poi, devono essere accompagnate anche da notizie relative a ciò che si sta facendo per aiutare gli utenti a contrastare tali problemi e a ciò che è già disponibile per tutelarli, fornendo link diretti ai siti che

[67] Consiglio d'Europa in cooperazione con la European Internet Services Providers Association (EuroISPA), H/Inf (2008) 9.

consentono alle famiglie di proteggere i loro figli, siano essi o meno istituzionali (ad es. Polizia postale o Telefono Azzurro)[68].

Parallelamente, il paragrafo n.20 indica 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.

Nonostante queste previsioni siano largamente applicabili al fenomeno del cyberbullismo, nella sezione relativa ai servizi di hosting, applicazioni e contenuti, le linee guida appaiono estremamente più utili a comprendere in che modo si intende disciplinare la responsabilità degli ISPs e i loro interventi.

Il ventesimo paragrafo dispone che il provider debba assicurarsi che i meccanismi di filtraggio o di blocco dei servizi sia legittimo, proporzionale e trasparente, in conformità con la raccomandazione del Consiglio d'Europa sulle misure per promuovere il rispetto per la libertà di espressione e di informazione[69]. Infatti, oltre ad avere l'obbligo di informare i clienti sulla natura, i criteri e le ragioni di tali meccanismi, il paragrafo 21 sottolinea che in caso di filtraggio, blocco o rimozione di contenuti illegali, ciò deve avvenire solo dopo aver contattato l'autorità competente per la verifica dell'illegittimità del contenuto, poiché agire senza aver prima provveduto a ciò può essere considerata una violazione alla libertà di espressione e di informazione.

Riguardo all'uso di applicativi come le *chat*, i blog, gli *inbox* ecc… il paragrafo 22 indica la necessità di spiegare agli utenti in che modo essi possano farne uso e quali siano le regole relative anche alla registrazione del profilo.

Per quanto riguarda l'Unione Europea, l'autoregolamentazione è uno degli strumenti della *European Strategy for a Better Internet for Children* (vedi *supra* pag. 35). L'obiettivo è sempre quello di garantire che i giovani, ma anche i genitori e gli insegnanti, abbiano accesso agli strumenti e alle informazioni che consentano un uso

[68] Par. 16, *Guidelines for ISPs providing access services*, H/Inf (2008) 9.

[69] CM/Rec (2008) 6.

sicuro della rete, in linea con quanto sin ora detto a proposito del Consiglio d'Europa. L'Unione sostiene, in tal senso, la *self-regulation* dei fornitori di servizi in modo da creare un sistema in cui eventuali problemi di sicurezza possano essere risolti rapidamente e da ciò sono nati i *Safer Social Networking Principles for the EU* (vedi *infra* pag. 104).

Per esempio, la *CEO Coalition*[70], nata nel dicembre 2011, ha elaborato strumenti di report più semplici per gli utenti, nuove impostazioni sulla privacy adeguate all'età, un uso più ampio di classificazione dei contenuti, una maggiore disponibilità di sistemi di *parental control* e una procedura di *takedown* efficace nei casi di contenuti pedopornografici.

Comunque, l'Unione Europea, con la direttiva 2000/31/CE sul commercio elettronico, aveva già escluso, da moltissimo tempo e in tutti gli stati membri, la possibilità di attribuire agli ISPs un obbligo generale di sorveglianza o di ricerca attiva degli illeciti. All'art. 15, infatti si afferma che: «Nella prestazione dei servizi di [*mere conduit*, *catching* e *hosting*] gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati». Tutto ciò avviene fermo restando che, per i servizi di hosting, l'art. 14 «lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime».

[70] Composto da: Apple, BSkyB, BT, Dailymotion, Deutsche Telekom, Facebook, France Telecom - Orange, Google, Hyves, KPN, Liberty Global, LG Electronics, Mediaset, Microsoft, Netlog, Nintendo, Nokia, Opera Software, Research In Motion, RTL Group, Samsung, Skyrock, Stardoll, Sulake, Telefonica, TeliaSonera, Telecom Italia, Telenor Group, Tuenti, Vivendi e Vodafone.

Ad ogni modo, torna il motivo iniziale della necessità di un intervento su più livelli: legislativo, educativo e poi anche relativo all'autoregolamentazione. Non a caso, sul sito stopcyberbullying.org si legge che, per fronteggiare il bullo che agisce online, è necessario informare immediatamente l'ISP perché questo tipo di molestie violano quasi sempre i "*terms of service*" e le condizioni d'uso del provider e possono avere gravi conseguenze per il titolare dell'account. Ma, subito dopo, è indispensabile anche contattare le autorità competenti, le quali possono intervenire in accordo con l'ISP e, ad esempio, rintracciare le informazioni sul titolare del profilo.

Sul sito www.wiredsafety.org è disponibile un interessante documento relativo alle violazioni dei termini di servizio[71] con cui si invitano gli utenti (genitori, insegnanti e ragazzi) a leggere attentamente le *policies* in modo da capire quali condizioni siano state violate e come. Nella maggior parte dei casi, vi è un collegamento diretto per le segnalazioni di abuso, però la maggior parte degli ISPs sono riluttanti ad agire subito dopo il primo contatto stabilito dall'utente. Ciò accade perché a volte il cyberbullo si comporta come se lui fosse la vittima, nel tentativo di coinvolgere l'ISP e farlo inconsapevolmente contribuire alle prepotenze (vedi le cd. *warning wars*, pag. 9).

Molto frequente è anche l'alterazione delle prove (ad es. fotoritocco allo *screenshot*, fotomontaggi ecc…) per far sembrare il fatto più grave di ciò che è in realtà e, inoltre, i providers ricevono centinaia di migliaia di segnalazione di termini di servizio ed è molto complicato definirne la priorità.

Per questo, spiega *Wired Safety*, la probabilità di ottenere un'azione disciplinare da parte dell'ISP dipende da quanto è dettagliato il *report* dell'utente, che deve assolutamente seguire le regole contenute nei *terms of service*. Nella maggior parte dei casi vengono richieste le seguenti informazioni: data e ora in cui le violazioni hanno avuto luogo (precisando il fuso orario), le copie delle e-mail o l'URL completa e corretta del newsgroup o della bacheca, gli *screenshots* dei messaggi offensivi, le copie di tutte le comunicazioni e le informazioni su quanto già fatto dall'utente per porre fine all'abuso.

Questo documento si conclude facendo presente all'utente che se le sue notifiche vengono ignorate, allora può rivolgersi anche alla polizia locale, chiamando in causa

[71] Wired Safety, *Reporting Terms of Service Violations*, 2010, in www.wiredsafety.org.

le autorità come già avveniva nelle *Human rights guidelines for Internet Service Providers*.

Ferma restando la deresponsabilizzazione degli ISPs, l'avvocato penalista Paolo Alma, in un'intervista rilasciata a Repubblica, ha spiegato come essa sia da affiancare a previsioni legislative che consentano di pervenire ad una soluzione rapida dei casi di cyberbullismo. Infatti è molto complicato assicurarsi che le prove restino a disposizione, considerato che sul web tutto può essere cancellato o disattivato - ecco perché tutti i siti consigliano di fare *screenshot*, salvare le conversazioni e stampare le prove di quanto accaduto[72], anche se ciò non costituisce base sufficiente per risalire al colpevole. Infatti, le informazioni vengono memorizzate da alcuni providers solo per un periodo di tempo limitato, per cui i file di log e gli indirizzi IP devono essere reperiti in modo tempestivo.

A tal proposito, l'esempio che l'avvocato riporta è quello di un caso in cui una minorenne aveva subito un furto di identità con finalità denigratorie. Il pm decise di archiviare il caso per la difficoltà incontrata nel risolverlo, visto che il gestore di telefonia non poteva conservare i dati oltre i sei mesi. «In quel caso – spiega l'avvocato – era necessario chiedere a Facebook una serie di informazioni preliminari che poi avremmo dovuto incrociare con quelle del settore telefonico per arrivare a trovare l'indirizzo del colpevole»[73]. Poco tempo dopo, la stessa vittima era stata oggetto di un video ripreso di nascosto e postato su YouTube insultandola, ma il nuovo pm acquisì subito i file di log, facendo rimuovere il video e riuscendo a rintracciare i colpevoli.

Negli Stati Uniti, il *Communications Decency Act* (CDA), approvato nel 1996 con lo scopo di evitare oscenità su Internet è stato recentemente integrato dalla *Section 230* che, al fine di incoraggiare i providers ad entrare nel mercato, gli garantisce l'immunità dalla responsabilità civile, anche nei casi di bullismo elettronico.

Secondo la legge di diffamazione tradizionale, infatti, vi sono tre soggetti che possono essere ritenuti responsabili per i commenti diffamatori: lo *speaker* (portavoce) o l'autore, il responsabile di effettuare il controllo editoriale e il

[72] Cfr. stopbullying.gov, bullying.about.com, www.wiredsafety.org, loveourchildrenusa.org.

[73] Intervista di Vittoria Iacovella a Paolo Alma, *Per colpire i responsabili trovare subito i loro dati*, 9 giugno 2013, in inchieste.repubblica.it.

distributore che era a conoscenza o aveva motivo di presumere della presenza di materiale diffamatorio ma non era intervenuto per rimuoverlo.

Contrariamente a queste previsioni, il paragrafo c del CDA, intitolato "*Protection for "Good Samaritan" blocking and screening of offensive material*", stabilisce che l'ISP non è responsabile per i contenuti immessi dagli utenti, differenziandolo quindi dalle tre figure sovra citate.

Inoltre, esso non può essere ritenuto responsabile per le azioni volontarie intraprese in buona fede per limitare l'accesso o la disponibilità del materiale che il provider o l'utente ritengono essere osceno, volgare, lascivo, sporco, eccessivamente violento, molesto o altrimenti discutibile, sia se tale materiale è costituzionalmente protetto sia se non lo è.

Questa disciplina a livello federale è stata applicata anche a livello nazionale da quegli stati che hanno approvato una legge contro il cyberbullismo (vedi *supra* pagg. 14-17) come ad esempio la Lousiana, che nel *Title 14* della *Criminal law* ha inserito la *Section 40.7*[74] per prevenire e reprimere i reati relativi al bullismo elettronico, ma precisando che nessuna previsione contenuta nella sezione si applica agli ISPs.

Tuttavia, negli USA, molti sostengono che i providers dovrebbero assumersi una parte di responsabilità per il danno causato dal cyberbullismo e che sia necessaria una modifica del *Communications Decency Act*. Secondo chi sostiene questa posizione, il Congresso dovrebbe rivedere il CDA per attribuire agli ISPs il compito di rimuovere i contenuti diffamatori a seguito della notifica degli utenti. Si dovrebbe, quindi, introdurre un sistema di *notice and take-down* come quello già previsto dalla *section 512* del *Digital Millennium Copyright Act,* che protegge gli online-service providers che inavvertitamente ospitano materiale che infrange i diritti di proprietà intellettuale. In questo modo, la revisione del CDA fornirebbe alle vittime di cyberbullismo un motivo valido per agire legalmente contro gli ISPs che scelgono di ignorare le legittime richieste di rimozione, visto che le previsioni relative alla diffamazione non sono sufficienti per fornire una tutela contro il fenomeno.

A prescindere dalle posizioni assunte nei singoli paesi, ciò che sembra più coerente con la natura neutrale della rete è far sì che il provider sia in grado di offrire sostegno al minore, mettendolo in condizione di conoscere gli strumenti cui egli può fare

[74] Sezione intitolata "Cyberbullying".

ricorso quando è vittima di cyberbullismo e anche adottando *policies* indirizzate alla tutela di coloro che subiscono tale abuso. Insomma, non deve esserci una responsabilità oggettiva, ma una "responsabilità sociale" derivante dal fatto che esso offre servizi in un mondo sempre più incentrato sulle ICT. Spetterà, poi, al giudice il compito di valutare la liceità di quanto commesso dal bullo e ciò, chiaramente, sottointende la necessità di una legge apposita, che, come già visto, manca sia a livello europeo che statunitense.

Capitolo 2

Le tutele garantite a livello nazionale e gli scenari di sviluppo delle normative

2.1 – Il Codice di autoregolamentazione per la prevenzione e il contrasto del cyberbullismo e le forme di tutela del codice penale in Italia

Nel febbraio 2014, in occasione del *Safer Internet Day*, Save the Children ha pubblicato i risultati di uno studio condotto in Italia sul cyberbullismo[75]. Il 69% dei ragazzi intervistati tra il 29 e il 31 gennaio 2014[76] lo ha indicato come il fenomeno sociale più pericoloso, addirittura prima dei fattori di rischio connessi all'uso di droghe (55%) e alle molestie da parte degli adulti (45%).

Le ragioni individuate tra le principali cause di bullismo elettronico sono pressoché le stesse da cui ha origine il fenomeno nella vita reale, cioè le caratteristiche fisiche (68%), la timidezza (62%), la bellezza nelle ragazze (58%), l'orientamento sessuale (56%) e il livello di preparazione scolastica elevato (54%). Non si tratta, quindi, soltanto dello sfruttamento dell'anonimato offerto dalla rete, che tra l'altro non costituisce una costante nei reati tra minori, ma soprattutto del rinforzo che il mondo virtuale offre agli attacchi perpetrati in quello reale (pubblico potenzialmente infinito, assenza di limiti spaziali e temporali alle prepotenze ecc…).

Nonostante gli intervistati siano quasi tutti d'accordo sulla necessità di confidarsi con un genitore (77%), quando gli viene chiesto in che modo si potrebbe prevenire il fenomeno, il 41% dei minori richiede un maggiore intervento da parte dei gestori dei social network congiuntamente ad un'attività di informazione e sensibilizzazione da parte della scuola, delle istituzioni, delle aziende e dei genitori.

Anche nel nostro paese, dunque, così come avviene a livello europeo e nel Nord America, vi sono esigenze di arginamento preventivo del bullismo elettronico e di tutela successiva delle vittime attraverso azioni congiunte di *stakeholders* diversi, ma egualmente chiamati in causa nella repressione del fenomeno.

---

[75] Ipsos Public Affairs per Save the Children Italia Onlus, *Safer Internet Day Study – Il Cyberbullismo*, febbraio 2014, in images.savethechildren.it.

[76] 458 interviste, a ragazzi di età compresa tra i 12 e i 17 anni, condotte tramite metodo CAWI.

A tal proposito, l'8 gennaio 2014 è stata approvata la prima bozza del Codice di Autoregolamentazione per la prevenzione e il contrasto del cyberbullismo. Il codice è stato sottoposto a consultazione pubblica fino al 24 febbraio sul sito del Ministero dello Sviluppo Economico, sul quale si legge il seguente comunicato stampa: « […] Si tratta del primo caso di autoregolamentazione con lo scopo di contrastare il fenomeno del cyberbullismo, di promuovere un uso positivo della Rete e di far conoscere - a chi ha meno strumenti di tutela - i meccanismi di sicurezza predisposti dagli stessi operatori del settore. Il Codice di autoregolamentazione prevede che gli operatori della Rete, e in particolare coloro che operano nei servizi di social networking, si impegnino ad attivare appositi meccanismi di segnalazione di episodi di cyberbullismo, al fine di prevenire e contrastare il proliferare del fenomeno. I meccanismi e sistemi di segnalazione dovranno essere adeguatamente visibili all'interno della pagina visualizzata; semplici e diretti, in modo da consentire anche a bambini e adolescenti l'immediata segnalazione di situazioni a rischio e di pericolo.
Gli operatori hanno convenuto che l'efficacia di questi meccanismi di segnalazione e di risposta è l'unico strumento possibile di controllo del fenomeno, per evitare che le azioni di bullismo siano ripetute nel tempo, amplificando così gli effetti che la condotta del cyberbullo ha in Rete sulla vittima»[77].
La bozza di regolamento è stata stilata dal Ministero dello Sviluppo Economico (rappresentato dall'allora vice ministro Antonio Catricalà), insieme alle principali istituzioni in materia di comunicazione e di tutela dei minori (Agcom, Polizia postale, Autorità Garante per la Privacy e Garante per l'infanzia), congiuntamente alle associazioni e agli operatori, come Confindustria digitale, Assoprovider, Google, Microsoft ecc…
All'interno del Codice, il cyberbullismo viene definito come quel fenomeno che consiste in un «insieme di atti di bullismo e di molestia effettuati tramite mezzi elettronici come l'e-mail, la messaggistica istantanea, i blog, i telefoni cellulari e/o i siti web posti in essere da un minore, singolo o da in gruppo, che colpiscono o danneggiano un proprio coetaneo incapace di difendersi»[78].

[77] Comunicato stampa: *Web, al via codice anti-cyberbullismo,* in www.sviluppoeconomico.gov.it.

[78] Ministero dello Sviluppo Economico, *Codice di autoregolamentazione per la prevenzione e il contrasto del cyberbullismo*, 8 gennaio 2014, in www.sviluppoeconomico.gov.it.

Sino ad ora, per l'Europa e gli Stati Uniti, si è parlato di progetti futuri, di bilanciamento tra diritti diversi e di azione congiunta da parte di tutti gli *stakeholder* della rete. Ebbene, la bozza del codice richiama l'attenzione su uno dei problemi cardine del cyberbullismo, cioè la responsabilità degli Internet Service Providers e gli strumenti che essi devono (o dovrebbero) mettere a disposizione per tutelare i minori dal fenomeno. All'art. 2, infatti, si parla di «sistemi di segnalazione che gli aderenti sono chiamati a mettere a disposizione» e che «devono essere adeguatamente visibili all'interno della pagina visualizzata, semplici e diretti in modo da consentire […] l'immediata segnalazione di situazioni a rischio e di pericolo». Insomma, a differenza di quanto detto sin ora, l'Italia sente l'esigenza non solo di sensibilizzare la sua popolazione rispetto al cyberbullismo (art. 4 comma 2 «Gli aderenti si impegnano altresì a sensibilizzare con campagne di formazione e informazione sull'uso consapevole della Rete»[79]), ma di agire tramite l'autoregolamentazione dei fornitori di servizi poiché essi sono i primi a poter arginare il bullismo elettronico, qualora esso si verifichi concretamente.

Infatti, a tal proposito, l'art. 3 prevede che: «Gli aderenti si impegnano a rendere efficienti i meccanismi di risposta alle segnalazioni (effettuati da personale opportunamente qualificato) azionati in termini di tempi di rimozione dei contenuti lesivi per la vittima del cyberbullismo, non superiori alle 2 ore dall'avvenuta segnalazione, al fine di evitare che le azioni si ripetano e/o si protraggano nel tempo, amplificando gli effetti che la condotta del cyberbullo ha in rete sulla vittima, per la quale l'efficacia della segnalazione costituisce l'unico strumento possibile di controllo».

Questa disciplina appare estremamente utile e consentirebbe di mediare le esigenze di tutela contro il cyberbullismo con l'assenza dell'obbligo di sorveglianza da parte dei providers prevista dal Decreto Legislativo 70/2003 (che ha recepito la direttiva sul commercio elettronico: 31/2000/CE). Esso, infatti, individua le tre tipologie fondamentali di ISP e ne determina un'esenzione generale di responsabilità, anche se vi sono alcune ipotesi in cui è previsto il coinvolgimento negli illeciti perpetrati. L'art. 14, in tal senso, descrive il provider che svolge attività di «*mere conduit*» (trasmissione o fornitura di accesso) ed esclude le sue responsabilità «a condizione

[79] Ibid.

che non dia origine alla trasmissione, non selezioni il destinatario della trasmissione, non selezioni né modifichi le informazioni trasmesse».

Nel caso in cui il provider offra servizi di «memorizzazione temporanea» (*catching*), non può essere ritenuto responsabile «a condizione che non modifichi le informazioni; si conformi alle condizioni di accesso alle informazioni; si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; 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».

In entrambi i casi, sia che si tratti di attività di *mere conduit*, sia che si tratti di servizio di *catching*, gli artt. 14 e 15 prevedono che «L'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza può esigere anche in via d'urgenza, che il prestatore, nell'esercizio delle [sue] attività […] impedisca o ponga fine alle violazioni commesse»[80].

Tuttavia, la tipologia cui si applicano maggiori responsabilità è quella dei providers impegnati nell'attività di *hosting*, cioè che offrono la possibilità di memorizzare i contenuti in maniera permanente e forniscono una serie di servizi non previsti nei casi di semplice trasporto e di hosting. Infatti: «Nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: 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; non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per

[80] Art. 14 comma 3 e art. 15 comma 2 del d. lgs. n. 70/2003.

disabilitarne l'accesso». Come si nota, quindi, in questo caso è previsto un coinvolgimento diretto del provider nel momento in cui si parla di «conoscenza» dei fatti, un elemento difficile da stabilire non soltanto praticamente, ma anche considerando che ciò comporterebbe un controllo continuativo dei contenuti immessi dagli utenti. Ciò, ovviamente, è impensabile per motivi pratici, ma è anche escluso dall'art.17 che prevede l'«assenza dell'obbligo generale di sorveglianza» sulla illiceità delle attività svolte mediante il provider. Tuttavia, il secondo comma "ritratta" l'esclusione generale di responsabilità stabilendo che: «Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto: ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite». Perciò, a questo punto, vi è un'ipotesi almeno parziale di responsabilità, perché il provider è tenuto a collaborare con le autorità, informandole dell'illecito, il che nuovamente pone il problema dell'effettiva «conoscenza» del reato, soprattutto laddove il terzo comma precisa che: «Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente».

Entrambe le previsioni, dunque, richiedono da parte del giudice una valutazione caso per caso del coinvolgimento dell'ISP, in quanto va dimostrato che esso era effettivamente a conoscenza del fatto e che la sua scelta di non rimuovere i contenuti illeciti non fosse conforme a quanto previsto dalla legge.

Il caso della valutazione del contenuto e del conseguente impedimento dell'accesso, sottolinea il delicato equilibrio tra libertà di manifestazione del pensiero e caratteristiche del web, in cui i providers non possono effettuare attività di censura, ma sono comunque chiamati ad avere un ruolo quantomeno di tutela nei confronti

degli utenti, soprattutto se si pensa al fenomeno del cyberbullismo. Probabilmente è per questo che la bozza del Codice di autoregolamentazione fa riferimento a meccanismi di risposta che devono essere eseguiti entro 2 ore dalla segnalazione, indicandoli come «l'unico strumento possibile di controllo» rispetto alle prepotenze subite dalla vittima.

Tuttavia, esso non risolve il problema relativo al potenziale ostacolo alla libertà di espressione. Infatti, bisognerebbe stabilire dei requisiti minimi per considerare "cyberbullismo" un fatto commesso sulla rete, in modo da evitare di censurare semplici manifestazioni del pensiero più aggressive del normale - il che è ciò che si cerca di evitare negli Stati Uniti in virtù del Primo Emendamento. Parallelamente, poi, si rischia di chiedere al provider di effettuare un controllo non previsto ai sensi del D. Lgs. 70/2003 perché nell'atto di rimozione del contenuto dannoso (o presunto tale) risiede non soltanto il concetto di "sorveglianza", ma anche una sorta di "potestà valutativa" di ciò che è lecito e ciò che non lo è (per il concetto di controllo preventivo cfr. Approfondimento 3a: YouTube e il bullismo, pag. 148).

Inoltre, il provider risulta ulteriormente coinvolto quando, nell'art. 17, si prevede che egli debba fornire le informazioni necessarie per l'identificazione dell'utente che ha commesso il reato[81].

A tal proposito, tornando al Codice di autoregolamentazione per la prevenzione e il contrasto del cyberbullismo, l'art. 4 dispone che: «Nel rispetto della normativa sulla riservatezza dei dati personali, gli aderenti potranno promuovere e attuare apposite politiche che consentano alle Autorità competenti di risalire all'identità di coloro che utilizzano il servizio per porre in essere comportamenti discriminatori e denigratori con l'intento di colpire o danneggiare l'immagine e/o la reputazione di un proprio coetaneo». Quindi vi è una complementarità tra l'art. 17 del D. Lgs. 70/2003 e la bozza del Codice laddove si prevede la possibilità di identificare l'utente nel caso egli commetta un illecito, rimanendo comunque all'interno di quanto previsto dal D. Lgs. 196/2003 («Codice in materia di protezione dei dati personali») all'art. 32 comma 1bis per cui «[…] i soggetti che operano sulle reti di comunicazione elettronica garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati».

[81] Art. 17 comma 2, D. Lgs. 30/2003.

Dal momento, però, che il Codice relativo al cyberbullismo non è ancora stato approvato definitivamente, è necessario comprendere quali siano le forme di tutela assicurate dallo Stato italiano alle vittime.

Considerando che il fenomeno richiede l'intervento sia della scuola che, eventualmente, della legge, bisogna innanzitutto analizzare le disposizioni scolastiche nazionali e del Ministero dell'istruzione, dell'università e della ricerca (MIUR) per capire di quali strumenti dispongano gli studenti per difendersi dal bullismo elettronico.

A tal proposito, il DPR del 21 novembre 2007, n. 235 (che ha modificato lo Statuto delle studentesse e degli studenti della scuola secondaria[82]) dispone al quarto comma dell'art. 1[83] che: «La vita della comunità scolastica si basa sulla libertà di espressione, di pensiero, di coscienza e di religione, sul rispetto reciproco di tutte le persone che la compongono, quale che sia la loro età e condizione, nel ripudio di ogni barriera ideologica, sociale e culturale». E, ancora, per il secondo comma dell' all'art.3[84]: «Gli studenti sono tenuti ad avere nei confronti […] dei loro compagni lo stesso rispetto, anche formale, che chiedono per se stessi», precisando, però, che: «In nessun caso può essere sanzionata, né direttamente né indirettamente, la libera espressione di opinioni correttamente manifestata e non lesiva dell'altrui personalità»[85]. Quindi, già nello Statuto rivolto agli studenti, si afferma il diritto di parola se esso non comporta danno a terzi, il che è alla base del corretto bilanciamento tra manifestazione del pensiero e diritti della persona di cui si parlava relativamente alla bozza del Codice sul cyberbullismo.

Tuttavia, il Decreto Presidenziale attribuisce alla prevenzione e all'educazione un ruolo fondamentale; infatti il secondo comma dell'articolo dedicato alla disciplina prevede che: «I provvedimenti disciplinari hanno finalità educativa e tendono al rafforzamento del senso di responsabilità e al ripristino di rapporti corretti all'interno della comunità scolastica […]». Infatti: «Il temporaneo allontanamento dello

[82] Decreto del Presidente della Repubblica 24 giugno 1998, n. 249.

[83] Art. 1 – Vita della comunità scolastica, Decreto del Presidente della Repubblica 24 giugno 1998, n. 249.

[84] Art. 3 – Doveri, Decreto del Presidente della Repubblica 24 giugno 1998, n. 249.

[85] Quarto comma dell'art.3 del DPR 249/1998.

studente dalla comunità scolastica può essere disposto solo in caso di gravi o reiterate infrazioni disciplinari, per periodi non superiori ai quindici giorni[86]». A tutela di ciò vi è la necessità di ricorrere a una decisione del Consiglio di istituto per le sospensioni permanenti o superiori alle due settimane[87]. Comunque: «L'allontanamento dello studente dalla comunità scolastica può essere disposto anche quando siano stati commessi reati che violano la dignità e il rispetto della persona umana o vi sia pericolo per l'incolumità delle persone». In questo due casi vi è una deroga a quanto previsto per l'allontanamento temporaneo[88] e , quindi, «la durata dell'allontanamento è commisurata alla gravità del reato ovvero al permanere della situazione di pericolo».

Pertanto, se si considerano queste disposizioni relativamente al cyberbullismo, è chiaro che il primo strumento di intervento di cui la vittima dispone è la scuola stessa, che è tenuta ad intervenire, anche con l'allontanamento temporaneo o permanente del colpevole dalla struttura[89], nel caso in cui vengano commessi i reati di cui sopra.

Tuttavia, nonostante vi possa essere anche l'intervento dell'autorità giudiziaria, «la scuola promuove un percorso di recupero educativo che miri all'inclusione, alla responsabilizzazione e al reintegro, ove possibile, nella comunità scolastica». Quindi, come già affermato in precedenza, è chiaro che se si applicano queste previsioni ai casi di cyberbullismo si nota un atteggiamento coordinato su più livelli (educativo - scolastico e familiare - e giudiziario), ma anche un'esigenza forte di attività riparatorie tese a responsabilizzare il cyberbullo anziché semplicemente punirlo per quanto ha commesso.

Specificamente riferita al bullismo è la Direttiva Ministeriale del MIUR n. 16 del 2007, che sottolinea la necessità di intervento della scuola, proprio perché essa costituisce il primo territorio in cui vengono poste in essere le prepotenze tra minori. Ciò deve accadere attraverso un'attività di prevenzione[90], articolata in specifici

[86] Comma 7 dell'art. 4 (Disciplina).

[87] Cfr. comma 6 dell' dell'art. 4 (Disciplina), modificato con DPR 235/2007.

[88] Comma 7 dell'art.4.

[89] Cfr. comma 9ter dell'art. 4 (Disciplina), introdotto con DPR 235/2007.

programmi di informazione ed educazione, ma anche con l'osservazione e lo studio del fenomeno, mediante la costituzione di osservatori regionali permanenti sul fenomeno del bullismo[91]. Il sito www.smontailbullo.it è nato proprio in seguito a queste disposizioni per rivolgersi a ragazzi, famiglie ed insegnanti nella prevenzione anche del cyberbullismo, parallelamente all'attività del numero verde nazionale 800-669696[92], cui si può chiedere sostegno e domandare informazioni su come comportarsi a livello giudiziario e non.

Il quarto paragrafo della direttiva, poi, riguarda proprio le reti informatiche[93] e, come già nello Statuto degli studenti, agisce in due direzioni: per un verso con l'elaborazione di protocolli di comportamento per i ragazzi sul web «d'intesa con le Forze dell'Ordine, le Associazioni a tutela dell'infanzia e gli organi competenti», ma anche attraverso la segnalazione alla «polizia postale di tutti i video e le foto illegali e lesivi dei soggetti coinvolti»; per altro verso «d'intesa con il Ministero delle Comunicazioni si promuoveranno iniziative rivolte agli studenti dei diversi ordini di scuola e mirate a favorire la comprensione delle caratteristiche formali e di contenuto dei media e delle nuove tecnologie e a incrementare le abilità per un utilizzo critico di tali strumenti di comunicazione di massa e di intrattenimento». Quindi, nuovamente, le strade intraprese sono quelle della prevenzione dei fenomeni come il cyberbullismo (anche se non esplicitamente nominato) e dall'altra la stesura di specifiche previsioni che consentano di contrastare gli episodi illeciti, garantendo una tutela alle vittime.

Un ultimo pilastro fondamentale a livello scolastico ha avuto origine a seguito dell'atto di indirizzo del Ministro della Pubblica Istruzione, Prot. n. 30/DIP/Segr. del 15 marzo 2007, recante «Linee di indirizzo e indicazioni in materia di utilizzo di "telefoni cellulari" e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti». Il suo testo non si riferisce ai telefonini soltanto come uno strumento di distrazione che va contro i doveri degli studenti *ex* art. 3 DPR 249/1998,

[90] Paragrafo 1 – Campagna di comunicazione diversificata, DM n. 16 del 2007.

[91] Paragrafo 2 – Costituzione di osservatori regionali permanenti sul bullismo, DM n. 16 del 2007.

[92] Paragrafo 3 – Attivazione di un numero verde nazionale, DM n. 16 del 2007.

[93] Paragrafo 4 – Mezzi di comunicazione e reti informatiche.

bensì ne sottolinea le potenzialità negative cui si è ispirata la Direttiva Ministeriale n. 104 del 2007, il pilastro cui si faceva riferimento pocanzi.

Quest'ultima affonda le sue radici non solo nello Statuto degli studenti, ma anche nel Codice in materia di protezione dei dati personali[94], perché la privacy viene tutelata sia in rapporto ai diritti e alle libertà fondamentali, che alla dignità umana, rimandando all'art. 2 comma 2 del DPR 249/1998 che prevede la tutela «del diritto dello studente alla riservatezza» da parte della comunità scolastica.

Pur riferendosi a tutti i soggetti dell'istituto (insegnanti, personale di servizio, studenti ecc…), dal momento che si parla di cyberbullismo, l'accento viene posto su quanto previsto per gli alunni, ricordando che il fenomeno indagato non consiste solo in offese ripetute da parte di un minore contro un coetaneo sul web, ma ad un tipo di persecuzione più vasta, che può comprendere anche le immagini, i filmati e il materiale audio relativi alla vittima stessa.

L'obiettivo della direttiva, quindi, è evitare che la protezione dei dati personali entri in contrasto con l'«utilizzo improprio dei telefoni cellulari o di altri dispositivi elettronici»[95], visto che spesso gli studenti li usano per «acquisire,[…], dati in formato audio, video o immagine che riproducono registrazioni vocali o filmati o fotografie digitali riconducibili a persone, studenti, docenti, o altri soggetti, che operano all'interno della comunità scolastica» e che «i dati in questione si configurano come "dati personali" ai sensi dell'art. 4, comma 1, lettera b) del predetto Codice[96]». Tali situazioni, ovviamente, possono coinvolgere anche i cd. "dati sensibili", sottoposti ad una tutela maggiore e, in generale, possono consistere nella diffusione di audio\video\immagini ad un pubblico indeterminato mediante l'utilizzo di internet ed avere finalità denigratorie. Per questo, il Ministero adotta la direttiva «recante linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni

[94] Codice in materia di protezione dei dati personali (D. Lgs. 196/2003)

[95] Direttiva Ministeriale n. 104 del 2007.

[96] Art. 4 comma 1, lettera b) del D. Lgs. 196/2003: «[…] "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale».

vocali»[97], un pilastro fondamentale della lotta al cyberbullismo e della tutela delle vittime.

Infatti, per proteggere i soggetti coinvolti nella diffusione di questo materiale, all'interno del testo «la raccolta, conservazione, utilizzazione e divulgazione a terzi dei predetti dati» viene considerata una forma di «"trattamento" di dati personali» se essi sono riconducibili ad un individuo specifico e se vengono diffusi ad un pubblico vasto se non addirittura indeterminato, viste le potenzialità della rete.

Inoltre, a tutela della vittima, viene citato anche l'art. 10 del Codice Civile sull'«Abuso delle immagini altrui» che prevede la possibilità di risarcimento e di adire l'autorità giudiziaria quando l'immagine diffusa «sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona […]», del genitore, dei coniugi o dei figli. Questa previsione attiva, quindi, la possibilità per i congiunti di poter richiedere la cessazione dell'abuso e si affianca alla legge 633 del 1941 relativa alla necessità di ottenere il consenso della persona per «l'esposizione, la riproduzione e la messa in commercio» del suo ritratto[98]. Se tale consenso viene a mancare, l'art. 161 del Codice sulla privacy stabilisce sanzioni amministrative ulteriormente aggravate nel caso si tratti di dati sensibili o giudiziari[99].

Proprio la tematica del consenso assume un rilievo fondamentale all'interno della direttiva quando essa prevede che «nel caso in cui il trattamento riguardi dati di tipo sensibile, occorre acquisire il consenso in forma scritta, fermo restando il predetto divieto di divulgare i dati sulla salute».

---

[97] Direttiva Ministeriale n. 104 del 2007.

[98] Art. 97, l. 633/1941: «Non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o colturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata».

[99] Art. 161del D. Lgs. 196/2003 – Omessa o inidonea informativa all'interessato: «La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore».

Il testo conclude affermando il ruolo fondamentale della scuola di adottare un regolamento consono al rispetto delle disposizioni ivi contenute e ribadisce che: «Gli studenti che non rispettano gli obblighi sopra richiamati, di preventiva informativa, nei casi che lo prevedono [cioè di diffusione a terzi dei dati personali], commettono una violazione, punita con una sanzione amministrativa, della cui applicazione è competente il Garante» per la Protezione dei Dati Personali[100]. Quindi, laddove non sia sufficiente una sanzione disciplinare, l'interessato può far valere i propri diritti di fronte all'autorità, che, non a caso, durante la Giornata Europea della protezione dei dati personali del 2013 si è dedicata al cyberbullismo realizzando la campagna online: "Social network: connetti la testa!". Sul sito www.garanteprivacy.it/connettilatesta è disponibile un tutorial che insegna ad usare i social network in modo sicuro, unitamente ad una serie di consigli del Garante e si può rispondere anche ad un questionario sui pericoli della rete.

Di estrema rilevanza, poi, è il ruolo dell'UNAR, l'Ufficio Nazionale Antidiscriminazioni Razziali, istituito con il D. Lgs. 215/2003 per recepire la direttiva comunitaria 2000/43/CE. Si tratta di un organo che opera all'interno del Dipartimento per le Pari Opportunità della Presidenza del Consiglio dei Ministri e che ha il compito, tra gli altri, di fornire «assistenza alle vittime di comportamenti discriminatori nei procedimenti intrapresi da queste ultime sia in sede amministrativa che giurisdizionale, attraverso l'azione dedicata di un apposito Contact center»[101] sulla base di quanto disposto dalla legge Mancino (n. 205 del 1993) e dalle direttive 43/2000/CE e 78/200/CE in tema di discriminazione.

Ciò è estremamente importante se si considera che in alcuni casi di cyberbullismo le attività diffamatorie muovono da ragioni quali la razza e l'origine etnica (dir. 43/2000/CE) o la religione, l'età, gli handicap, le tendenze sessuali e le convinzioni personali (dir. 78/2000/CE), trasformando la persecuzione in un vero e proprio *hate speech*.

Ebbene, se sussistono tali motivazioni, la vittima minorenne o un testimone possono appellarsi all'UNAR, il quale per far cessare le attività del cyberbullo mette a disposizione un sito internet e una linea telefonica gratuita per la raccolta delle

[100] Art.166 del D. Lgs. 196/2003.

[101] www.unar.it.

segnalazioni cosicché il personale possa analizzarle e comprendere in che modo procedere. Infatti, per i casi che non hanno rilevanza penale, l'Ufficio rimuove l'elemento discriminatorio dal web attraverso una comunicazione diretta con colui che ha pubblicato suddetto contenuto o il gestore del sito web. Per questo, l'UNAR dialoga continuamente con gli ISPs in modo da avvalersi delle previsione di collaborazione previste dal D. Lgs. 70/2003 che si sostanziano nell'apertura di un'istruttoria a seguito della segnalazione con la quale si avvia il monitoraggio dell'attività discriminatoria. Se a seguito di ciò la denuncia risulta fondata, allora l'UNAR contatta il provider notificandogli formalmente il contenuto illecito affinché lo rimuova, onde evitare le responsabilità previste dal già citato decreto del 2003.
Se, invece, si tratta di un caso che ha rilevanza penale, l'Ufficio avvia una collaborazione con l'Osservatorio per la sicurezza contro gli atti discriminatori (OSCAD) e la Polizia Postale affinché vi sia monitoraggio e rimozione dei contenuti abusivi attraverso l'individuazione dei responsabili, nei confronti dei quali viene avviato il procedimento giudiziario.

Continuando con ciò che riguarda il profilo strettamente attinente alla legislazione italiana, nell'ordinamento dello Stato non è presente una norma relativa al cyberbullismo, così come non è presente a livello europeo né a quello federale negli Stati Uniti d'America. Pertanto al fenomeno, come visto pocanzi nel caso del trattamento dei dati personali, vengono applicate le previsioni relative a fattispecie già esistenti nel Codice Penale, posto che, se il reato viene commesso da un ragazzo di età compresa tra i 14 e i 18 anni, il DPR 488 del 1988 stabilisce che ad esso vengano applicate le norme del processo penale minorile. Se, invece, il minore quando ha compiuto il fatto aveva un'età inferiore ai 14 anni allora ai sensi dell'art. 97 c.p. non può essere perseguito, ma soltanto rieducato.
Innanzitutto, con riferimento a quanto detto sulla protezione della privacy, il cyberbullo può essere punito ai sensi dell'art. 615-bis c.p. sull'appropriazione indebita di audio o video con la previsione di «più grave reato» per «chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini» in questione. La vittima può querelare colui che l'ha offesa (*ex* art. 615-bis), secondo quanto previsto dall'art. 120 c.p. che introduce disposizioni relative ai

minori di anni 18 stabilendo che: «Per i minori degli anni quattordici e per gli interdetti a cagione d'infermità di mente, il diritto di querela, è esercitato dal genitore o dal tutore. I minori che hanno compiuto gli anni quattordici e gli inabilitati possono esercitare il diritto di querela e possono altresì, in loro vece, esercitarlo il genitore ovvero il tutore o il curatore, nonostante ogni contraria dichiarazione di volontà, espressa o tacita, del minore o dell'inabilitato».

La querela, infatti, è uno strumento estremamente utile nei casi di cyberbullismo perché consente di procedere contro il bullo anche senza il permesso del minore che, in questo modo, non è chiamato a prendere decisioni che lo porrebbero in una situazione di ulteriore difficoltà rispetto al suo coetaneo. Inoltre, essa è applicabile (*ex* art. 597 c.p.) ai casi di "ingiuria" previsti dall'art. 594 c.p., che stabilisce la possibilità di punire chiunque «offende l'onore [percezione che l'individuo ha di sé] o il decoro di una persona presente», con un'aggravante nei casi in cui «l'offesa sia commessa in presenza di più persone». Chiaramente, trattandosi di un fenomeno che riguarda il web, la persona è "presente" con il suo account anche se non connessa ad internet nel momento in cui il reato viene perpetrato e, qualora si tratti di contenuti pubblici (ad es. post in bacheca, commenti sul blog, risposte in un forum ecc…) è chiara la «presenza di più persone».

Spesso, inoltre, la vittima (o chi per lei) querela il cyberbullo appellandosi al reato di diffamazione, previsto dall'art. 595 c.p., il quale punisce «chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione [percezione che gli altri hanno dell'individuo]» e prevede un'aggravante della pena se l'offesa viene arrecata con un «mezzo di pubblicità».

L'articolo 610 del codice penale, poi, è dedicato alla "violenza privata" e diventa fondamentale laddove punisce: «Chiunque, con violenza o minaccia, costringe altri a fare, tollerare, od omettere qualche cosa». La parola chiave che si collega perfettamente al cyberbullismo è "tollerare", perché il bullo sul web agisce prepotentemente esattamene come nella vita reale e, per di più, lo fa in modo continuativo, costringendo la vittima a scegliere se subire rimanendo connessa e con un profilo attivo oppure se cancellarsi dal social network o non accedere ad internet. Ciò, ovviamente, è contrario al principio di neutralità della rete poiché il web nasce libero e altrettanto libero deve essere l'accesso che le persone devono avere ad esso,

senza subire condizionamenti esterni, quali le violenze psicologiche e le offese ripetute.

Importante è anche l'art. 612 c.p. relativo alle minacce (con un'aggravante prevista per le "minacce gravi"), che possono essere punite se la persona offesa querela colui che le pone in essere e, spesso, il bullismo elettronico è fatto di intimidazioni oltreché di offese.

Un altro aspetto rilevante risiede nella previsione di un'aggravante all'articolo 339 c.p., nei casi in cui la violenza privata o la minaccia sia commessa «[…]da più persone riunite, o con scritto anonimo, o in modo simbolico, o valendosi della forza intimidatrice derivante da segrete associazioni, esistenti o supposte». Questo è un aspetto molto interessante, poiché spesso sui social network vengono create pagine apposite per prendersi gioco di una persona e più minori vi aderiscono oppure vengono aperti blog o *topic* all'interno dei forum che hanno lo stesso scopo. Inoltre, non è raro che si creino gruppi utilizzati per deridere la vittima senza che lei lo sappia.

L'art. 339 prosegue con la distinzione tra reati commessi con l'uso di armi (anche da parte di una sola persona), più facilmente realizzabili nel caso del bullismo tradizionale e quelli commessi senza di esse, ma perpetrati da «più di dieci persone» che ovviamente riguardano il cyberbullismo.

Inoltre, ai sensi dell'art. 8 della legge n. 38 del 23 aprile 2009: «Fino a quando non è proposta querela per il reato di cui all'articolo 612-bis del codice penale, […] la persona offesa può esporre i fatti all'autorità di pubblica sicurezza avanzando richiesta al questore di ammonimento nei confronti dell'autore della condotta. La richiesta è trasmessa senza ritardo al questore. Il questore, assunte se necessario informazioni dagli organi investigativi e sentite le persone informate dei fatti, ove ritenga fondata l'istanza, ammonisce oralmente il soggetto nei cui confronti è stato richiesto il provvedimento, invitandolo a tenere una condotta conforme alla legge e redigendo processo verbale […]». Tant'è che: «La pena per il delitto di cui all'articolo 612-bis del codice penale è aumentata se il fatto è commesso da soggetto già ammonito ai sensi del presente articolo»[102]. Tuttavia, queste previsioni appaiono

[102] Art. 8 comma 3, legge n. 38 del 23 aprile 2009.

possibili soltanto per gli «Atti persecutori»[103] e lo «Stalking»[104], puniti mediante querela della persona offesa «con la reclusione da sei mesi a quattro anni» se il colpevole mette in atto una «condotta reiterata, minaccia o molesta taluno in modo da 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». Ciò spiega per quale motivo, molto spesso le vittime di cyberbullismo si difendano dai propri persecutori appellandosi a suddette disposizioni, soprattutto considerando che è prevista un'aggravante «se il fatto è commesso a danno di un minore […] o di una persona affetta da disabilità». In questi due casi, inoltre, «si procede di ufficio» per l'avvio dell'azione penale, senza necessità di querela, ma questo comporta che per coloro che non sono maggiorenni non sia possibile utilizzare l'ammonizione di cui all'art. 8 della legge 38/2009, che invece sarebbe estremamente funzionale nello scoraggiare il perpetrare dell'attività del cyberbullo, similmente a quanto avviene con l'ordine di prevenzione della Corte Suprema in Nuova Scozia (vedi *infra* pag. 88).

Comunque, come si diceva nell'introduzione, spesso gli episodi connessi al fenomeno sono implementati dal cd. *sexting*, (diffusione in rete di foto scattate senza il permesso del soggetto, immortalato nudo o svestito, solitamente in uno spogliatoio o un bagno) e, considerato che si tratta di minori, è chiara la gravità del fenomeno, giacché una volta postati, i contenuti possono essere scaricati, copiati o linkati, rendendo difficoltosa la loro eliminazione dalla rete.

Fermo restando che vi sono la Direttiva Ministeriale n. 104 del 2007 e le disposizioni ad essa connesse (vedi *supra* pag. 59), per tutelarsi in caso di "pubblicazioni oscene" si può utilizzare l'art. 528 c.p., il quale si applica a chi «adopera qualsiasi mezzo di pubblicità atto a favorire la circolazione» di questo tipo di materiale, in cui, ovviamente rientrano le fotografie che un minore scatta ad un altro minore nudo o svestito, diffondendole poi sul web.

Ai casi di *sexting*, è bene ricordarlo, si possono applicare anche le disposizioni sulla pedopornografia di cui agli artt. 600bis, ter e quater del codice penale, intendendo

[103] Art. 612bis c.p.

[104] Ibid.

per “pornografia minorile” «ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali»[105].

Inoltre, unitamente a quanto previsto dal Codice sulla privacy, vi è una legge fondamentale, la 547 del 1993 riguardante i reati informatici (modificata nel 2008 con legge n.48 che recepisce la Convenzione di Budapest e nel 2012 con legge n. 12) che ha inserito nel Codice Penale l’art. 615ter, sull’«Accesso abusivo ad un sistema informatico o telematico». Questo, infatti, punisce: «Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo» ed è applicabile a tutti quei casi in cui il cyberbullo utilizza programmi per accedere in remoto al computer della vittima.

In quest’ultimo caso, se vi è «violazione, sottrazione e soppressione di corrispondenza», il colpevole può essere punito ai sensi dell’art. 616 c.p. poiché esso intende per "corrispondenza" anche quella «informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza». Parallelamente l’art. 618 c.p. tutela dalla «Rivelazione del contenuto di corrispondenza», che, quindi, è considerato reato.

Se, invece, il cyberbullo ruba la password per hackerare il pc o per assumere l’identità della vittima, allora può essere punito ai sensi dell’art. 615quater[106], introdotto dalla medesima legge oppure dall’art. 615quinquies nel caso in cui utilizza programmi «diretti a danneggiare o interrompere un sistema informatico»[107].

---

[105] Art. 600ter del Codice Penale

[106] Art.615quater del Codice Penale – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici: « Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. […]».

[107] Art. 615quinquies del Codice Penale – Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico: « Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri

La controversia in dottrina, ovviamente, risiede nella possibilità o meno di estendere alla rete le norme preesistenti, oltre che applicarle quelle specificamente adottate per il web. Nel caso del cyberbullismo, però, vi è un vuoto normativo in toto, tale che esso non può essere colmato se non attingendo alle fattispecie sinora richiamate.

2.2 – L'applicazione di fattispecie esistenti e l'emendamento del *Criminal Justice and Courts Act* britannico

Nel Regno Unito, il cyberbullismo è sempre più considerato un motivo di preoccupazione e una violazione dei diritti dei minori, con un forte impatto sui giovani, sulle loro famiglie, sugli insegnanti e sui problemi che esso può creare a scuola e nella vita privata come conseguenza dell'uso di siti di social networking e dalle altre piattaforme del web.

I primi passi verso un tentativo di regolamentazione normativa del fenomeno sono stati compiuti con il *Byron Review*[108], un rapporto ordinato nel settembre 2007 dall'allora primo ministro Gordon Brown e consegnato il 27 marzo 2008 allo *UK Department for Children, Schools and Families*.

Scritto e supervisionato dalla dottoressa Tanya Byron[109], esso si è concentrato sull'uso dei videogiochi e di internet - in particolare dei siti di social networking - da parte dei minori, raccomandando un focus prioritario della *Child Internet Safety Strategy* sullo sviluppo di un quadro normativo più efficace. Quest'ultimo, infatti, dovrà basarsi sulle *best practices* sinora sperimentate e sulla promozione della trasparenza, ma soprattutto dovrà fornire alle famiglie gli strumenti e le tutele di cui hanno bisogno per proteggere i loro figli.

A tal fine, il rapporto auspica la presenza di un *code of practice* "volontario", monitorato indipendentemente dai provider, relativo alla moderazione degli *user generated content* e incita i siti internet a partecipare al pubblico impegno sulle

---

apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».

[108] The Report of the Byron Review, *Safer Children in a Digital World*, Department for Children, Schools and Families, and Department for Culture, Media and Sport, in www.dcsf.gov.uk.

[109] Psicologa e scrittrice britannica, professoressa di *Public Understanding of Science* alla Edge Hill University.

procedure di *take-down*. Esso, inoltre, richiede che vengano intraprese iniziative volte a chiarire la legge su determinati tipi di materiale offensivo online, invitando l'industria di internet a promuovere attivamente la circolazione di una pubblicità responsabile relativa alle attività dei bambini sulla rete.

Il *Byron Review*, inoltre, ha chiesto un nuovo *Kitemark*[110] - un protocollo formale di verifica, che costituisce il riferimento per la certificazione - per i software di *parental control*, sottolineando anche che i provider di ricerca dovrebbero dare agli utenti la possibilità di bloccare le impostazioni di "ricerca sicura" e fornire chiari collegamenti, all'interno delle pagine di ricerca, alle informazioni relative alla sicurezza dei bambini. In ultimo, il rapporto punta a stimolare la revisione delle buone pratiche sulla verifica dell'età e incoraggia i fornitori di servizi a tenere conto del cambiamento dei rischi per i minori vista la possibilità di un accesso a internet tramite cellulare.

Tre mesi dopo, nel giugno 2008 il governo ha pubblicato il "*Byron Review Action Plan*" che ha definito come le raccomandazioni della *Byron Review* sarebbero state attuate concretamente.

Tra le tante azioni intraprese, spicca senz'altro la creazione della *Cyberbullying Taskforce* all'interno del *Department for Children, Schools and Families,* la quale ha il compito di studiare e monitorare il fenomeno per proporre dei rimedi attraverso raccomandazioni per il governo, per le forze di polizia e per le scuole in modo da mettere in pratica ciò che può rendere queste ultime più sicure.

In realtà, già prima del rapporto del 2008, vi era una notevole attività nel Regno Unito relativa alla questione del cyberbullismo, svolta tra comitati, tavole rotonde e gruppi di riflessione che però analizzano il fenomeno nel contesto più ampio dell'*e-security*.

Per esempio, l'agenzia governativa *British Educational Communications and Technology Agency* (Becta), che garantisce l'uso efficace e innovativo della tecnologia attraverso l'apprendimento, lavora dal 2005 con l'industria e con le istituzioni dell'istruzione per fornire strumenti che consentono di promuovere le migliori pratiche. Essa pone l'accento soprattutto sullo sviluppo di misure di

[110] Marchio di certificazione di qualità del Regno Unito, di proprietà della British Standards Institution (BSI Group) che lo gestisce al fine di identificare i prodotti per i quali il rispetto degli standard di sicurezza è fondamentale.

sicurezza da applicare alla rete, lavorando con dirigenti scolastici, insegnanti, ragazzi, genitori, autorità locali e Internet Service Providers.

Questa agenzia propone anche un approccio coordinato per ridurre i rischi del web, disegnando insieme ai diversi *stakeholders* un pacchetto di *policies*, di pratiche, di istruzione, di infrastrutture e di tecnologia per affrontare la questione.

Parallelamente, l'*Office for Standards in Education* controlla regolarmente la formazione sulla sicurezza di Internet nelle scuole, mentre il *Council for Child Internet Strategy* mette a punto una serie di interventi e di politiche volte a migliorare le conoscenze dei giovani e dei genitori. Promuovendo un *National Acceptable Use Policy toolkit*, infatti, esso si rivolge a tutte le scuole affinché possa essere insegnato un uso responsabile delle reti e delle attrezzature informatiche, compresi i telefoni cellulari.

Infine, la *Media Literacy Task Force* è stata costituita appositamente per affrontare la questione dell'e-security e nella sua *Charter for Media Literacy* del 2009 sostiene che il modo più efficace per garantirle la sicurezza sulla rete sia proprio quello fornire ad adulti e bambini un'alfabetizzazione mediatica che li renda più responsabili.

Poco dopo la pubblicazione di questa carta, nel dicembre dello stesso anno, il Primo Ministro e il Segretario di Stato del *Department for Children, Schools and Families* hanno chiesto alla Dottoressa Tanya Byron di fornire una rapporto sui progressi della *Byron Review*, pubblicato a marzo 2010 con il titolo "*Do we have safer children in a digital world?*". Al suo interno viene fatto presente che nel 2008 si era posto l'accento sulla raccomandazione che i siti si impegnassero a rimuovere i contenuti che violano le loro condizioni di utilizzo, una volta che questi fossero stati segnalati da un utente come inappropriati.

Ebbene, il rapporto del 2010 sottolinea che non vi è stato alcun progresso visibile in tal proposito né per ciò che riguarda i giovani (cyberbullismo), tantomeno per ciò che riguarda gli adulti.

I prestatori di servizi avrebbero dovuto abbattere i tempi di rimozione, effettuando tale operazione con coerenza e trasparenza, invece essi continuano a pubblicare contenuti che violano i loro *terms of service* senza dare alcuna spiegazione alla persona che li ha segnalati.

In realtà, però, tre dei principali fornitori di servizi di telefonia mobile - Orange, T-Mobile e O2 - prevedono la presenza di un moderatore per sostenere chi ha bisogno di assistenza e per sorvegliare le *chatroom*, intervenendo se necessario. Questi, fra l'altro, offrono una consulenza via web ai genitori e ai figli per la sicurezza su internet e sul cellulare, ma soprattutto su cosa fare nel caso in cui i minori siano vittime di cyberbullismo. Nei casi più gravi, per prima cosa, essi suggeriscono di contattare la polizia, ma, in generale, forniscono anche delle squadre per rintracciare la fonte delle chiamate offensive.

Insomma, fatta eccezione per gli operatori di telefonia mobile, sino al 2010 la situazione appariva esattamente come quella italiana, americana ed europea in genere. Pur rimanendo molti i tentativi di fronteggiare il fenomeno, sia riassumendolo nel tema della sicurezza in rete (Becta, *National Acceptable Use Policy toolkit, Charter for Media Literacy* ecc…), sia isolandolo nella sua fattispecie concreta (*Byron Review* ed azioni successive), ciò che risulta è un vuoto normativo relativamente alla tutela delle vittime che possono proteggersi soltanto grazie all'applicazione di disposizioni riferite a reati simili.

In questo senso, l'*Education and Inspections Act* del 2006 è stato adottato per includere poteri normativi applicabili anche ai casi di cyberbullismo, come la possibilità per gli insegnanti di regolare la condotta degli alunni persino fuori dalla scuola o come quella di poter confiscare i loro telefoni cellulari.

Tuttavia, questa legge non configura il fenomeno come un reato specifico e costringe le vittime a difendersi ricorrendo alle leggi penali relative alle comunicazioni o ai comportamenti molesti e minacciosi[111]. Infatti, secondo le *Interim guidelines on prosecuting cases involving communications sent via social media*[112] questo tipo di comunicazioni sono assimilabili ai reati previsti dalle leggi preesistenti e applicate dal *Crown Prosecution Service*.

Ciò che va tenuto in conto nell'applicazione delle fattispecie già disciplinate, però, è la distinzione tra comunicazioni che possono costituire minacce credibili di violenza alla persona o di danni materiali e quelle comunicazioni che invece colpiscono

[111] Malicious Communications Act (1988), Criminal Justice and Public Order Act (1994), Protection from harassment Act (1997), Section 127 of the Communications Act (2003) e Defamation Act (2013).

[112] Disponibili su www.cps.gov.uk.

specificamente un individuo o un gruppo e che possono configurarsi come molestie o *stalking* (tutelate dal *Protection from harassment Act* del 1997).

Tuttavia, il direttore delle *Public Prosecutions* stabilisce che anche le comunicazioni che non rientrano in nessuna delle due categorie sopracitate, vale a dire quelle che possono essere considerate grossolanamente offensive, indecenti, oscene o false, possono essere tutelate nel caso in cui avvengano su un social media[113].

Pur non parlando specificamente di cyberbullismo, dunque, esso ricade perfettamente nelle "*communications sent via social media*" e nelle tre tipologie individuate, pertanto ad esso si possono applicare diversi tipi di disposizioni.

Nel caso di "minaccia credibile" si può applicare la sezione n.16 dell'*Offences Against the Person Act* (1861) se essa consiste nel dichiarare di voler uccidere una persona. Se, invece le intimidazioni consistono in una vera e propria linea di condotta dal carattere continuativo, allora si applicherà l'art. 4 del *Protection from harassment Act*.

In realtà, le minacce credibili di violenza alla persona o di causare danni alla proprietà possono anche ricadere sotto la tutela della *Section 127* del *Communications Act*, che vieta l'invio di messaggi di carattere "intimidatorio" attraverso una rete pubblica di telecomunicazioni. Tuttavia, prima di avviare un procedimento penale ai sensi di suddetta sezione, i procuratori devono prestare attenzione alle parole del *Lord Chief Justice in Chambers*[114] che ha affermato l'impossibilità di applicare tali disposizioni se si tratta di «un messaggio che non crea paura o apprensione in coloro cui viene comunicato o che probabilmente lo leggeranno, […] per la semplice ragione che esso manca di contenuti minacciosi».

Quindi, come regola generale, le minacce che non sono credibili non dovrebbero essere perseguite, a meno che non facciano parte di una serie di molestie specificamente destinate ad un individuo e pertanto protette dal *Protection from harassment Act*.

Inoltre, qualora vi sia discriminazione, si possono applicare le disposizioni della sezione 28-32 del *Crime and Disorder Act* (1998) e la sezione 145 del *Criminal*

[113] Director of Public Prosecutions, *Guidelines on prosecuting cases involving communications sent via social media*, 19 dicembre 2012, in www.cps.gov.uk.

[114] Neutral Citation Number: [2012] EWHC 2157, Case n. CO/2350/2011.

Justice Act che prevede un'aggravante nei casi di riferimenti razziali/religiosi o la sezione 146 che, invece, la prevede nei casi di discriminazioni sulla disabilità, sull'orientamento sessuale o sull'identità transgender.

Per quanto riguarda le comunicazioni indirizzate specificamente ad un individuo o ad un gruppo, si applica la sezione 7 del *Protection from harassment Act* se esse si configurano come una linea di condotta continuativa (stalking o molestie), ma è applicabile anche il *Criminal Justice Act,* nelle parti sovra citate, quando vi è una discriminazione.

Nel caso di comunicazioni grossolanamente offensive, indecenti, minacciose, oscene o false, che costituiscono almeno la metà dei casi di cyberbullismo, la tutela è riscontrabile nella *Section 1* del *Malicious Communications Act* o nella *Section 127* del *Communications Act*.

Quest'ultima disposizione è già stata analizzata, mentre la prima fonte citata si occupa dell'invio di una comunicazione elettronica con l'intento di causare disagio o ansia nel destinatario, attraverso contenuti indecenti o offensivi, oltreché falsi o trasmessi con identità nascosta.

Il reato si ha nel momento stesso in cui la comunicazione viene inviata, senza che vi sia il requisito giuridico che essa raggiunga il destinatario. Ciò appare molto interessante se si considera che in molti casi di cyberbullismo vengono aperte pagine o blog con l'intento di tormentare la vittima senza che essa venga "formalmente" contattata, ma rivolgendosi ad un pubblico piuttosto differenziato che può non comprenderla.

Anche la *Section 127* del *Communications Act* si rivolge ai messaggi inviati per provocare fastidio, disagio o ansia e dal carattere gravemente offensivo, minaccioso, indecente o falso. Tuttavia, a differenza del *Malicious Communications Act*, deve essere dimostrata la consapevolezza dell'imputato sul fatto che il messaggio avesse questo tipo di caratteristiche, pertanto vanno provati sia l'intento di far recepire al destinatario il contenuto trasmesso che la terminologia utilizzata all'interno della comunicazione.

Similmente al *Malicious Communications Act*, invece, anche in questo caso il reato è commesso con il solo invio, senza necessità che la vittima visualizzi il messaggio.

A tal proposito, nel caso Chambers v. DPP[115], la *Divisional Court* ha stabilito che, dal momento che un messaggio inviato da Twitter è accessibile a tutti coloro che hanno accesso a Internet e si tratta di un contenuto inviato tramite una rete pubblica di telecomunicazione, è possibile applicare la *Section 127* del *Communications Act*.
Tuttavia, stando a queste previsioni, potrebbero essere denunciati un gran numero di casi, anche pressoché inesistenti, considerando che Facebook, Twitter, YouTube ecc… danno vita a centinaia di milioni di comunicazioni ogni mese.
Nel Regno Unito, proprio per prevenire questo tipo di problema, il *common law*, dopo aver recepito l'art. 10 della Convenzione Europea dei Diritti dell'Uomo nello *Human Right Act*, stabilisce un diritto di espressione in negativo, cioè definisce i casi in cui può esservi censura, mantenendo libere tutte le altre forme di espressione seppur scioccanti, sgradevoli, satiriche, iconoclaste, maleducate, di cattivo gusto, dolorose per chi le subisce o contenenti pareri impopolari o fuori moda su questioni gravi o banali.
Ciò che determina la perseguibilità del reato, come già visto, è che le affermazioni siano grossolanamente offensive, indecenti, oscene o false e che abbiano lo scopo di causare disagio o ansia nel destinatario, sia molestandolo che minacciandolo.
Tuttavia, questo tipo di previsioni sono piuttosto complesse da applicare ai casi di cyberbullismo, non solo per il fatto che si tratta di un fenomeno che coinvolge minori, ma anche perché l'estensione alla rete di fattispecie già esistenti andrebbe ad imbavagliare la libera espressione sul web.
Per quanto riguarda, invece, i reati connessi al bullismo elettronico e relativi al furto di identità, di chiave d'accesso o comunque all'hackeraggio in genere, è applicabile il *Computer Misuse Act* del 1990, il quale si riferisce al materiale informatico cui si è acceduto o che è stato modificato senza autorizzazione e all'accesso effettuato sempre senza permesso, ma con l'intento di commettere o facilitare la commissione di altri reati.
Anche in questo caso manca del tutto la previsione di illeciti relativi al cyberbullismo e le disposizioni sono piuttosto insufficienti per arginare il fenomeno, soprattutto ricordando che esso riguarda i minori. Dunque, sempre più chiara è l'esigenza di adottare una disciplina specifica, che individui concretamente le diverse ipotesi di

[115] Ibid.

configurazione del reato, i contesti e le sue modalità, ma soprattutto le conseguenze cui i colpevoli andrebbero in contro.

Nel marzo 2013, sul sito della *National Society for the Prevention of Cruelty to Children*[116] sono state pubblicate delle statistiche sul cyberbullismo ricavate dalla comparazione dei report e delle ricerche governative in materia.

Così, mentre l'NSPCC dichiara che un bambino su cinque è stato vittima del fenomeno tra il 2012 e il 2013, al punto che *ChildLine*[117] ha effettuato 4.507 consulenze ai giovani che erano preoccupati di essere presi di mira, il 2 agosto dello stesso anno, una ragazzina inglese di 14 anni, Hannah Smith, viene trovata impiccata nella sua camera a seguito delle continue prepotenze subite sul social network Ask.fm (vedi *infra* pag. 178).

A partire da questo evento, nel Regno Unito si inizia a sentire l'impellente necessità di modificare in fretta la legislazione per affrontare il problema del bullismo elettronico e i primi segnali arrivano dal Galles, dove il *Children's Commissioner*, Keith Towler, propone di renderlo un crimine.

Il dibattito si è protratto a lungo, tra la paura di imbavagliare il web e l'esigenza di proteggere i minori da un illecito così pericoloso ma ancora senza tutela giuridica. Tuttavia, il 27 marzo 2014, il *Criminal Justice and Courts Bill Committee* si è riunito per discutere una possibile modifica alle disposizioni della legge.

L'emendamento al *Criminal Justice and Courts Act*, proposto dal deputato conservatore Angie Bray, prevede una condanna fino a due anni di carcere per i colpevoli di cyberbullismo e di "*text-message abuse*". Il segretario della giustizia, Chris Grayling, ha sostenuto questa innovazione poiché essa permetterebbe di raggiungere nuove regole a funzionali a combattere le molestie sessuali e gli abusi verbali perpetrati su internet o tramite telefoni cellulari sia in Inghilterra che in Galles.

In realtà, questo "aggiornamento" delle pratiche della Crown Court consentirebbe non soltanto una pena detentiva, ma prolungherebbe anche il periodo di tempo messo a disposizione delle autorità per costruire il caso e perseguire i trasgressori. Pertanto,

[116] www.nspcc.org.uk.

[117] www.childline.org.uk.

esso avrebbe una doppia utilità nella tutela delle vittime, auspicata anche dal ministro labourista per la Cultura, i Media e lo Sport, Helen Goodman.

Sul versante opposto, invece, si colloca chi esprime preoccupazione sull'eventuale criminalizzazione, poiché essa non insegnerebbe ai giovani come comportarsi sul web. Il consigliere di David Cameron, Claire Perry, ha dichiarato che l'approccio dovrebbe consistere nell'introdurre pratiche comuni dei providers, come la possibilità di applicare filtri, la presenza di *warning pages* che avvertono della presenza di contenuti per adulti e il blocco dei materiali pornografici sui servizi pubblici di Wi-Fi.

Insomma, anche nel Regno Unito appare sempre più evidente l'esigenza di un quadro giuridico chiaro per affrontare il problema del cyberbullismo, sia in relazione alle pene da comminare ai colpevoli, sia per quanto riguarda la possibilità per chi lo subisce di avere il tempo e i mezzi per proteggersi e difendersi. Parallelamente, riprende vita il tema del coinvolgimento degli ISP che dovrebbero mettere a disposizione degli strumenti utili affinché i minori possano usufruire del web in modo sicuro.

Intanto, dopo la discussione del Comitato tenutasi il 27 marzo, l'emendamento presentato in Parlamento si aggiunge alle modifiche alle leggi che dovranno essere votate quest'anno.

2.3 – Le innovative proposte di legge della Nuova Zelanda e del Canada

Analizzati alcuni dei panorami americani ed europei, è interessante soffermarsi sull'emisfero australe, all'interno del quale vi è l'Oceania, un terzo continente oltre ai due già osservati, che presenta non poche innovazioni.

Dei diversi paesi che la compongono, si è scelto di analizzare la Nuova Zelanda per poi giungere sino al Canada poiché dei loro ordinamenti si sente parlare poco, quasi fossero troppo lontani per influire sulle politiche occidentali, eppure essi stanno delineando linee di sviluppo di grande importanza in riferimento al fenomeno del cyberbullismo.

All'indirizzo www.cyberbullying.org.nz vengono forniti una serie di interessanti spiegazioni che vanno dalla semplice definizione del fenomeno ad una più accurata

lista delle cose da fare se ne si è vittima o se si conosce qualcuno che sta subendo un abuso.

Il sito è patrocinato da NetSafe, un'organizzazione indipendente senza scopo di lucro che promuove l'uso sicuro e responsabile della rete, che ha sede in Nuova Zelanda e riunisce moltissimi partner provenienti dal governo, dal settore legislativo, industriale e anche educativo[118], con una partecipazione fondamentale dei giovani e dei genitori. L'obiettivo è quello di educare e sostenere i cittadini, ma anche le organizzazioni relative alle ICT, rispetto ad una serie di questioni, tra cui il cyberbullismo.

Tra i suoi progetti più recenti spicca sicuramente la creazione della *National Cyber Bullying Taskforce*, che si occupa di studiare in che modo si dovrebbero implementare la prevenzione e il contrasto del fenomeno, lavorando con le agenzie governative, i fornitori di servizi ICT e i rappresentanti del settore dell'istruzione. Questo originalissimo organo, che ricorda quello istituito in Gran Bretagna nel 2008, ha tre obiettivi chiave per proteggere i giovani neozelandesi: innanzitutto, lo sviluppo di un approccio *multi-stakeholder*s coordinato, che aiuterà le scuole e i giovani ad affrontare le minacce relative al fenomeno. In secondo luogo, esso si ripropone di sviluppare un uso produttivo della tecnologia da parte di adulti e ragazzi. In ultimo, l'intento è anche quello di cercare una soluzione appropriata che l'intera comunità possa applicare per ridurre il numero di incidenti di bullismo elettronico.

Come già visto in Europa e negli Stati Uniti, dunque, anche in questo caso l'approccio non è esclusivamente legislativo, cioè non si cercano solo rimedi giuridici al fenomeno, bensì l'obiettivo è quello di effettuare un lavoro congiunto tra providers, settore dell'istruzione e governo, al fine di ottenere maggiore tutela per le vittime di abusi sul web.

A dimostrazione di ciò, vi è *l'Education Act*, che nella *National Administrative Guideline 5* stabilisce che le scuole devono provvedere ad assicurare agli studenti un ambiente sicuro sia dal punto di vista fisico che emotivo.

[118] Tra i partner principali vi sono: la Commerce Commission, la Department of Internal Affairs Censorship Compliance Unit, l'ECPAT ChildALERT, Internet NZ, IBM, Microsoft, Symantec, Telecom, Vodafone, i ministri dello Svilippo economico e dell'Istruzione, l'ufficio del Privacy Commissioner, la NZ Police, tutte le scuole primarie e secondarie della Nuova Zelanda, ma anche le università e gli istituti tecnici, la SPINZ – Suicide Prevention Information NZ, la State Services Commission ecc… (cfr. www.netsafe.org.nz).

Ciò si riferisce anche a quei comportamenti, come il cyberbullismo, che possono accadere al di fuori delle mura scolastiche ma che hanno conseguenze sul benessere dei ragazzi che vivono l'ambiente dell'istituto[119].

Un aspetto molto interessante risiede nel fatto che la responsabilità penale in Nuova Zelanda si ha non appena compiuti i 10 anni di età, mentre i maggiori di 16 anni che commettono un reato vengono trattati dai tribunali al pari degli adulti. Ciò significa che le disposizioni riferibili al fenomeno si applicano in toto anche ai minorenni, pur non essendoci una legge specifica sul bullismo elettronico.

A tal proposito, infatti, il cyberbullismo può essere un reato secondo una serie di leggi diverse, inclusa il *Defamation Act* del 1992 e le sezioni 249 e 252 del *Crimes Act*, sostituite rispettivamente dalla *Section 15* del *Crimes Amendment Act* del 2003[120] e dalla *Section 5* del *Crimes Amendment Act* del 2011[121].

La prima disposizione riguarda i casi di «*Accessing computer system for dishonest purpose*» e fissa a cinque anni la pena detentiva per chi, direttamente o indirettamente, accede a qualsiasi sistema informatico con intenzione, disonestà o inganno e, senza giusta pretesa, tenta di ottenere qualsiasi proprietà, privilegio, servizio, vantaggio pecuniario, benefit, considerazione o di causarne la perdita in qualsiasi altra persona. La pena aumenta a sette anni nel caso in cui l'obiettivo sia effettivamente raggiunto e non resti solo un tentativo vano.

La seconda disposizione, invece, si riferisce ai casi di «*Accessing computer system without authorisation*», prevedendo la possibilità di reclusione sino a due anni per chi accede intenzionalmente, direttamente o indirettamente, a qualsiasi sistema informatico senza permesso, sapendo di non essere autorizzato o agendo incautamente senza sapere se si possa effettivamente accedervi.

Ovviamente, entrambe le previsioni possono essere estese ai casi di cyberbullismo, ma non ne esauriscono affatto la complessità, dal momento che esso si articola in una serie di fattispecie tra loro molto differenti.

Per questo, vi sono altre leggi che riescono, seppur parzialmente, a colmare il vuoto lasciato dall'assenza di una normativa specifica. E' il caso, ad esempio, della *Part 9A*

[119] The National Administration Guidelines (NAGs), in www.minedu.govt.nz.

[120] Crimes Amendment Act 2003 (2003 N. 39).

[121] Crimes Amendment Act 2011 (2011 N. 29).

della *Crimes Law*, intitolata *Crimes against personal privacy*. Al suo interno, infatti, vengono individuati illeciti quali l'acquisizione[122], la pubblicazione, l'esportazione o la vendita di «*intimate visual recording*»[123] , ma il problema è che queste previsioni sono formulate in un linguaggio neutro, che non considera lo sviluppo delle nuove tecnologie, limitandosi piuttisto a mettere in atto principi di base che necessitano di essere tradotti nelle esigenze del mondo moderno.

Il *Summary Offences Act* del 1981 prevede l'esistenza di un reato di intimidazione, commesso da una persona che, con l'intento di spaventare o intimidire l'altro o sapendo che il suo comportamento potrebbe ragionevolmente avere questo tipo di conseguenze, minaccia di danneggiare la vittima, qualsiasi membro della sua famiglia o una delle sue proprietà[124].

A questa disposizione si collega l'*Harassment Act*, che crea un reato di molestia laddove il colpevole induce la vittima a temere per la propria sicurezza o per quella di un membro della sua famiglia[125].

Il *Telecommunications Act* vieta l'uso improprio degli apparecchi telefonici, con riferimento sia alle offese perpetrate utilizzando un linguaggio indecente o osceno, sia all'utilizzo del telefono per disturbare, infastidire o irritare, anche laddove non vi sia dialogo durante la chiamata o vi sia la trasmissione maliziosa di comunicazioni o suoni che offendono il destinatario[126].

L'applicabilità di queste disposizioni ai casi di cyberbullismo è possibile ed auspicabile, soprattutto in assenza di una legislazione specifica. Tuttavia, alla luce dei più recenti fatti di cronaca (vedi Approfondimento 3b: Le indagini degli inquirenti e le decisioni dei giudici, pag. 171), una delle previsioni più interessanti è quella della *Section 179* del *Crimes Act*, ai sensi della quale è un reato consigliare, incitare o indurre una persona al suicidio se essa poi effettivamente commette o tenta di commettere il gesto.

---

[122] Section 216H: Prohibition on making intimate visual recording, Crimes Act (1961), in www.legislation.govt.nz.

[123] Section 216J: Prohibition on publishing, importing, exporting, or selling intimate visual recording, Crimes Act (1961), in www.legislation.govt.nz.

[124] Summary Offences Act 1981, section 21.

[125] Harassment Act 1997, section 8.

[126] Telecommunications Act 2001, section 112(a).

Nell'ottica del bullismo elettronico, considerati i numerosi casi di adolescenti che si tolgono la vita a seguito delle prepotenze subite, tale previsione costituisce un'ulteriore forma di tutela per la vittima (o per la sua famiglia), poiché consente di provare quantomeno il ruolo svolto dal cyberbullo nell'indurla al suicidio. L'aspetto controverso risiede, ovviamente, nella differenziazione tra istigazione diretta, magari con dei post espliciti su un social network e istigazione indiretta, per cui a seguito di un comportamento continuativamente e pubblicamente molesto, la vittima decide di togliersi la vita. In quest'ultimo caso, infatti, ma in generale anche nel primo, la difesa si basa sempre sull'instabilità psicologica della vittima, che viene presa come elemento a sé stante e pre-esistente rispetto alle attività minatorie.

Proprio questo tipo di problematiche sottolineano l'esigenza di una disciplina chiara e specifica per il fenomeno, poiché pur essendo possibile applicargli le fattispecie già esistenti, esse non bastano a regolarne le conseguenze complesse e sfaccettate che può assumere. L'*Harrasment Act*, per esempio, nella *Section 3* precisa che si può parlare di molestia solo quando il comportamento viene ripetuto in almeno due occasioni diverse e nell'arco di tempo di 12 mesi o più. Quindi, anche in questo caso, è piuttosto problematico applicare al cyberbullismo tali disposizioni, poiché non è detto che il fenomeno abbia una durata pari ad un anno e soprattutto è necessario interrompere le prepotenze sin da subito, non certo dover aspettare 12 mesi prima di poter intervenire.

Un'altra previsione interessante è quella della *Section 66* del *Crimes Act*, relativa alla colpevolezza di tutti coloro che prendono parte al reato su incitamento, consiglio o esortazione, il che, nel caso del bullismo elettronico, è facilmente riconducibile a quei gruppi di persone che si coalizzano per inviare messaggi offensivi ad un altro soggetto o denigrarlo su una pagina o un sito.

In realtà, molto spesso si può ricorrere anche alla cd. *civil law*, che comprende sia la *common law* che gli statuti ed essa può risolvere le controversie tra cittadini e consente di ottenere un risarcimento per i danni subiti. In questi casi, pur non essendo previsto l'intervento della polizia, è possibile applicare la legge civile anche ai torti subiti attraverso comunicazioni online.

La *law of torts*, infatti, protegge ad esempio il reato di violazione della privacy, fornendo un rimedio nel caso in cui vengano resi pubblici fatti per i quali vi era una

ragionevole aspettativa di privacy, essendo la pubblicazione altamente offensiva per la persona interessata. Questo tipo di previsione è applicabile nei casi di *sexting* o in quelli in cui il cyberbullo si prende gioco della vittima immettendo in rete materiali imbarazzanti che la riguardano.
Un altro caso in cui si può applicare la *civil law* è quello della diffamazione che, pur avendo una specifica legge con relative sanzioni penali[127], consente di adottare rimedi in sede civile per le dichiarazioni che possono influire negativamente sulla reputazione di una persona e delle quali non può essere dimostrata la veridicità. Inoltre, è prevista una tutela in caso di pubblicazione di informazioni scambiate in confidenza dal momento che la loro diffusione si configura come un torto.

Alla luce di quanto detto, pur essendovi leggi che esprimono principi flessibili e tecnologicamente neutri, le fattispecie esaminate sono state regolate molto prima dell'avvento dei nuovi media, perciò è piuttosto difficile adattarle in toto alle nuove forme di comunicazione. Queste leggi da estendere anche al web, poi, sono sparse nei diversi statuti, che necessitano di essere incrociati per poter risolvere i diversi illeciti. Inoltre, vi sono disposizioni del diritto penale che hanno diverse conseguenze rispetto a quanto previsto per gli stessi reati dalle prescrizioni del diritto civile.
Proprio per questo, la *Law Commission* neozelandese ha pubblicato un rapporto sulla comunicazione digitale dannosa, «*Harmful digital communications*»[128], nel tentativo di risolvere questi problemi e non soltanto di emendare le leggi già esistenti, ma anche di proporre nuovi reati così da affrontare i danni specifici di alcuni tipi di comunicazione digitale.
Innanzitutto, la proposta è quella di colmare le lacune di diritto penale relative ai potenziali danni della comunicazione, configurando nuovi reati e apportando modifiche a quelli già esistenti nel *Crimes Act* del 1961 e nel *Summary Offences Act* del 1981 che già da tempo, pur con linguaggio tecnologicamente neutro, consentivano di affrontare le conseguenze della comunicazioni nocive.

[127] Defamation Act 1992.

[128] Ministerial Briefing Paper, Law Commission, *Harmful digital communications: the adequacy of the current sanctions and remedies*, Wellington, New Zealand, August 2012, in www.lawcom.govt.nz.

Per quanto riguarda le minacce, le intimidazioni e i messaggi offensivi, la legge penale[129] persegue soltanto quei casi in cui la vittima ha ragione di temere danni fisici, sia a persone che a cose. L'inflizione di angoscia o disagio psicologico non sono protetti, a meno che non si tratti di un grave pregiudizio psichiatrico, che comunque deve essere provato da una perizia specialistica.

Il problema, infatti, è che l'uso delle nuove tecnologie può avere effetti più invadenti e pervasivi, quindi il potenziale danno emotivo è maggiore rispetto a prima. C'è il rischio di autolesionismo o comunque di disagi psicologici, anche se essi non sono legati alla specifica paura di danni fisici, bensì riguardano sentimenti come l'umiliazione e la paura di un attacco verbale e non vi è ragione di pensare che questi tipi di danni emotivo debbano essere considerati meno gravi.

Proprio a dimostrazione di ciò, nelle recenti modifiche al *Privacy Act* del 1993 si è configurato un nuovo reato di violazione della privacy che protegge un danno immateriale, costituito da perdita della dignità, lesione ai sentimenti o significativa umiliazione. In tal senso, anche nell'*Harrasment Act*, la concessione di un ordine restrittivo ha come criterio quello dell'angoscia del querelante.

Inoltre, come si è visto in precedenza, anche il *Telecommunications Act*, sin dal 1987, ha reso un reato l'utilizzo di un dispositivo telefonico «ai fini di disturbare, infastidire o irritare qualsiasi persona» o per trasmettere con malizia una comunicazione o dei suoni che offendono il destinatario.

Per avvalorare la tesi della necessità di apportare cambiamenti alle previsioni esistenti, la *Law Commission* sottolinea il fatto che le giurisdizioni estere stanno iniziando a muoversi per criminalizzare le comunicazioni che causano grave disagio psicologico, come ad esempio il Regno Unito, che configura come reato l'invio di una comunicazione elettronica indecente/gravemente offensiva oppure di carattere osceno/minaccioso[130].

Un altro esempio è quello del Texas, che ad oggi vieta espressamente l'impersonificazione online di un altro soggetto, utilizzando il suo nome o il suo

[129] Crimes Act 1961.

[130] Communications Act 2003 (UK), section 127.

account su un social network o su un sito internet, con l'intento di nuocere, ingannare, intimidire o minacciare[131].

Tuttavia, anche per quanto riguarda la *civil law* si sente l'esigenza di apportare modifiche alle previsioni relative agli ordini restrittivi dell'*Harassment Act*. Questo, infatti, oltre a dover includere espressamente le comunicazioni elettroniche come atto di molestia specifico, dovrebbe tenere conto delle peculiarità della rete e ridurre la previsione secondo cui il comportamento è da definirsi "molesto" solo quando viene ripetuto in almeno due occasioni diverse e nell'arco di tempo di 12 mesi o più. A tal proposito, infatti, il web consente di pubblicare contenuti che possono provocare danni per un lunghissimo periodo, anche se essi vengono postati una sola volta. Peraltro, la vittima spesso non è in grado di rimuovere suddetti contenuti, quindi, di fatto, sarebbe opportuno modificare la *Section 3* in modo tale che un comportamento molesto possa essere definito tale anche quando costituito da un unico atto con effetti prolungati nel tempo.

All'interno del *paper* della *Law Commission*, si raccomanda, inoltre, la creazione di un Tribunale delle comunicazioni che opererebbe come un "giudice delle molestie", imponendo una serie di sanzioni e rimedi, tra cui la possibilità di concedere un risarcimento monetario, la pubblicazione delle scuse o della correzione di quanto affermato, di ordinare il diritto di replica per la vittima o che l'imputato cessi il comportamento in questione, ma anche la possibilità di ordinare la rimozione dei contenuti tanto al colpevole quanto all'ISP.

La giurisdizione del tribunale si estenderebbe a tutte le forme di comunicazione elettronica, inclusi i commenti sui siti web, sui forum e sui blog, ma anche quelle realizzate nei social media (ad es. Facebook e Twitter) o via e-mail e chat/messaggi. Tuttavia, la *Commission* prevede esplicitamente l'esclusione delle comunicazioni via telefono (SMS/telefonate) da queste previsioni, poiché esse sono funzionali a tenere testa alla caratteristiche distintive della comunicazione elettronica, cioè la sua capacità di diffondersi al di là del mittente e del destinatario originari.

Coloro che avrebbero diritto di sporgere denuncia al tribunale sarebbero non solo le vittime, ma anche i loro tutori o i genitori in caso esse siano minorenni o disabili oppure il personale scolastico che voglia agire a protezione degli studenti. Anche la

[131] Texas Penal Code, Chapter 33, Section 33.07(a).

polizia avrebbe accesso al tribunale laddove, nel corso delle indagini, si rendesse conto che la comunicazione elettronica costituisce una minaccia alla sicurezza della vittima.

Queste nuove previsioni legislative si applicherebbero a tutti i maggiori di 14 anni, andando così a coprire una larga parte del fenomeno del cyberbullismo e imponendo al colpevole una pena detentiva fino a tre mesi o una multa non superiore ai 2000 dollari.

La seconda opzione offerta dalle riflessioni della *Law Commission* è quella della creazione di un Commissario per le comunicazioni, collegato all'attività della *Human Rights Commission*. Questi non avrebbe i poteri esecutivi di un tribunale, ma il suo ruolo sarebbe quello di fornire informazioni e, se possibile, risolvere i problemi in maniera informale, per esempio attraverso la mediazione, identificando quali previsioni legislative sta violando il comportamento del cyberbullo. Inoltre, egli potrebbe anche formulare raccomandazioni rivolte alle autorità competenti con l'obiettivo di prevenire i problemi o migliorare la situazione esistente oppure, nei casi di danno grave, il Commissario potrebbe denunciare il caso alla polizia.

Tuttavia, a protezione della libertà di espressione e della natura aperta e neutrale del web, il *paper* si conclude con l'enunciazione dei principi che devono essere applicati solo a quelle comunicazioni che provocano notevole stress emotivo ad un soggetto, identificandole nei casi di:

- divulgazione dati personali sensibili;
- minacce/intimidazioni;
- messaggi gravemente offensivi, indecenti o osceni;
- comunicazioni che sono parte di un modello di condotta che costituisce molestia;
- false accuse;
- incitamento di terzi ad inviare messaggi alla vittima con l'intenzione di danneggiarla;
- incoraggiamento a suicidarsi;
- pubblicazione di materiale confidenziale;

- denigrazione per origini etniche, religiose, convinzioni etiche, genere, orientamento sessuale o disabilità[132].

Per quanto riguarda le responsabilità dei providers, in Nuova Zelanda essi non possono essere incriminati se provano di non essere a conoscenza della presenza del materiale diffamatorio e se essi non hanno ricevuto alcuna segnalazione, pertanto, in entrambi i casi, non possono essere accusati di negligenza.

In sostanza, la posizione prevalente è quella di non ritenerli legalmente responsabili, in prima istanza, per la diffusione di contenuti creati dai loro utenti[133]. Tuttavia, vi possono essere occasioni in cui un intermediario viene costretto da un ordine del tribunale a rimuovere i contenuti. Tra l'altro, una volta che ciò è avvenuto, il giudice può anche richiedere che le *cache* vengano svuotate così da rendere più efficace il *take-down*.

Tuttavia, molti ISPs hanno assunto strumenti di autoregolamentazione, compresa la definizione di termini di utilizzazione e la creazione di comunità che si occupano della moderazione e della risposta alle segnalazioni.

Una delle caratteristiche della riforma proposta dalla *Law Commission* è quella di fornire un meccanismo autorevole di mediazione per le controversie locali e, nei casi in cui la mediazione non riesce, di assicurare rimedi per coloro che sono colpiti da comunicazioni elettroniche dannose.

L'obiettivo, però, è quello di rendere responsabili le persone per i loro contenuti, non gli ISPs, i quali, tuttavia, dovrebbero collaborare nella risoluzione dei casi più complessi.

Insomma, ancora una volta, come già visto negli altri stati analizzati, l'intento è quello di sviluppare politiche nazionali e protocolli degli ISPs che siano uniformi, trasparenti e accessibili, per sviluppare sia norme che tecniche in grado di contrastare

---

[132] «There should be no communications which cause significant emotional distress to an individual because they: Disclose sensitive personal facts about individuals […] Are threatening, intimidating or menacing […] Are grossly offensive […] Are indecent or obscene […] Are part of a pattern of conduct which constitutes harassment […] Make false allegations […] Contain matter which is published in breach of confidence […] Incite others to send messages to a person with the intention of causing that person harm […] Incite or encourage another to commit suicide […] Denigrate a person by reason of that person's colour; race; ethnic or national origins; religion; ethical belief; gender; sexual orientation or disability», Ministerial Briefing Paper, Law Commission, *Harmful digital communications: the adequacy of the current sanctions and remedies*, Wellington, New Zealand, August 2012, in www.lawcom.govt.nz.

[133] Defamation Law 1992.

il cyberbullismo e gli altri fenomeni dannosi delle comunicazioni elettroniche. A questa prospettiva, poi, si aggiunge la necessità di intervenire sul piano dell'educazione, altro tratto comune rispetto a ciò che sta accadendo nel resto del mondo.

Il *paper*, infatti, sottolinea come il bullismo elettronico non possa essere assolutamente separato dalle altre forme nocive di comunicazione via web, ma riconosce anche che esso ha la priorità nel cercare soluzioni alle patologie del mondo digitale poiché coinvolge bambini e adolescenti, cioè il gruppo più vulnerabile all'uso improprio della rete[134]. Pertanto, è necessario emendare la *National Administrative Guideline 5* così da coinvolgere le scuole affinché esse adottino *policies* e procedure relative al contrasto del fenomeno, ma anche programmi educativi funzionali alla sua prevenzione.

Il ministro della Giustizia, Judith Collins, ha accolto con favore le 160 pagine di raccomandazioni proposte dalla *Law Commission* e nel maggio 2013 le ha trasformate nella proposta di legge *Harmful Digital Communications Bill*, largamente basata sulle previsioni del *paper* del 2012 sinora descritte, con l'eccezione della sostituzione dell'originario progetto di un Tribunale delle comunicazioni con un'*Agency* incaricata di investigare sui casi di cyberbullismo e di risolverli innanzitutto con la mediazione, per poi passare alla *District Court* nel caso la controversia non venga risolta. Inoltre, verrebbe emendato anche la *Section 179* del *Crimes Act*, innalzando a tre anni la pena massima per l'istigazione al suicidio.

Il 24 febbraio 2014 si sono chiuse le consultazioni pubbliche sulla proposta di legge ed essa è in attesa di essere ridiscussa in parlamento nelle prossime settimane, ma è già stata accolta con favore dalla popolazione e dalle istituzioni neozelandesi.

Per quanto riguarda il Canada, esso si compone di tre territori e dieci province che danno vita ad una struttura federale in cui non solo vi è una Costituzione[135] condivisa, ma questa è anche integrata da una Carta dei diritti e delle libertà[136] che

[134] Chapter 6: The education sector, in *Harmful digital communications: the adequacy of the current sanctions and remedies*, Ministerial Briefing Paper, Law Commission, Wellington, New Zealand, August 2012, in www.lawcom.govt.nz.

[135] Constitution Act, 1867.

[136] Constitution Act, 1982.

rende il paese uno dei più sviluppati al mondo dal punto di vista della tutela offerta ai suoi cittadini.

Con riferimento al fenomeno del cyberbullismo, a livello statale vi sono stati notevoli progressi negli ultimi due anni a causa di numerosi episodi di cronaca che, comunque, hanno consentito di implementare la legislazione per una maggior tutela delle vittime.

In Nuova Scozia, ad esempio, nell'agosto 2013 è stato promulgato il *Cyber-Safety Act*, «*An Act to Address and Prevent Cyberbullying*»[137] a seguito del tentato suicidio di Rehtaeh Parsons, una diciassettenne di Dartmouth. La ragazza, a seguito delle gravi lesioni riportate, è caduta in coma irreversibile finché il 7 aprile i genitori non hanno deciso di staccare le macchine che le consentivano di rimanere in vita.

L'insano gesto è stato attribuito alla distribuzione online di foto di un presunto stupro di gruppo avvenuto 17 mesi prima del suo suicidio, nel novembre 2011. Infatti, i quattro ragazzi che l'avevano violentata avevano diffuso le immagini che, nel giro di soli tre giorni, avrebbero comportato la ricezione da parte della vittima di numerosi messaggi su Facebook di persone che chiedevano di avere rapporti sessuali con lei.

Un anno dopo il presunto stupro, la *Royal Canadian Mounted Police* ha chiuso le indagini dichiarando l'impossibilità di formulare delle accuse a causa dell'assenza di prove, nonostante le foto ritraessero una minorenne. Tuttavia, dopo il tentato suicidio, la RCMP ha annunciato un riesame del caso e la sua riapertura provocando la reazione della madre della vittima che ha accusato il sistema giudiziario canadese di essere inadeguato rispetto al problema del bullismo e delle molestie via web.

L'indignazione internazionale e quella del mondo di internet hanno condotto all'adozione del *Cyber-Safety Act* dell'agosto 2013, che definisce "cyberbullismo" qualsiasi comunicazione elettronica mediante l'utilizzo di tecnologie tra cui computer, altri dispositivi elettronici, social network, messaggi di testo, *instant messaging*, siti web e di posta elettronica, con atti di solito ripetuti o con effetto permanente, destinati a provocare o che causano ragionevolmente paura, intimidazione, umiliazione, angoscia o altri danni anche alla salute di una persona, al

[137] Government Bill no. 61 , 5th Session, 61st General Assembly, Nova Scotia, 62 Elizabeth II, 2013, *Cyber-safety Act*, by The Honourable Marilyn More - Minister responsible for the Advisory Council on the Status of Women, in nslegislature.ca.

suo benessere emotivo, alla sua autostima o alla sua reputazione e comprende sia l'aiuto che l'incoraggiamento di questo tipo di comunicazione[138].

La nuova legge consente alle vittime, adulte o minorenni, di chiedere un ordine di protezione il quale nei casi di anonimato comporta anche l'identificazione del colpevole, mentre in quelli più gravi può portare al sequestro del telefono o del dispositivo elettronico utilizzato dal cyberbullo.

La possibilità di citare in giudizio l'autore del reato o i suoi genitori - nel caso si tratti di un minore - implica che, per l'infrazione di quanto previsto dall'ordine di protezione, possa essere comminata una pena dai sei mesi ai due anni di reclusione e/o una multa di massimo cinquemila dollari.

Dal momento che l'aiuto e l'incoraggiamento sono considerati reati al pari di chi dà avvio alle attività di cyberbullismo, anche le persone che diffondono materiale dannoso possono essere citate in giudizio.

Comunque, una delle maggiori novità del *Cyber-Safety Act* è la creazione della *CyberScan Unit*, la prima del suo genere in tutti il Canada, attiva dal settembre 2013 e diretta dall'ex agente di polizia Roger Merrick, il quale si occupa di coordinare cinque investigatori che hanno il compito di rispondere a tutte le denunce di bullismo elettronico. Chiunque (ragazzi, genitori, insegnanti ecc…) potrà presentare un reclamo alla squadra che, situata all'interno del Dipartimento di Giustizia, farà in modo di negoziare risoluzioni formali o informali e, se necessario, potrà adire il giudice e richiedere un ordine di prevenzione. Si tratta di un provvedimento simile a quello di protezione, ma quest'ultimo è demandabile direttamente al tribunale dalla vittima o dai suoi familiari se si tratta di un minore - nel qual caso può essere richiesto anche da un poliziotto.

Il *Cyber-Safety Act*, inoltre, ha introdotto degli emendamenti all'*Education Act* per riflettere la necessità di cooperazione con gli investigatori da parte delle scuole, che si pongono come uno dei cardini nella risposta agli episodi di bullismo elettronico che si verificano dentro e fuori dai corridoi. Infatti, le nuove disposizioni precisano

[138] «"cyberbullying" means any electronic communication through the use of technology including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, typically repeated or with continuing effect, that is intended or ought reasonably be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation, and includes assisting or encouraging such communication in any way», *Cyber-safety Act*, par. 3 b).

che il direttore dell'istituto può prendere i provvedimenti necessari, come specificato nella *Provincial school code of conduct policy*, tra cui la sospensione dello studente per un periodo non superiore a cinque giorni di scuola nei casi di comportamenti gravemente distruttivi tenuti sia all'interno della scuola che al di fuori di essa se essi hanno conseguenze sull'attività di apprendimento e sul clima scolastico[139].

Martedì 11 febbraio 2014, il *Cyber-Safety Act* è stato testato per la prima volta su un adulto, quando un giudice ha emesso un ordine di prevenzione bullismo nei confronti di un uomo, Christopher George Prosper, che ha postato su Facebook commenti osceni sul capo della *Pictou Landing First Nation*, Andrea Paul, e sulla sua famiglia.

La donna si è rivolta alla *CyberScan Unit* che ha contattato il colpevole intimandogli di rimuovere i messaggi illeciti e di astenersi dal proseguire nelle pubblicazioni. Tuttavia, dopo sole due settimane, l'uomo ha ripreso la sua attività, spingendo il direttore della squadra ad appellarsi alla Corte Suprema per ottenere un ordine di prevenzione che è stato concesso per la durata di un anno, imponendo a Prosper di rimuovere tutti i messaggi incriminati, di astenersi dal contatto con Paul e di cessare qualsiasi attività di cyberbullismo, richiedendo anche 750 dollari di risarcimento per le spese processuali.

Pur non trattandosi di un caso che coinvolge minori, la vicenda ha confermato la validità della nuova legge che si rivela utile nel depotenziare le minacce del web con riferimento alle prepotenze e alle persecuzioni diffamatorie o minacciose.

Nonostante la Nuova Scozia sia l'unico dei territori canadesi ad avere una legge specifica per il cyberbullismo, nel resto del paese, a livello statale, sono state introdotte modifiche ai diversi statuti in modo da contemplare il fenomeno a livello legale. In Ontario, per esempio, *l'Education Act*[140] include nella definizione di "bullismo" anche il bullismo per via elettronica, che si realizza con la creazione di una pagina web o un blog in cui l'autore si prende gioco di un'altra persona, con l'impersonificazione della vittima che viene spacciata per l'autore di contenuti o di messaggi postati su internet o con la comunicazione elettronica di materiale a più di un individuo con l'intento di denigrare un soggetto determinato[141].

[139] Chapter 1, Subsection 64, Section 121-122, Education Act.

[140] Education Act, R.S.O. 1990, CHAPTER E.2.

[141] Section One, Education Act, R.S.O. 1990, CHAPTER E.2.

Questa sezione è stata introdotta grazie agli emendamenti previsti dal *Bill 14*[142] del 2011 «*An Act to designate Bullying Awareness and Prevention Week in Schools and to provide for bullying prevention curricula, policies and administrative accountability in schools*».

Come già visto nelle altre nazioni analizzate, anche in Ontario la legge richiede alle scuole di fornire agli studenti degli strumenti di prevenzione del bullismo, programmi di recupero volti ad assistere le vittime e corsi di sviluppo professionale, progettati per insegnare ai docenti in che modo affrontare il fenomeno.

Anche il Québec, con il *Bill 56: An Act to prevent and stop bullying and violence in schools*, ha modificato l'*Education Act* e *l'Act Respecting Private Education*, definendo "bullismo" qualsiasi comportamento diretto o indiretto, commento, atto o gesto, anche attraverso l'uso dei social media, destinato a danneggiare, ferire, opprimere, intimidire o ostracizzare e comprendente anche il cyberbullismo[143].

Il disegno di legge pone l'obbligo di creare un ambiente di apprendimento sano e sicuro per gli studenti e per il personale scolastico, imponendo agli istituti di collaborare a tale scopo tramite l'adozione di un piano anti-bullismo e anti-violenza per prevenire e affrontare il fenomeno, sia esso rivolto ad un alunno che ad un insegnante.

Il *plan* deve, poi, essere aggiornato annualmente e distribuito a tutti i genitori, includendo anche le spiegazioni delle procedure per la segnalazione di episodi relativi ad un atto di bullismo, ma anche e soprattutto per quelle relative alle prepotenze che avvengono tramite l'uso dei social media (cyberbullismo)[144].

Nello stato di Alberta, l'*Education Act* è stato rivisto nel 2012 per definire il bullismo come comportamento ripetuto e ostile o umiliante, tenuto da un individuo nella comunità scolastica in cui l'atteggiamento è destinato a provocare paura, angoscia o danni psicologici/alla reputazione di uno o più individui. La legge si rivolge anche ai

[142] Bill 14, Anti-Bullying Act, 2012.

[143] «[…] the word "bullying" means any direct or indirect behaviour, comment, act or gesture, including through the use of social media, intended to injure, hurt, oppress, intimidate or ostracize, and includes cyberbullying», *Bill 56: An Act to prevent and stop bullying and violence in schools*, 2012, in www.assnat.qc.ca.

[144] «[…] procedures for reporting, or registering a complaint concerning, an act of bullying or violence and, more particularly, procedures for reporting the use of social media for cyberbullying purposes», *Bill 56: An Act to prevent and stop bullying and violence in schools*, 2012, in www.assnat.qc.ca.

fatti commessi per via elettronica e a quelli che non si verificano all'interno dell'edificio scolastico, ma le sue disposizioni sono di notevole importanza soprattutto perché, nella sezione relativa alle responsabilità degli studenti, richiedono di segnalare gli episodi di cyberbullismo e di non tollerare il fenomeno neanche se le prepotenze sono indirizzate a qualcun altro[145].

Allo stesso modo, nel New Brunswick, la *Section 1* dell'*Education Act* comprende nella definizione di bullismo sia quello effettuato online che quello praticato offline, tant'è che esso garantisce agli studenti un ambiente di apprendimento libero da molestie, cyberbullismo e altre forme di disturbo[146], così come dovrebbe avvenire nello stato di Manitoba, qualora venisse approvata la proposta di legge del 2012 (*Bill 18 - The Public Schools Amendment Act*) che introdurrebbe l'abuso tramite comunicazioni elettroniche tra le forme di bullismo sinora previste.

In sostanza, dunque, fatta eccezione per la Nuova Scozia, in Canada non vi sono specifiche leggi territoriali che tutelano le vittime di cyberbullismo, bensì si predilige un approccio educativo, in cui le istituzioni scolastiche giocano un ruolo fondamentale nella prevenzione e nella repressione del fenomeno.

Passando al livello federale, la *Section 2* della Canadian *Charter of Rights and Freedoms* garantisce la libertà di espressione, ma questo diritto è sottoposto a limiti ragionevoli e democratici previsti dalla legge che, nel caso del cyberbullismo riguarderebbero la tutela della *Section 7*, relativa al diritto alla vita, alla libertà e alla sicurezza della persona. Tuttavia, nella maggioranza dei casi, queste due disposizioni non sono state accettate come presupposto per la difesa nei casi civili o penali di bullismo elettronico.

Comunque, non sono escluse ulteriori forme di protezione, alle quali si può ricorrere grazie alle leggi federali, che riguardano sia l'ambito civile che quello penale.

Nell'ambito del *Criminal Code* canadese, infatti, esistono due approcci al fenomeno. Il primo è relativo alle molestie, disciplinate dalla *Section 264* del codice, in cui si configura come crimine quello di porre in essere comportamenti minacciosi per un individuo, inducendolo a temere per la propria sicurezza o per quella della sua

[145] Chapter E-0.3, Division 1 – Responsibilities, *Student responsibilities*, Education Act, Statutes of Alberta, 2012 in www.qp.alberta.ca.

[146] Chapter E-1.12, Education Act - Loi sur l'éducation, Assented to February 28, 1997, in www.gnb.ca.

famiglia, punibili con un massimo di 10 anni di carcere. Nonostante queste disposizioni valgano soprattutto per lo *stalking*, dove la frequenza causa la paura (più che il contenuto), esse si applicano ai cyberbulli in quanto è considerata molestia anche la comunicazione ripetuta, sia direttamente che indirettamente, con la vittima o chiunque la conosca.

Sul sito della polizia di Montréal[147], infatti, il *Criminal Harassment* viene esemplificato nel caso in cui un ragazzo usi internet per comunicare reiteratamente con qualcuno, sapendo che il destinatario si sente minacciato. Infatti, la *Section 264* precisa che, anche se l'autore non aveva intenzione di spaventare la vittima, egli può essere accusato di molestie se quest'ultima si sente intimidita.

Per di più, la *Section 264.1* si rivolge specificamente alla pronuncia di minacce che causano la morte o i danni fisici di una persona, il che, unitamente alla *Section 241* relativa all'istigazione al suicidio (*Counseling suicide*), si rivela particolarmente utile nella valutazione dei casi in cui la vittima si toglie la vita o a quelli di intimidazioni persistenti (*Section 246*).

Il secondo approccio del *Criminal Code*, invece, riguarda la diffamazione, protetta dalla *Section 301*, che prevede fino ad un massimo di due anni di carcere per la pubblicazione di calunnie e può riferirsi al bullismo elettronico nel caso in cui, ad esempio, internet venga utilizzato per ridicolizzare la vittima sia attraverso le affermazioni che mediante la pubblicazione di immagini.

Inoltre, sempre all'interno del *Criminal Code*, sono previsti altri reati come, tra gli altri, l'estorsione (*Section 346*), che può verificarsi quando il cyberbullo insidia continuamente un compagno di scuola affinché egli porti un oggetto di valore in classe per sottrarglielo o lo costringa a fornirgli password di accesso aggredendolo per iscritto o accusandolo pubblicamente.

E' da considerarsi reato anche l'invio di messaggi falsi (*Section 372*) con l'intento di ferire o di danneggiare la vittima, pur sapendo che le informazioni trasmesse non sono vere. Così, mentre nel secondo caso sono previsti un massimo di due anni di carcere, nella prima fattispecie il periodo di detenzione non può essere inferiore ai quattro anni.

[147] www.spvm.qc.ca.

Con riferimento ai crimini più strettamente informatici, la *Section 430* punisce chiunque commette distrugge o altera i dati volontariamente o ne fa un uso illecito, compreso quello di negarvi l'accesso a colui che ne avrebbe diritto (es: furto di password), mentre le *Section 432* e *403* si riferiscono, rispettivamente, all'uso non autorizzato del computer e all'*Identity fraud*.

Per quanto riguarda l'ambito civile, invece, il cyberbullo può essere ripreso in quanto le sue azioni possono far percepire alla vittima di trovarsi in un ambiente pericoloso, dal momento che le prepotenze online si trasformano spesso in prese in giro o esclusione nelle classi. In questi casi, quindi, le scuole sono tenute ad adottare ogni azione necessaria affinché il comportamento scorretto cessi, compresa quella di punire uno studente nonostante ciò che egli fa avvenga fuori dall'istituto e via web[148].

Anche questa volta, dunque, emerge il legame tra il profilo educativo e quello normativo, che vanno di pari passo nella repressione del fenomeno.

Più recentemente, a seguito del suicidio di Amanda Todd nell'ottobre del 2012 (vedi pag. 185) è emersa una nuova forma di bullismo che attualmente non è coperta dal diritto penale canadese. Si tratta di quei casi in cui vengono caricati materiali intimi o sessuali senza il consenso della persona ritratta nella foto o ripresa nel video.

Qualunque sia la motivazione del bullo, l'impatto di questo tipo di cyberbullismo può essere devastante per l'autostima, la reputazione e la salute mentale del giovane, tanto da spingerlo a togliersi la vita, come nel caso di Rehtaeh Parsons.

Per rispondere a questa lacuna del *Criminal Code*, il Canada ha introdotto una proposta di legge che, tra le altre cose, dovrebbe creare un nuovo reato, consistente nella distribuzione non consensuale delle immagini intime e punito con una pena massima di cinque anni di reclusione.

Nel novembre del 2013, infatti, il Parlamento ha iniziato le discussioni sul *Bill C-13*, intitolato proprio "*The Protecting Canadians from Online Crime Act*" e adottato a seguito del *report* federale-provinciale-territoriale "*Cyberbullying and the Non-consensual Distribution of Intimate Images*" del giugno 2013.

Quest'ultimo sottolinea come il bullismo elettronico stia generando una crescente preoccupazione nei genitori, nella polizia, nei docenti e nei cittadini in genere, a

[148] Legislation respecting Education, Constitution Act, 1867.

causa del suo incremento e del fatto che spesso si è posto come fattore dominante in una serie di suicidi compiuti dagli adolescenti.

Il gruppo di lavoro, a tal proposito, raccomanda un'azione multilivello, che coinvolga sia il governo federale che i singoli stati, ma anche tutti gli *stakeholdes* interessati, così da intraprendere iniziative che aiutino ad affrontare il fenomeno.

Il *report*, inoltre, sottolinea la necessità di emendare il *Criminal Code*, cosicché esso possa rispondere in modo più efficace al cyberbullismo.

Innanzitutto, infatti, si raccomanda che i tre reati contenuti nella *Section 372* (messaggi falsi, telefonate indecenti, telefonate moleste) vengano modernizzati così da rendere chiaro che questi reati possono essere commessi attraverso l'uso di comunicazioni elettroniche e che queste hanno una portata ben più ampia di quella tradizionale *one-to-one*.

In secondo luogo, il gruppo di lavoro sottolinea che, dal momento che il cyberbullismo si verifica nel cyberspazio e la prove elettroniche necessarie per comminare la pena devono essere ottenute dai providers e dai fornitori di servizi di social media, la capacità di conservare e ottenere tali elementi probatori è cruciale per ogni indagine.

Attualmente i poteri della polizia canadese non sono sufficienti per affrontare le problematiche degli illeciti informatici, soprattutto considerando che il fenomeno sta assumendo varie forme, compreso l'uso di e-mail, *instant messaging* e post molesti e minacciosi immessi su piattaforme di social networking. Sono frequenti anche i casi di creazione di siti web che deridono e tormentano la vittima o quelli di avvio di sondaggi offensivi su di essa, ma, soprattutto, sempre più comune è la pubblicazione online o la distribuzione elettronica di foto o video imbarazzanti che mostrano una persona impegnata in attività sessuali esplicite o i suoi organi sessuali in una situazione in cui la persona avrebbe una ragionevole aspettativa di privacy.

Pertanto, una modifica del *Criminal Code* potrebbe consentire alle forze dell'ordine di inviare al giudice la richiesta di autorizzazione (*production orders*) per intercettare le comunicazioni private consentirebbe di salvare le prove che spesso i providers rimuovono automaticamente dopo un determinato lasso di tempo. L'emissione da parte della Corte di questo permesso garantirebbe il controllo dell'attività svolta per

le indagini e si potrebbe applicare sia ai casi di cyberbullismo nei casi previsti dalla *Section 372*, che in quelli di distribuzione non consensuale di immagini intime.

Alla luce di quanto rilevato nel *report*, il *Bill C-13* fornirebbe alle forze dell'ordine i mezzi necessari per combattere il crimine in un ambiente virtuale, in modo che esse siano autorizzate a condurre indagini appropriate, pur mantenendo i controlli giudiziari e gli equilibri necessari per proteggere la privacy dei cittadini.

La proposta di legge, infatti, mantiene il requisito di un'appropriata supervisione giudiziaria nei casi in cui sia necessario l'accesso ai dati degli utenti, per il quale è necessaria un'autorizzazione del giudice. Tuttavia, introduce per i reati commessi via internet la possibilità di avere accesso ai dati e di conservarli, così da acquisire prove elettroniche che consentano una maggiore tutela delle vittime, soprattutto laddove il colpevole si nasconde dietro l'anonimato del web.

Il *Bill C-13*, comunque, non deve essere confuso con l'aggiunta di nuovi poteri "sorveglianza", poiché l'obiettivo non è monitorare i cittadini né intercettare arbitrariamente le loro comunicazioni, come è stato sottolineato più volte da coloro che ne criticano le innovazioni. Lo scopo, infatti, oltre ad arginare il fenomeno del cyberbullismo, è quello di aggiornare competenze già esistenti nel *Criminal Code*, come quelle già previste per i dati finanziari (ad esempio numeri di conto), trasferendo anche ai crimini del web la possibilità di ottenere *production orders* finalizzati alla trasmissione e alla conservazione di elementi rilevanti per la risoluzione del caso. Inoltre, a tutela dei cittadini, il disegno di legge impone il soddisfacimento di elevati requisiti legali prima che un giudice possa emettere un mandato per rintracciare e monitorare gli utenti.

Ciò che cambia, quindi, non sono i poteri in sé, piuttosto le previsioni introdotte dalla *Section 487.0195*, che emenda la *487.0194*, stabilendo la non necessità di richiedere *production orders* al giudice qualora terzi decidano volontariamente di assistere le autorità nelle indagini, fornendo essi stessi i dati necessari alla risoluzione del caso, a meno che non vi sia un esplicito ordine della corte affinché la collaborazione cessi.

Dunque, il *Bill C-13* dovrebbe integrare le esigenze di conservazione dei dati da parte della polizia con la possibilità dei cittadini di mantenerli volontariamente e

renderli disponibili senza incorrere in alcuna responsabilità penale o civile, attivando una cooperazione tra settore pubblico e privato[149].

Questa legislazione è molto specifica nel suo intento, che si realizza nel contribuire a scoraggiare la distribuzione delle informazioni e delle immagini online, equivalenti alle molestie, alle intimidazioni e alle calunnie già esistenti nel codice penale per le interazioni offline.

Per quanto riguarda il resto delle previsioni della proposta di legge, essa andrebbe anche a vietare la distribuzione non consensuale delle immagini intime che non viene tutelata appieno dalle *Section 162* e *163*, le quali si occupano solo di voyeurismo e pubblicazioni oscene. Il cd. *sexting*, infatti, è ormai una pratica molto diffusa tra i cyberbulli, che postano in rete foto e video dei loro coetanei nudi o impegnati in attività sessuali, ma esso è parte di una più ampia pratica che comporta la derisione della vittima anche al di là degli elementi visivi pubblicati. Ovviamente, il fatto che il *Bill C-13* consenta al giudice di ordinare la rimozione di questi materiali da internet, impedirne la pubblicazione al colpevole e persino imporre il rimborso alle vittime per le spese sostenute nel rimuovere i contenuti, è una grande forma di protezione. Tuttavia, questa previsione è volta alla tutela soltanto di una parte del reato, che, invece, più spesso si configura come diffamazione e persecuzione, sia diretta che indiretta.

Dunque, se si volesse osservare il futuro cui va in contro la legge federale canadese, è necessario sottolineare che per quanto sia utile e proficuo arginare il fenomeno con nuove previsioni normative, è abbastanza chiaro che esse non esaurirebbero affatto l'universo delle fattispecie possibili, nonostante gli emendamenti alla *Section 372* e gli strumenti a disposizione delle autorità pubbliche.

Inoltre, rimarrebbe incerto anche il ruolo giocato dagli Internet Service Providers, nella misura in cui la proposta di legge non specifica se essi debbano essere o meno ritenuti responsabili per i contenuti immessi dagli utenti. Il Canada, come l'Italia e l'Europa in genere, stabilisce il loro coinvolgimento negli illeciti valutando se l'ISP

[149] «487.0195: (1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing. (2) A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so», Bill C-13, Second Session, Forty-first Parliament, 62 Elizabeth II, 2013 in www.parl.gc.ca.

fosse o meno a conoscenza del fatto e se, successivamente alle segnalazioni abbia rimosso il contenuto diffamatorio. Pertanto, non vi è un obbligo generale di sorveglianza e il mancato controllo non costituisce negligenza visto l'enorme volume del traffico in rete. Tuttavia, il provider si trova a dover decidere se agire o non agire nei casi in cui vi è un reclamo poiché a quel punto si attiva una "presunta conoscenza" dell'illecito, che potrebbe essere punita qualora l'ISP non abbia valutato correttamente la questione e l'abbia lasciata irrisolta - a meno che, poi, non rimuova il contenuto entro un ragionevole lasso di tempo[150].

Un esempio della necessità di estendere le normative anche alle forme di collaborazione dei providers si trova nel caso dell'(ex) adolescente David Knight, bersagliato sulla rete da alcuni coetanei. La sua persecuzione, infatti, culminò nella creazione di una pagina web su Yahoo! intitolata "*Welcome to the page that makes fun of Dave Knight*", sulla quale i cyberbulli si prendevano gioco di lui e della sua famiglia, lo accusavano di adescare e intrattenere attività sessuali con altri minorenni più giovani di lui utilizzando la droga dello stupro e incitavano gli altri utenti a prendere parte all'attività diffamatoria.

Il problema, però, non fu che il sito era stato attivo per diversi mesi prima che un compagno di classe riferisse a Knight della sua esistenza, poiché, appunto, i providers non possono effettuare controlli su tutto il materiale che veicolano. Il fatto sconcertante fu che, quando la madre della vittima chiese a Yahoo! di chiudere la pagina, il provider si rifiutò finché, sette mesi dopo, la donna non agì per vie legali, il che spinse il prestatore di servizi ad oscurare il sito.

Dunque, nuovamente, emerge l'esigenza di dar vita a disposizioni normative che coordino le attività degli investigatori, dei giudici e degli ISPs, poiché non è affatto sufficiente introdurre misure unilaterali per arginare il fenomeno, tantomeno basare la gran parte delle previsioni sulla diffusione di immagini intime, che, pur essendo parte del problema, non impediscono ai cyberbulli di trovare altre modalità per diffamare le loro vittime. A tal proposito, quindi, si pone anche l'esigenza di individuare con una disposizione normativa una definizione univoca del fenomeno, che ricomprenda tutte le fattispecie in cui esso di può configurare e che si possa

[150] Copyright Act, R.S.C., 1985, c. C-42, in laws-lois.justice.gc.ca.

applicare a livello federale così da garantire le stesse forme di tutela in ciascuno stato.

Tuttavia, le leggi non bastano per tutelare i giovani.

Infatti, in un recente studio del *Senate Committee on Human Rights*, intitolato "*Cyberbullying Hurts: Respect for Rights in the Digital Age*"[151], sono stati ascoltati decine di canadesi di tutte le età ed è emerso che, pur scoraggiati dalle disposizioni normative, i giovani vedono le conseguenze giuridiche come una possibilità remota e temono molto di più i provvedimenti disciplinari presi all'interno delle scuole nonché le reazioni delle famiglie.

Pertanto, il Canada dovrebbe integrare le eventuali leggi penali (o quelle già esistenti) con dei rimedi relativi alla prevenzione, migliorando i programmi di istruzione e coordinando tutti gli *stakeholders* della società, sia a livello pubblico che privato.

Il Comitato, infatti, raccomanda al governo federale di lavorare con le province e i territori per stabilire una strategia armonizzata per affrontare il cyberbullismo, che rispetti la convenzione dell'ONU sui Diritti del Fanciullo e che comprenda un piano per promuovere la consapevolezza dei ragazzi e dei genitori rispetto al fenomeno.

L'educazione, dunque, è fondamentale poiché attraverso essa i più giovani possono diventare buoni cittadini digitali e fare scelte informate e responsabili quando usano i mezzi di comunicazione elettronica, tant'è che lo stesso *Committee* sottolinea che l'insegnamento dei diritti umani e digitali è una componente fondamentale di qualsiasi strategia coordinata. Esso, inoltre, ha proposto l'adozione di programmi di giustizia ripartiva che possano consentire di mediare tra la vittima e il cyberbullo per una risoluzione civile delle controversie, parallelamente alla cooperazione con l'industria di internet, il cui supporto è indispensabile nell'assicurare una rete più sicura per i ragazzi.

Sulla scia di quanto recentemente previsto dal *Cyber-Safety Act* in Nuova Scozia, il rapporto del Senato ha raccomandato al governo federale di iniziare un percorso insieme ai diversi territori e alle province, così da poter creare una *task-force* (simile alla *CyberScan Unit*), il cui mandato sarebbe quello di monitorare in modo uniforme il fenomeno a livello nazionale.

[151] Dicembre 2012, in www.parl.gc.ca.

In sostanza, una strategia coordinata dovrebbe includere un piano per la promozione della consapevolezza sul cyberbullismo in tutto il Canada, stabilendo programmi di supporto e di istruzione per i bambini e i loro genitori, nonché per gli insegnanti e il personale scolastico. Inoltre, per assicurare che suddette risorse siano disponibili in ogni regione del paese bisognerebbe adottare una legge che si occupi di dare una definizione universale dei comportamenti caratterizzano il fenomeno, così da poter applicare le conseguenze, sia civili che penali, in modo uniforme su tutto il territorio.Ciò che emerge, così come valutato già nell'analisi degli altri paesi selezionati, è che non vi è una soluzione rapida al bullismo elettronico, tantomeno si può garantire *in toto* che esso non danneggi i più giovani. Tuttavia, i genitori, gli insegnanti, le forze dell'ordine, i politici e i providers hanno tutti un ruolo chiave nel rendere la prevenzione efficace, che consiste nell'assumersi una maggiore responsabilità collettiva prima ancora di agire per reprimere gli abusi.

Approfondimento 2:

La Repubblica di Singapore: un caso virtuoso dall'Oriente

Molto spesso, nel fare riferimento alle disposizioni legislative più all'avanguardia, si presta attenzione a ciò che avviene nelle nazioni più vicine all'Europa culturalmente e geograficamente, senza badare a quanto avviene in altri paesi che, seppur lontani, avrebbero da impartire molte lezioni.

E' il caso, ad esempio, di quanto recentemente avvenuto in Malesia, nella Repubblica di Singapore, uno dei primi paesi ad offrire una tutela giuridica contro il cyberbullismo.

Infatti, nel marzo 2014, con la presentazione in Parlamento e l'approvazione del *Protection from Harassment Bill*, gli utenti web hanno un nuovo strumento di difesa specificamente diretto agli abusi online contenente rimedi civili e sanzioni penali.

Il *Factsheet on the protection from Harassment Act 2014*[152], pubblicato dal Ministro della Legge il 1 marzo, stabilisce che le *Sections* dalla 13A alla 13D del *Miscellaneous Offences (Public Order and Nuisance) Act* (Cap. 184), pur criminalizzando le molestie e le minacce/provocazioni di violenza, non erano direttamente applicabili al web. Quindi, la nuova legge è stata adottata poiché applica esplicitamente alla rete gli stessi standard di ciò che costituisce suddetti reati nel mondo reale, aggiungendo che anche gli atti di molestie commessi al di fuori di Singapore saranno un reato, laddove vi sia un nesso sufficiente con la vittima allocata all'interno della Repubblica. Inoltre, essa prevede che le sanzioni per suddetti crimini via web vengano aumentate per riflettere la gravità del comportamento e saranno applicate delle aggravanti per i recidivi.

Il *Factsheet* precisa, poi, che quanto previsto dal nuovo *Harrasment Act* include situazioni di *sexual-harassment*, cyberbullismo e bullismo tra ragazzi, rendendo anche lo *stalking* un crimine. Così, in tutte queste situazioni, a parte i danni per cui la vittima può citare in giudizio i colpevoli, essa può anche richiedere ai tribunali di applicare *protection order* contro il molestatore, affinché ad esso sia imposto di desistere dal perpetrare l'abuso. Inoltre, se quest'ultimo consiste nella pubblicazione

[152] www.mlaw.gov.sg.

di materiale offensivo per la vittima, la Corte può persino imporre al colpevole o all'amministratore del sito di rimuovere il materiale incriminato. Per di più, qualora le circostanze richiedano un intervento urgente, il giudice potrà concedere un *expedited protection order*, cioè un ordine di protezione accelerato.

Se, invece, è stata pubblicata una *false statements of fact* (falsa dichiarazione) su una persona, la Corte può imporre che venga pubblicata una notifica che avvisi i lettori della falsità delle affermazioni e che riporti la realtà dei fatti.

Per evitare fraintendimenti e dimostrare che queste disposizioni si applicano a tutti i reati previsti, la legge fornisce esempi espliciti di molestie, che riguardano sia lo *stalking* che il cyberbullismo. In quest'ultimo caso, la fattispecie presa in esame prevede che:

- se X e Y sono compagni di classe;
- X posta uno scritto volgare Y su un sito web accessibile a tutti i loro compagni di classe;
- uno dei compagni di classe di Y gli mostra il messaggio;
- Y è in difficoltà;
- allora X è colpevole di un reato.

Dal punto di vista penale, il colpevole degli illeciti previsti verrà multato fino a S$[153]5.000 o recluso fino a 12 mesi. L'aggravante per i recidivi prevede l'innalzamento della somma ad un massimo di S$10.000 e della pena detentiva fino a due anni.

Il Membro del Parlamento Hri Kumar ha più volte dichiarato che la legge ha l'obiettivo di rendere le persone responsabili dei crimini che commettono online, ma ha anche espresso la sua preoccupazione per l'effettiva attuazione delle nuove previsioni, a causa di orientamenti poco chiari per quanto riguarda i trasgressori anonimi. I suoi colleghi Pritam Singh e Zaqy Mohammad, hanno invece posto l'accento sul fatto che il nuovo *Harrasment Act* non dovrebbe essere utilizzato per inibire la libertà di parola di personaggi pubblici come i blogger o i giornalisti. Essa, infatti, secondo quanto affermato da Mohammad, dovrebbe essere utilizzata soltanto per porre fine alle attività di *stalker* e cyberbulli, non per imbavagliare le critiche politiche o sociali.

[153] Dollaro di Singapore.

Singh, inoltre, ha ricordato al governo che la questione del bullismo è un problema complesso, che non può essere adeguatamente risolto solo attraverso la legislazione.
Come si è più volte ripetuto all'interno di questo lavoro, infatti, si tratta di un fenomeno da risolvere non soltanto a livello giuridico, ma anche dal punto di vista educativo, nelle scuole e all'interno delle famiglie.
Comunque, il caso della Repubblica di Singapore resta senz'altro un esempio virtuoso di intervento legislativo, che sta alimentando il dibattito sulla questione del cyberbullismo in moltissimi paesi.

Capitolo 3

I social network e loro *policies*

Nel rapporto redatto da Ipsos Public Affairs per Save the Children Italia Onlus, intitolato *Safer Internet Day Study – Il Cyberbullismo*[154], il 69% dei ragazzi intervistati ha indicato il bullismo elettronico come il fenomeno sociale più pericoloso.

Tuttavia, il dato più significativo è emerso quando è stato posto il quesito relativo a quali forme assume la persecuzione della vittima da parte del cyberbullo:

Dall'immagine riportata[155] appare chiaro, quindi, come i social network costituiscano al tempo stesso uno strumento di relazione e una minaccia diretta per i giovani che ne fanno uso, ma anche per quelli che vengono perseguitati sul web indirettamente (pagine o gruppi creati appositamente, siti web, blog etc…).

Dal momento che, come si è visto, non vi sono norme a livello sovrannazionale né statale - salvo eccezioni come la Nuova Scozia e qualche stato americano - che tutelino i giovani rispetto al cyberbullismo, è essenziale comprendere quali siano gli

[154] 458 interviste, a ragazzi di età compresa tra i 12 e i 17 anni, condotte tramite metodo CAWI.

[155] Ipsos Public Affairs per Save the Children Italia Onlus, *Safer Internet Day Study – Il Cyberbullismo.*

strumenti messi a disposizione dalle piattaforme di social networking per prevenire, arginare e reprimere il fenomeno.

L'Unione Europea, ad esempio, come risultato dell'attività della *Social Networking Task-Force* creata nel 2008, ha dato vita ai cd. *Safer Social Networking Principles*, un accordo di autoregolamentazione firmato dai maggiori fornitori di servizi social in Europa, i quali si sono impegnati ad attuare misure per garantire la sicurezza dei minori sulle loro piattaforme.

Innanzitutto, infatti, si prevede che essi creino del materiale chiaro e semplice appositamente per i giovani, in modo da fornire loro le conoscenze e le competenze per navigare attraverso i social in modo sicuro.

Inoltre, i *Terms of Service* devono fornire informazioni chiare su ciò che costituisce un comportamento inappropriato nonché le conseguenze della violazione di questi termini.

Visto che, come più volte ripetuto, il cyberbullismo non è solo una questione da risolvere a livello normativo, i *providers* dovrebbero anche offrire ai genitori e ai docenti degli strumenti che li aiutino ad insegnare ai ragazzi il corretto uso di internet, favorendo il dialogo e il senso di responsabilità.

Il secondo principio, invece, fa riferimento alla necessità di garantire che i servizi forniti siano adatti agli utenti di riferimento, intendendo con ciò che gli ISPs dovrebbero cercare di limitare l'esposizione a contenuti o contatti potenzialmente inappropriati. Ad esempio, essi dovrebbero utilizzare degli avvisi o imponendo un'età minima per la registrazione, richiedendo, in quest'ultimo caso, delle informazioni che consentano di definirla. Inoltre, sarebbe auspicabile l'adozione di meccanismi di *parental control* o di segnalazione di contenuti inappropriati.

A tal proposito, il terzo principio riguarda proprio l'implementazione degli strumenti a disposizione degli utenti relativamente a comportamenti o materiali potenzialmente dannosi. Ad esempio, vi è la possibilità di rendere privato il proprio profilo e di far sì che lo sia in automatico se si tratta di un minore oppure quella di poter bloccare/rifiutare le richieste di amicizia sgradite. Nella relazione si fa anche riferimento alla possibilità di vietare i post sulla propria bacheca o di effettuare un controllo preventivo prima della loro pubblicazione, ma anche alla fornitura di

strumenti di facile utilizzo che consentano di segnalare contatti e contenuti che violano i Termini di Servizio.

Di quest'ultimo caso, infatti, si occupa specificamente il quarto principio, che, oltre a richiedere suddetti mezzi, auspica la presenza delle informazioni necessarie affinché l'utente possa redigere un *report* efficace e in modo che egli conosca le modalità di gestione delle segnalazioni da parte della piattaforma.

Il quinto principio, invece, si riferisce a suddetti processi risolutivi cosicché essi siano messi in atto per visionare e rimuovere rapidamente il contenuto offensivo.

I fornitori di servizi, inoltre, dovrebbero adottare forme di cooperazione con gli organi preposti dalla giurisdizione locale, come le *hotline* o le forze dell'ordine, così da poter rispondere più efficacemente alle minacce per la sicurezza degli utenti.

Gli ultimi due principi, invece, fanno riferimento alla necessità di incoraggiare gli utenti ad un uso sicuro dei dati personali e delle proprie informazioni, per poi passare all'adozione di una serie di procedure che possono essere utilizzate per promuovere il rispetto dei Termini di Servizio. Queste ultime sono estremamente importanti poiché includono le forme automatizzate di moderazione (ad es. filtri), ma anche quelle umane che possono interagire con gli utenti in tempo reale o comunque in un intervallo temporale ragionevole.

Nonostante i *Safer Social Networking Principles* siano stati sottoscritti da 21 diverse compagnie[156], la Commissione Europea, tra dicembre 2010 e gennaio 2011, aveva rilevato che dei 13 social analizzati[157], soltanto due[158] avevano applicato come opzione di default quella di avere un profilo privato se all'atto di registrazione l'utente risultava minorenne. Nel caso di Facebook, poi, la Commissione aveva sottolineato che, sebbene i meccanismi di notifica per i contenuti o comportamenti inappropriati siano facili da usare, il social non rispondeva prontamente alle segnalazioni degli utenti e che, quando un minore accede alla piattaforma, alcune delle inserzioni visualizzate lateralmente nella home contengono pubblicità inadatte.

[156] Arto, Bebo, Facebook, Studenti.it, Hyves, Myspace, Nasza-klaza, Netlog, One, Rate, VZnet, Tuenti, Zap, Dailymotion, Google, Microsoft Europe, Skyrock, Stardoll, Sulake, Yahoo Europe e Wer-kennt-wen.

[157] Arto, Bebo, Facebook, Studenti.it, Hyves, Myspace, Nasza-klaza, Netlog, One, Rate, VZnet, Tuenti e Zap.

[158] Bebo e MySpace.

Insomma, come si può notare, ciascuna piattaforma ha la sua *policy* e, proprio per questo, si è deciso di analizzarle singolarmente per poi dar conto, alla fine, dei casi di cronaca più rilevanti, in modo da inquadrare la concreta applicazione ed utilità delle regole virtuali in rapporto alla legislazione nazionale.
Suddetta analisi, peraltro, muoverà da un resoconto delle forme di tutela messe a disposizione dai social network per altre fattispecie che si ritengono essere estendibili al cyberbullismo, per poi focalizzarsi sulle eventuali disposizioni relative esclusivamente ad esso.

3.1 – I meccanismi di segnalazione a disposizione degli utenti di Facebook

Il fenomeno del bullismo non è nuovo, ha radici profonde ed è una presenza costante nella vita (scolastica e di quartiere) di moltissimi ragazzi, ma esso ha certamente cambiato le sue caratteristiche nel corso degli anni, potendosi avvalere di nuovi strumenti che lo rendono ancora più pervasivo. Oggi, infatti, con l'utilizzo di internet e dei social media, i giovani possono essere vittima di cyberbullismo in ogni luogo e in ogni momento, non solo in modo diretto, ma anche senza sapere che sono state create pagine web appositamente per denigrarli.
Di questo fenomeno, inoltre, ne esistono ben due tipologie. La prima si verifica quando viene pubblicato un video che testimonia l'atto di bullismo, a prescindere che a caricarlo sia proprio il colpevole piuttosto che chiunque altro di sua conoscenza o un utente anonimo. Questo tipo di video, in realtà, non è l'unico, poiché spesso vengono immessi sul web anche quelli relativi ad atti sessuali o particolari intimi di un minore, il che chiama in causa la cd. *revenge porn*, che può consistere anche nell'*upload* di immagini dello stesso tipo, solitamente per vendicarsi di un ex fidanzato (da con confondere con il *sexting* – vedi pag. 10).
La seconda tipologia, invece, ben più diffusa, si articola in due diverse configurazioni, spesso tra loro complementari. Innanzitutto vi è quella della diffamazione, che si può realizzare attraverso post e commenti denigratori sul profilo che la vittima ha su un social network, mantenendo l'anonimato o utilizzando la propria identità. Ciò avviene anche con la creazione di gruppi (segreti e non) o pagine che prendono di mira un ragazzo anche senza che lui ne sia a conoscenza. In

ogni caso, l'attività diffamatoria si serve di affermazioni scritte, di sondaggi e della pubblicazione di foto e di video che in alcuni casi possono essere realizzati di nascosto, mentre in altri la vittima è consapevole dell'esistenza di questo materiale, ma non vorrebbe vederlo pubblicato. Questa categoria differisce in parte da quella evidenziata nella prima tipologia poiché in essa si faceva riferimento specifico alle piattaforme espressamente dedicate all'upload di video (es. YouTube), in cui, se il video è pubblico, milioni di utenti possono avere accesso alle riprese tramite la semplice ricerca di parole chiave. Sulle piattaforme di social networking, invece, essi sono situati all'interno di un profilo, di una pagina o di un gruppo, perciò costituiscono una minima parte di altre attività e non sono immediatamente reperibili.

In secondo luogo, vi è la persecuzione che si realizza in privato, attraverso la chat, gli *in-box* o qualunque tipo di messaggistica istantanea offerta dal social network, che consente al cyberbullo di proseguire le intimidazioni e gli insulti anche sottoforma di comunicazione privata.

Il problema dunque, non è dato soltanto dal riuscire a coinvolgere nelle prepotenze un vastissimo numero di persone (potenzialmente indefinito), ma soprattutto quello della continuità con cui queste vengono compiute. Infatti, grazie ad uno *smartphone* o un qualsiasi dispositivo elettronico connesso ad internet, i ragazzi possono essere online costantemente e la vittima del cyberbullo non ha alcun posto in cui rifugiarsi per allontanarsi dalle molestie. Per di più, anche quando essa chiude l'account o disattiva il profilo, le attività diffamatorie possono continuare senza che sia necessaria la sua presenza come utente del web.

Fatte queste precisazioni, appare chiaro il ruolo di fondamentale importanza ricoperto dalle *policies* dei social network, poiché l'intervento della piattaforma è uno *step* essenziale per arginare gli abusi diretti o indiretti, prima ancora della possibilità di contattare le autorità competenti.

Nel 2011, uno studio del *Pew Research Center's*[159], intitolato *Internet&American Life Project*, ha intervistato 800 ragazzi tra i 12 e i 17 anni, sottolineando che, tra di essi, 9 utenti di Facebook su 10 hanno assistito ad atti di bullismo sul social medium.

[159] www.pewinternet.org.

Due anni dopo, le statistiche di Liam Hackett nel suo *Annual Bullying Survey* del 2013 hanno mostrato che il 54% dei 2000 *teenager* inglesi intervistati sostiene che su Facebook si abbia il doppio delle possibilità di cadere vittima del cyberbullismo.

Insomma, essendo uno dei social network più utilizzati al mondo, la piattaforma creata da Mark Zuckerberg nasconde numerose insidie per coloro che vi si iscrivono. In effetti, guardando le sue *policies* nella prospettiva del contrasto al fenomeno analizzato, emergono sostanziose disposizioni che possono essere utilizzate per reprimere gli abusi tra minori.

Innanzitutto, prendendo atto dei rischi della rete, nella sezione "Normativa sull'utilizzo dei dati" intitolata "Minorenni e sicurezza", Facebook dichiara di trattare «con estrema serietà le questioni relative alla sicurezza, soprattutto per quanto riguarda i bambini, e invita i genitori a insegnare ai propri figli le norme per un utilizzo sicuro di Internet»[160].

Inoltre, i *Terms of Use* prevedono che l'età minima per creare un profilo debba essere di 13 anni, tant'è che quando si tenta di registrarsi come un bambino di età inferiore la sottoscrizione viene negata. Tuttavia, essendo un requisito basato sull'auto-dichiarazione, basta chiudere e riaprire il browser per potersi registrare nuovamente e dichiarare un'età superiore a quella reale.

Una volta creato un profilo, Facebook consente di immettervi informazioni sulla scuola, il lavoro, la data di nascita e su tutta una serie di interessi personali. L'utente, poi, può cercare e aggiungere degli "amici" e pubblicare aggiornamenti di stato, condividere foto, video e link, ma anche essere taggato dai suoi contatti in ciascuno di questi post. E' possibile, inoltre, utilizzare funzioni di *geotagging*, che consentono la registrazione nel luogo in cui si è al momento della connessione (nonostante esso possa essere aggiunto anche in un secondo momento). La quantità di informazioni disponibili e a chi esse siano visibili dipende dalle impostazioni della privacy, per cui, ad esempio, si può decidere che le proprie attività siano visibili solo allo stesso utente oppure ai suoi amici o agli amici degli amici, fino ad arrivare all'opzione "pubblica" o a quella "personalizzata", che consente di escludere alcuni amici dall'accesso ai contenuti pubblicati.

[160] www.facebook.com/about/privacy/minors.

Comunque, oltre a potersi mettere in contatto con altre persone, si può aderire alle pagine o ai gruppi, ma anche crearne di nuovi oppure partecipare agli eventi o realizzare un invito più o meno aperto al pubblico.

In aggiunta alla possibilità di utilizzare il proprio profilo autonomamente grazie alle funzioni del diario, gli utenti possono commentare gli elementi condivisi dagli amici, dalle pagine e nei gruppi, scrivere sulla bacheca di altre persone o interagire *one-to-one* in privato grazie al sistema di chat/*in-box*, che comunque consente anche di inviare messaggi a più destinatari, così come, grazie al *tagging*, un post sulla bacheca di un amico può essere visibile anche su quella delle altre persone menzionate.

Insomma, vi sono tutta una serie di funzioni utilissime che, se utilizzate in maniera errata costituiscono uno degli strumenti più potenti e pervasivi nelle mani dei cyberbulli.

Non a caso, Facebook nei suoi "Standard della comunità", facenti parte delle Condizioni d'uso, dichiara di offrire «alle persone di tutto il mondo la possibilità di pubblicare contenuti personali, vedere il mondo attraverso gli occhi di altre persone, connettersi e condividere contenuti ovunque. Le conversazioni che si svolgono su Facebook e le opinioni qui espresse rispecchiano la diversità degli utenti di Facebook». Tuttavia, «per rispettare le esigenze e gli interessi di utenti di tutto il mondo, Facebook tutela le forme di espressione che rispettano gli standard della comunità […]» che servono a far capire «[…] quali forme di espressione sono accettate e quale tipo di contenuti può essere segnalato o rimosso».

All'interno della pagina dedicata a ciò[161], il social dichiara che la sua prima priorità è la sicurezza. A tal proposito, infatti, «non è consentito minacciare in modo verosimile altri utenti, né organizzare atti di violenza reali. […]» ed è prevista la rimozione di contenuti intimidatori con possibilità di «adire le vie legali qualora fossero rilevati seri rischi di danno fisico o minacce alla sicurezza pubblica».

Subito dopo queste previsioni, gli standard fanno riferimento all'autolesione, un tasto dolente per coloro che si occupano di cyberbullismo, giacché molte giovani vittime hanno deciso di togliersi la vita anche a causa delle prepotenze subite, annunciandolo sul proprio profilo di Facebook. Non poco frequenti, poi, sono i casi di istigazione al

[161] www.facebook.com/communitystandards.

suicidio, poiché spesso l'atto di bullismo prende forma nel "suggerimento" di uccidersi.

In questo senso, si rivelano utili le previsioni per cui viene rimosso «qualsiasi contenuto che promuova o incoraggi automutilazione, disturbi alimentari o abuso di droghe pesanti». Inoltre, il social collabora «con organizzazioni di supporto e prevenzione contro il suicidio per fornire assistenza alle persone con intenti suicidi»[162].

Arrivando al caso specifico del bullismo elettronico, la sezione ad esso dedicata fa riferimento anche alle intimidazioni, stabilendo che Facebook «non tollera atti di bullismo o molestie. [E per quanto sia consentito] agli utenti di esprimere liberamente le proprie opinioni su persone e argomenti di interesse pubblico, [verranno presi] provvedimenti in caso di segnalazione di comportamenti offensivi nei confronti di singoli individui. Il ripetuto invio agli altri utenti di richieste di amicizia o messaggi indesiderati è una forma di molestia»[163]. Ovviamente, il social «non consente i contenuti che incitano all'odio, ma attua una distinzione tra contenuti seri e meno seri». Quindi, mentre da un lato gli utenti vengono incoraggiati «a mettere in discussione idee, eventi e linee di condotta», si mantiene fermo il divieto di discriminare le persone «in base a razza, etnia, nazionalità, religione, sesso, orientamento sessuale, disabilità o malattia»[164]. Questa previsione relativa all'*hate speech* è parte integrante del problema del cyberbullismo, poiché, in molti casi, esso si verifica ai danni di persone disabili, straniere o omosessuali, pertanto è estremamente utile a tutelare gli utenti in tali eventualità.

Come visto in precedenza, comunque, il fenomeno non riguarda soltanto la diffamazione, ma anche la possibilità di impersonificare la vittima, tant'è che negli Standard della comunità, in riferimento a ciò, si sottolinea che in questi casi vi è una violazione delle condizioni di Facebook, poiché gli utenti non devono (pur potendo) registrarsi con profili falsi o fingere di essere un'altra persona. Inoltre, la sezione relativa all'identità fa riferimento anche alla privacy, sottolineando che è vietato

[162] Ibid.

[163] Ibid.

[164] Ibid.

«pubblicare le informazioni personali degli altri senza aver prima ottenuto il loro consenso»[165].

Per quanto riguarda, invece, la condivisione dei contenuti, mentre alle immagini di nudità sono imposte solo delle limitazioni, fermo restando «il diritto delle persone di condividere contenuti importanti per loro, siano essi fotografie di una scultura come il David di Michelangelo o foto di famiglia di una madre che allatta al seno il figlio», non è tollerata la presenza di «contenuti pornografici e con riferimenti espliciti al sesso, specialmente nel caso in cui siano coinvolti dei minorenni»[166]. Queste disposizioni, ovviamente, divengono utili nei casi di *sexting* che, come più volte ricordato, sta via via assumendo maggiore rilevanza all'interno delle strategie utilizzate dal cyberbullo.

Dopo aver parlato anche di proprietà intellettuale, *phishing*, *spam* ecc… Facebook inserisce alla fine della pagina un box relativo alla «Segnalazione di contenuti offensivi» nei casi in cui l'utente rilevi del materiale che ritiene essere una violazione dei termini di servizio e/o degli Standard della comunità, facendo notare, però, che «la segnalazione di un contenuto non ne garantisce la rimozione dal sito»[167].

Poco dopo, comunque, il social network sottolinea l'eventualità che non vi sia rimozione o blocco dei contenuti che appaiono inaccettabili o fastidiosi, poiché esso è stato creato per favorire le comunicazioni, la condivisione e il contatto tra le persone, che, tuttavia, possono appartenere a comunità diverse e quindi avere parametri di giudizio differenti rispetto a ciò che viene pubblicato dagli utenti, dai gruppi o dalle pagine. Ecco perché questi, per essere rimossi, devono necessariamente contravvenire ai principi[168] e alle condizioni d'uso basate su di essi.

Queste ultime, infatti, sono parte integrante nella risoluzione delle controversie che possono sorgere, in quanto, oltre a stabilire le normative sull'utilizzo dei dati e gli standard della comunità, danno vita alla Dichiarazione dei diritti e delle

---

[165] Ibid.

[166] Ibid.

[167] Ibid.

[168] Principi di Facebook: 1) Libertà di condivisione e di contatto; 2) Proprietà e controllo delle informazioni; 3) Libero flusso di informazioni; 4) Uguaglianza fondamentale; 5) Valore sociale; 6) Piattaforme e standard aperti; 7) Servizio fondamentale; 8) Benessere comune; 9) Processo di trasparenza; 10) Un unico mondo, in www.facebook.com/principles.php.

responsabilità, cioè quell'insieme di regole che disciplinano la «relazione con gli utenti e con chiunque interagisca con Facebook»[169].

Non a caso, essa ribadisce dei punti che, assieme a quanto descritto sopra, possono essere considerati fondamentali nella risoluzione del fenomeno del cyberbullismo. Si tratta di veri e propri consigli all'utente, come «[…] Non cercare di ottenere informazioni di accesso o accedere ad account di altri utenti. Non denigrare, intimidire o molestare altri utenti. Non pubblicare contenuti: minatori, pornografici, con incitazioni all'odio o alla violenza, con immagini di nudo o di violenza forte o gratuita. […] Non usare Facebook per scopi illegali, ingannevoli, malevoli o discriminatori. […] Non favorire o incoraggiare alcuna violazione della presente Dichiarazione o delle nostre normative. […] Non fornire informazioni personali false su Facebook o creare un account per conto di un'altra persona senza autorizzazione. […] Non usare Facebook se non ha raggiunto i 13 anni»[170]. Insomma, si tratta di un elenco di *best practices* degli utenti, che il social network affianca alla protezione dei diritti di terzi, poiché la questione non riguarda solo l'uso responsabile e sicuro della rete, ma anche un comportamento rispettoso dei diritti umani in genere, tanto che si dichiara esplicitamente: «È vietato pubblicare o eseguire azioni su Facebook che costituiscano violazione dei diritti di terzi o delle leggi vigenti in alcun modo. Ci riserviamo il diritto di rimuovere tutti i contenuti o le informazioni che gli utenti pubblicano su Facebook, nei casi in cui si ritenga che violino la presente Dichiarazione o le nostre normative»[171].

Tutto ciò che è stato citato sinora è largamente applicabile ai casi di bullismo elettronico, anche se, con riferimento alle "dispute" relative ai contenuti potenzialmente dannosi o inappropriati, alla fine della Dichiarazione di responsabilità si legge: «Anche se forniamo delle regole per la condotta degli utenti, non controlliamo né guidiamo le azioni degli utenti su Facebook e non siamo responsabili dei contenuti o delle informazioni che gli utenti trasmettono o condividono su Facebook. Non siamo responsabili di alcuna informazione o contenuto offensivo, inappropriato, osceno, illegale o altrimenti deplorevole presente

[169] www.facebook.com/legal/terms.

[170] Ibid.

[171] Ibid.

su Facebook. Non siamo responsabili della condotta, sia online che offline, di alcun utente su Facebook». Insomma, di fatto, il social network si chiama fuori da qualsiasi coinvolgimento nelle responsabilità delle persone che fanno uso della piattaforma, in linea sicuramente con quanto previsto dalla *Section 230* del *Communications Decency Act* statunitense (vedi *supra* pag. 47).

Dunque, in tal senso, è sembrerebbe piuttosto complicato capire cosa aspettarsi nel caso in cui venga segnalato un caso di cyberbullismo, perché la a-territorialità del web fa sì che non vi sia una disposizione unica e applicabile in tutti i paesi, né dal punto di vista della responsabilità dei *providers*, tantomeno da quello della potenziale infrazione delle leggi statali, essendo queste ultime differenti a seconda del territorio.

Facebook, quindi, risolve il problema affermando che: «Se le azioni dell'utente violano nella forma e nella sostanza la presente Dichiarazione o creano dei rischi legali per la società, [esso si riserva] il diritto di interrompere la fornitura di parte o di tutti i servizi di Facebook nei confronti dell'utente stesso» poiché «l'utente si impegna a rispettare tutte le leggi applicabili ogni volta che usa o accede a Facebook».

Pertanto, il social network non si ritiene responsabile degli illeciti commessi tramite i servizi offerti, però si fa carico di una "*social responsibility*" che non si realizza solo con la rimozione dei contenuti inappropriati rispetto alle sue *policies*, ma anche con la sospensione totale o parziale per l'utente delle funzioni della piattaforma. Inoltre, in linea con la direttiva europea 2000/31/CE sul commercio elettronico che, escludendo un'ipotesi generale di responsabilità, prevede in alcuni casi una collaborazione dell'ISP con le autorità (vedi *supra* pagg. 53-56), Facebook delinea con precisione anche le forme di suddetta collaborazione nel suo "Centro per la sicurezza".

All'interno della sezione dedicata alla legge, infatti, si dichiara che: «Se Facebook riceve una richiesta ufficiale avente come oggetto i dati di un account, il primo passo consiste nello stabilire la legittimità della richiesta»[172]. Ciò, dunque, sottolinea la disponibilità della piattaforma a reprimere gli illeciti come, nel nostro caso, quelli compiuti dal cyberbullo tramite falso profilo o mediante account originale. Queste misure di arginamento, infatti, possono consistere nel «fornire informazioni a

[172] www.facebook.com/safety/groups/law.

rappresentanti ufficiali delle forze dell'ordine per aiutarli a rispondere e far fronte alle emergenze, comprese quelle che coinvolgono rischio di danni immediati, prevenzione dei suicidi e recupero di minori dispersi. Potremmo anche fornire alle forze dell'ordine delle informazioni per aiutarle a prevenire o a far fronte a frodi o altre attività illegali, nonché ad altre violazioni delle Condizioni di Facebook»[173].

Chiaramente, ciò può avvenire soltanto attraverso una richiesta ufficiale da parte delle autorità, a seguito della quale, se si tratta di indagine penale, i dati di un account verranno salvati «per 90 giorni in attesa della ricezione del processo legale formale»[174].

Tuttavia, nei casi di "richieste di emergenza", che richiedono di ottenere le informazioni richieste in brevissimo tempo per la «tutela di un danno imminente a un bambino o al rischio di morte o serio danno fisico a qualsiasi persona, un agente delle forze dell'ordine può presentare richieste attraverso il sistema di richieste online per le forze dell'ordine su facebook.com/records». A ciò si aggiunge il fatto che «se una richiesta riguarda un caso di sfruttamento o sicurezza minorile, è opportuno specificarlo nella richiesta», così da poter permettere al social network di gestire il caso «in modo immediato ed efficace».

Tra l'altro, anche se i requisiti elencati affinché vengano fornite le informazioni richieste sono tutti relativi alle disposizioni legislative statunitensi, nella sezione «Requisiti per i procedimenti giudiziari internazionali», si precisa che, per gli stati esteri, «potrebbe essere necessaria una richiesta *Mutual Legal Assistance Treaty* o una rogatoria per ottenere il rilascio dei contenuti di un account».

Tuttavia, rispetto alla possibilità di rilasciare dati dei cittadini europei, Facebook pubblica un'interessante informativa che riguarda la sua adesione al programma *Safe Harbor*[175], nato in seguito all'emanazione della direttiva della Commissione europea sulla protezione dei dati personali[176]. Quest'ultima vieta il trasferimento di dati personali verso paesi non appartenenti all'Unione Europea che non soddisfano gli standard di "adeguatezza" da essa stabiliti.

---

[173] Ibid.

[174] Ibid.

[175] export.gov/safeharbor.

[176] Direttiva 95/46/CE.

Così, per colmare le eventuali differenze tra USA e UE relative all'approccio alla tutela della privacy e, soprattutto, per uniformare la disciplina dei *providers* nei due continenti, superando il problema della a-territorialità della rete, lo *US Department of Commerce* e la Commissione europea hanno elaborato un quadro unico di riferimento nel programma *Safe Harbor*. La sua adozione è stata necessaria, in quanto, ai sensi della direttiva sulla protezione dei dati personali, le aziende operanti nell'Unione Europea non sono autorizzate ad inviare dati personali a paesi non appartenenti allo Spazio economico europeo, se non vi è una garanzia che essi riceveranno adeguati livelli di protezione.

Il programma si basa sul rispetto dei cd. *Privacy Principles*, i sette cardini che le organizzazioni americane della rete devono rispettare per entrare a far parte dell'accordo. Essi consistono nella fornitura agli utenti di:

- informazioni sul fatto che i loro dati vengono racconti e su come ciò avviene (*notice*);
- una possibilità di "*opt-out*" rispetto alla raccolta e al trasferimento dei dati a terzi (*choice*);
- un adeguato livello di protezione nel trasferimento dei dati a terzi che può avvenire solo verso quelle organizzazioni che rispettano questi standard (*onward transfer*);
- garanzie relativamente alla perdita delle informazioni raccolte, affinché vi sia il minor rischio possibile che ciò accada (*security*);
- dati pertinenti e utili rispetto allo scopo per cui sono stati raccolti (*data integrity*);
- poter accedere alle informazioni conservate su di loro, così da potergli permettere di correggerli o cancellarli se sono inesatti (*access*);
- strumenti efficaci per l'applicazione di questi principi (*enforcement*).

In quest'ultimo caso, infatti, come parte degli obblighi per chi entra a far parte del programma, si impone alle organizzazioni di avere un sistema di risoluzione delle controversie per indagare e risolvere i singoli reclami. Nel caso in cui, però, un'organizzazione non rispetti queste previsioni essa potrà essere esclusa dal programma e qualora si basi, del tutto o in parte, sull'autoregolamentazione per garantire i *Safe Harbor Privacy Principles*, allora la loro inosservanza sarà perseguibile dalla *Federal Trade Commission*, ai sensi delle leggi che proibiscono atti sleali e ingannevoli.

Nel quadro della sua partecipazione al programma, Facebook risolve attraverso TRUSTe le eventuali dispute tra l'utente e il social network che riguardano l'attuazione delle condizioni d'uso e le procedure di rimozione o esclusione dai servizi (es: abuso da parte di un altro utente, hackeraggio dell'account, scoperta di un profilo appartenente ad un minore di 13 anni ecc…).

Date queste premesse, dunque, si nota come l'aspetto più interessante del cyberbullismo sui social network chiami in causa molte questioni differenti, dalla privacy alla reputazione, passando per il furto di identità o l'impersonificazione, fino ad arrivare alla neutralità della rete e alle intimidazioni.

Insomma, la peculiarità del fenomeno è proprio quella di incarnarsi nelle fattispecie più varie, ecco perché è stato necessario, a partire dai principi e dalle condizioni di Facebook, delineare un quadro generale che le raccogliesse tutte.

Considerato ciò, comunque, la piattaforma mette a disposizione degli utenti anche una sezione specifica relativa al bullismo elettronico che si ricollega ai meccanismi di segnalazione e rimozione dei contenuti, valido per tutta una serie di materiali inappropriati.

Il 21 maggio 2014, infatti, nel Centro per la sicurezza ha preso vita la piattaforma di prevenzione contro il bullismo[177], adottata in collaborazione con Telefono Azzurro e Save The Children Italia, che costituisce l'evoluzione della sezione intitolata "Prevenzione del bullismo"[178]. Quest'ultima, nata nel novembre 2013, conteneva suggerimenti per adolescenti, genitori e insegnanti su come affrontare il fenomeno, ma soprattutto l'elenco delle risorse online a disposizione, accuratamente descritte, che consentono di agire su Facebook.

Il portavoce dell'azienda, Matt Steinfeld, a tal proposito aveva dichiarato proprio l'intento della compagnia di costruire meccanismi di tutela a partire da quanto già previsto dal social network relativamente alla segnalazione di contenuti offensivi o dannosi. Per esempio, nel 2011 era stata introdotta la cd. "segnalazione sociale", «una funzione dello strumento di segnalazione per risolvere i problemi con i post, i diari e altri contenuti presenti sul sito». Questa, infatti, serve a segnalare un

[177] www.facebook.com/safety/bullying.

[178] www.facebook.com/safety/bullying/teens.

contenuto ritenuto inadeguato che però non viola le Condizioni d'uso ed invita l'utente o un suo amico registrato ad inviare un messaggio alla persona che lo ha caricato affinché lo rimuova. Questo meccanismo ha riscosso particolare successo, al punto che Facebook, per far fronte al cyberbullismo, aveva poi inserito nella pagina sugli strumenti per la sicurezza[179] il seguente paragrafo: «In caso di bullismo o comportamento indesiderato, quando non vuoi contattare direttamente la persona in questione, puoi usare la funzione di segnalazione sociale per chiedere aiuto a un genitore, un insegnante o un amico fidato. Avrai così la possibilità di condividere quel contenuto, allegandovi un messaggio di spiegazione, con qualcuno di cui sai di poterti fidare».

La piattaforma, dunque, aveva attivato sin dal 2013 quel meccanismo di intervento coordinato su più livelli cui si è spesso fatto riferimento nel corso di questo lavoro e aveva già chiarito all'utente la possibilità di «bloccare la persona che ha pubblicato il contenuto e segnalarla a Facebook, [consentendogli] di prendere le misure appropriate. La segnalazione sociale può essere usata anche per aiutare gli amici che hanno bisogno di supporto»[180].

Oggi, nella piattaforma di prevenzione contro il bullismo si legge ancora che si tratta di un insieme di «risorse per ragazzi, genitori ed insegnanti» e viene mantenuta l'articolazione su questi tre livelli «al fine di fornire risorse e strumenti per la gestione degli atti di bullismo e delle relative conseguenze»[181].

Si tratta di un lavoro frutto della collaborazione tra Facebook e lo Yale Center for Emotional Intelligence, i cui membri, in particolare Marc Brackett e Robin Stern, hanno aiutato la piattaforma a sviluppare questo sistema di prevenzione dove verrà reindirizzato chiunque segnali episodi di bullismo, così da fornirgli consigli utili nonappena l'utente ne abbia necessità. Non a caso, nella *home* della piattaforma si legge: «Fermiamo il bullismo. Presentazione di strumenti, suggerimenti e programmi per aiutare le persone a difendere se stesse e gli altri»[182]. Subito sotto, vi è

[179] www.facebook.com/safety/tools.

[180] www.facebook.com/safety/bullying.

[181] Ibid.

[182] Ibid.

l'inquadramento del fenomeno, descritto come «qualsiasi tipo di atteggiamento aggressivo che comporta uno squilibrio di potere, dovuto ad esempio allo status sociale o alla stazza fisica. Oltre ad attacchi fisici o verbali, il bullismo comprende le minacce, la diffusione di dicerie o l'esclusione intenzionale di una persona da un gruppo»[183].

Infatti, su Facebook, i modi in cui il bullo può perseguitare la sua vittima sono numerosi:

- taggandola in foto intime o imbarazzanti senza il suo consenso;
- pubblicando post ingiuriosi sulla sua bacheca;
- inviandole messaggi minacciosi o offensivi in chat/*in-box*;
- realizzando pagine o gruppi per deriderla in pubblico;
- commentando in modo sgradevole le sue foto o i suoi aggiornamenti di stato.

Nella sezione dedicata ai ragazzi, la piattaforma divide l'iter in due fasi. La prima è quella che fornisce "Maggiori informazioni" e spiega le diverse configurazioni del fenomeno, rivolgendosi alla vittima, agli amici e persino al bullo. La seconda fase, invece, "Passa all'azione" e definisce per queste tre categorie di soggetti quali strumenti si possono adottare contro gli atti di bullismo.

A chi subisce le prepotenze viene spiegato come difendersi, cosa fare, come parlare con qualcuno (sia che si traddi di un adulto o che direttamente del persecutore) e quali strumenti/opzioni di Facebook sono utilizzabili al fine di far cessare gli abusi.

Agli amici delle vittime viene fornito lo stesso percorso di sostegno, in modo da capire come si possa essere d'aiuto a chi sta subendo simili prepotenze, mentre al bullo viene spiegato il perché delle sue azioni e viene consigliato di scusarsi.

Anche la sezione dedicata ai genitori divide l'iter nella fase informativa e in quella attiva, rivolgendosi sia ai parenti delle vittime che a quelli dei bulli. In entrambi i casi è previsto uno step dialogico, in cui si deve conversare efficacemente con il ragazzo e parlare del problema, ma nella fase di azione le strade prendono due direzioni diverse: i genitori della vittima dovranno sviluppare un piano di azione con il figlio, mentre quelli del bullo dovranno valutare le diverse soluzioni. Nel primo caso, poi, vengono individuate le risorse messe a disposizione da Facebook e viene consigliato di approfondire la questione, soprattutto facendo riferimento all'autolesionismo e al

[183] Ibid.

sexting. Nel secondo caso, invece, i parenti del bullo vengono invitati a trovare una soluzione e ad andare fino in fondo alla questione, in modo da evitare il ripetersi o il protrarsi del comportamento aggressivo.

Nella sezione dedicata agli insegnanti, le due fasi precedentemente citate (informativa e attiva) sono piuttosto simili a quelle descritte per i genitori, anche se translate nel contesto scolastico. Ad essse, però, se ne aggiunge una terza, quella della prevenzione, in cui si incoraggia il docente a creare «un ambiente in cui sia chiaro che qualsiasi forma di bullismo non è sinonimo di popolarità». Ciò avviene creando un «decalogo di buona condotta» e ricordando «agli studenti di chiedere aiuto», ma soprattutto creando «norme di sicurezza a scuola». In quest'ultimo caso, prima ancora di aver descritto la serie di sistemi che possono essere attivati per proteggere gli studenti, Facebook invita gli insegnanti a parlare «con il legale della scuola prima che si verifichi il primo caso di bullismo per capire quali misure [si dovrebbero] adottare e quali responsabilità spetterebbero [al docente], ad esempio in caso di mancata prevenzione adeguata o risposta al bullismo online». Ciò dimostra la necessità di un intervento coordinato su più livelli, cui spesso si è fatto riferimento nel corso di questo lavoro, in cui anche la legge ha un ruolo determinante dal punto di vista non solo della repressione ma anche della prevenzione.

Insomma, da qualsiasi punto di vista la si guardi, che sia con gli occhi di un ragazzo o di un adulto, Facebook ha fornito una guida intelligente e completa alle modalità di prevenzione e repressione del cyberbullismo, che dimostra il suo tentativo virtuoso di rispondere alla responsabilità sociale che si attiva nel momento in cui un provider decide di fornire un servizio agli utenti.

Le recenti innovazioni, dunque, rappresentano un *exemplum* di quanto auspicato sin dall'inizio di questo lavoro, soprattutto laddove vi è un vero e proprio dialogo con gli utenti. Infatti, l'approccio della piattaforma non è limitato a fornire delle condizioni di utilizzo e degli strumenti per reprimere gli illeciti, ma cerca di guidare gli adulti e i ragazzi ad un corretto uso dei suoi servizi, a prescindere dal fatto che essi siano dalla parte delle vittime o da quella dei cyberbulli.

La *home* della piattaforma contro il bullismo, comunque, si conclude con tutta la serie di partner internazionali che collaborano con Facebook per arginare il fenomeno a livello preventivo e successivo. Si tratta di organizzazioni quali Save

The Children, Stop CyberBullying, Connect Safely, Childnet, ISPCC, Telefono Azzurro e moltissime altre, cui già si è spesso fatto riferimento nel corso di questo lavoro, a dimostrazione del fatto che l'intervento multilivello è ormai un approccio internazionale di contrasto al cyberbullismo, unitamente a strategie che vanno oltre i confini nazionali per adeguarsi al carattere di a-territorialità della rete.

A livello pratico, qualora si cerchino informazioni prima di segnalare le prepotenze, nella pagina "Strumenti e risorse per la sicurezza", nella sezione "Segnalazione abusi"[184], alla domanda "Cosa devo fare se sono vittima di atti di bullismo, molestie o attacchi da parte di qualcuno su Facebook?" viene risposto che esistono diversi modi per fermare queste azioni. Si tratta degli stessi strumenti citati nella piattaforma di prevenzione contro il bullismo, le cui diverse configurazioni vengono elencate nella sezione "Come segnalare i contenuti"[185] e che, ovviamente, si possono facilmente applicare a ciò cui l'utente può accedere.

Infatti, ferma restando la possibilità di chiudere il proprio account, è possibile segnalare l'utente o i contenuti offensivi che egli pubblica. Ciò avviene mediante un meccanismo di report che può essere applicato a diverse funzioni offerte dalla piattaforma, tra cui: diari, messaggi, gruppi, pagine, foto e video, post, post sul diario personale, domande ecc…

A questo punto, però, si un altro strumento nelle mani degli utenti che si ritrovano ad essere vittima del cyberbullismo pur non essendo iscritti al social network. Infatti, anche nel caso in cui egli non abbia la possibilità di visualizzare ciò che avviene sulla piattaforma (ad es. gruppi segreti o chiusi) oppure se non possiede un account, Facebook mette a disposizione un modulo[186] per ovviare al problema:

[184] www.facebook.com/help.

[185] Ibid.

[186] Ibid.

Questa opzione può essere utilizzata anche quando l'utente possiede un profilo ma, dopo aver rimosso l'utente dalle amicizie ed averlo bloccato, gli insulti e le prepotenze continuano. In questi casi, Facebook suggerisce anche di chiedere ai propri amici di segnalare a loro volta il diario e i contenuti della persona in questione, così da agire in modo collaborativo (cd. "segnalazione sociale", vedi pag. 117). Inoltre, qualora si sia a conoscenza di un caso di bullismo elettronico, grazie alla voce "Altro abuso o comportamento indesiderato" è possibile per chiunque (fornito o meno di un account) fare presente la questione mediante segnalazione.

La serie di problemi previsti, poi, copre una gamma molto ampia di aspetti che il cyberbullismo può assumere, come l'uso illegittimo di materiale fotografico, la violazione dei diritti ad esempio con la creazione di una pagina o un gruppo con intenti denigratori, le minacce di violazione della privacy ecc…

Comunque, oltre a quelli sovra citati, esistono anche altri due modi, seppur indiretti, in cui il bullo può prendersi gioco della sua vittima, cioè rubandole la password di accesso all'account e utilizzandolo a suo nome o creando un profilo falso per impersonificarla.

Mentre nel primo caso è possibile reimpostare la password attraverso dei semplici passaggi nella sezione "Account violati"[187], nel secondo caso invece è necessario compilare un'apposita richiesta contenente:

«[…] - un'immagine scannerizzata o digitale di un documento di identità ufficiale (ad esempio, la patente di guida o il passaporto);

- una dichiarazione autenticata che confermi la tua identità;

- una copia della denuncia relativa alla tua richiesta»[188].

In ogni caso, è possibile verificare a che punto sia la segnalazione mediante l'accesso, dalle impostazioni del proprio profilo, alla sezione "Riepilogo segnalazioni" che consente di annullare l'azione, di verificare se e quando sono state adottate delle misure a seguito del report, ma anche di sapere in cosa esse consistono.

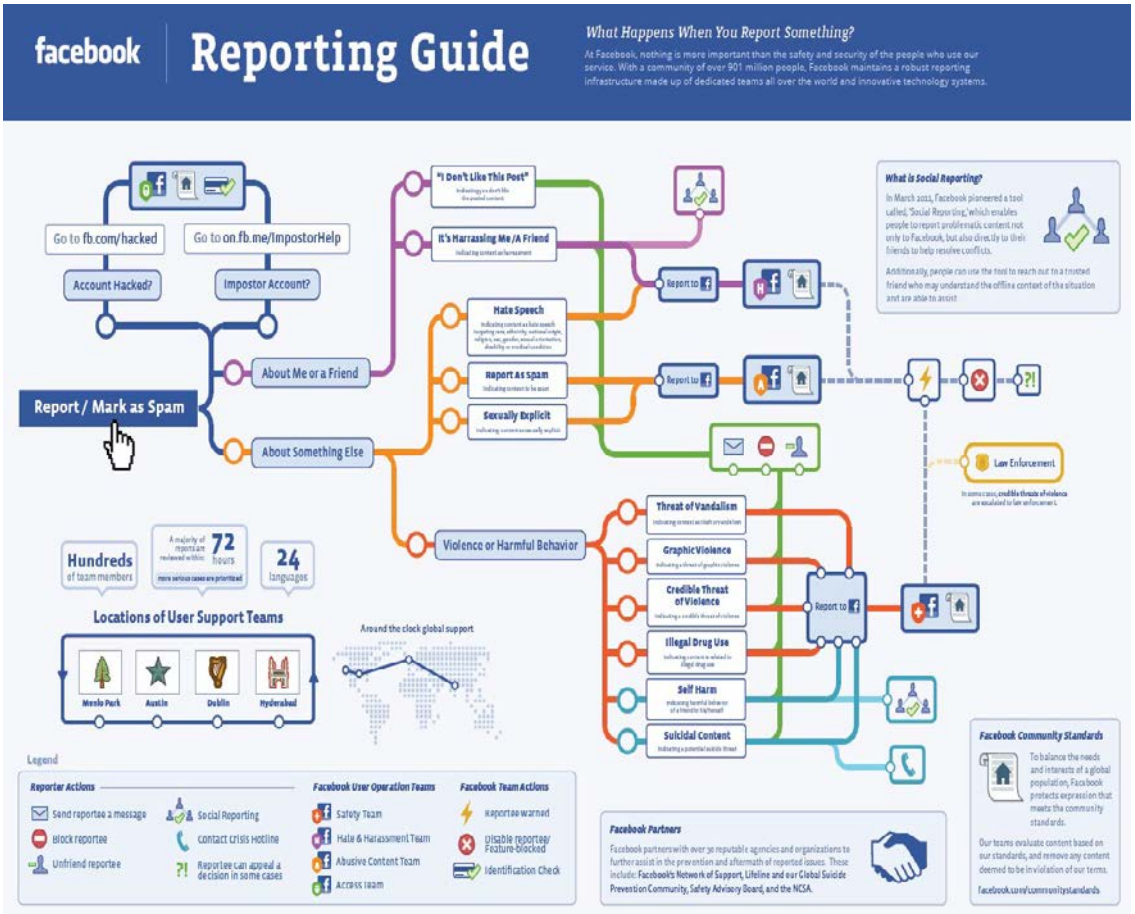
Se si osservano tutti gli elementi sino ad ora considerati, sembrano essere disponibili moltissime disposizioni a tutela delle vittime del cyberbullismo ed appare molto semplice espedire le procedure necessarie ad impedire la continuazione delle prepotenze. In realtà, però, l'iter di risposta ad una segnalazione è estremamente lungo a causa del gran numero di *alert* giornalieri che Facebook riceve.

A proposito di ciò, la piattaforma ha pubblicato sulla pagina ufficiale di Facebook Safety[189] una nota che si pone come una guida ufficiale al «*reporting process*», fornendo un *infographic* che sintetizza i vari passaggi di avanzamento:

[187] Ibid.

[188] Ibid.

[189] www.facebook.com/fbsafety.



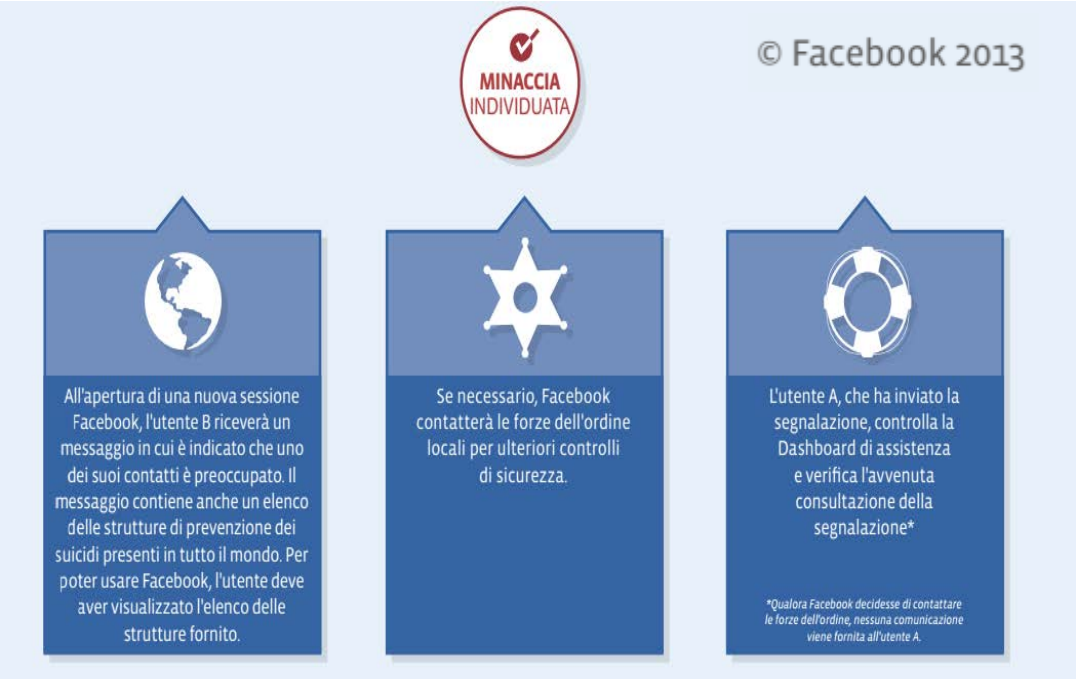
Dunque, vi sono quattro team, uno per la sicurezza rispetto ai contenuti violenti (*Safety team*), uno che si occupa di incitamento all'odio e di minacce (*Hate&Harrassment Team*), un altro per lo spam o per i materiali sessualmente espliciti (*Abuse Content Team*) e infine quello relativo all'accesso (*Access Team*). Le squadre sono situate tra Menlo Park, Austin, Dublino e Hyderabad e lavorano no-stop ogni giorno della settimana per gestire i report in oltre 24 lingue. Infatti, quando una persona invia una segnalazione, a seconda del motivo per cui l'ha effettuata, essa viene inviata all'equipe competente che si occupa di valutare se i contenuti rispettano gli Standard della comunità per poi rimuoverli in caso contrario.

Se la Dichiarazione dei diritti e delle responsabilità o le *policies* vengono violate, il contenuto viene rimosso e la persona che lo ha postato viene contattata. Inoltre, nei casi più gravi, è possibile che il team decida di revocare la capacità di un utente di condividere determinati tipi di materiale o di utilizzare alcune funzioni, fino ad arrivare al caso in cui esso provveda a disattivare l'account o a contattare le forze dell'ordine.

Tuttavia, è possibile che il contenuto non sia illecito e pertanto venga mantenuto, ma la persona che lo segnala potrebbe volerlo rimuovere comunque, ad esempio nel caso in cui un cyberbullo pubblichi una foto della sua vittima che questa ritiene imbarazzante. In questo caso si può utilizzare la sovra citata "segnalazione sociale" che consente di risolvere le controversie direttamente tra gli utenti.

Oltre all'intervento dei suoi team, comunque, Facebook si avvale delle competenze di oltre 30 agenzie di prevenzione del suicidio in tutto il mondo e alla rete di supporto per gli utenti LGBT.

Nel primo caso, infatti è prevista un'unità di crisi che interviene nel caso in cui l'utente A segnali contenuti relativi ad un potenziale suicidio dell'utente B, per cui una volta che la minaccia è stata individuata avviene quanto riportato nel grafico ufficiale di Facebook[190]:



In ogni caso è anche possibile non contattare Facebook, che comunque rimanda ai numeri nazionali delle linee di supporto per la prevenzione del suicidio[191] per far sì che vi sia più di un'alternativa per fronteggiare tempestivamente tale rischio.

[190] Facebook, the Jed Foundation and the Clinton Foundation, *Guide to help college students identify signs of distress*, in www.facebook.com/safety/tools.

[191] www.facebook.it/help.

Considerato l'elevato numero di adolescenti che, di recente, si è tolto la vita annunciandolo sul social network o pubblicandovi vere e proprie lettere di addio, queste risorse divengono fondamentali anche nei casi di cyberbullismo, poiché consentono di intervenire sull'aspetto psicologico del fenomeno oltreché su quello pratico, relativo alla repressione degli abusi del bullo.

Con riferimento a ciò, inoltre, sono estremamente utili le previsioni inserite all'interno del Centro per la sicurezza a proposito della "rete di supporto di Facebook" poiché sempre più spesso i ragazzi sono oggetto di minacce e abusi da parte dei cyberbulli a causa del loro orientamento sessuale. Infatti, lo stesso sito dichiara di collaborare con «organizzazioni nazionali[192] per combattere il cyberbullismo che ha come vittime i giovani LGBT».

La "*Facebook Network of Support*" (NOS), infatti, è composta da cinque associazioni che si occupano di tutela dei diritti delle lesbiche, degli omosessuali, dei bisessuali e dei transessuali e collabora con la campagna di MTV "A Thin Line" per offrire supporto alla piattaforma nella risoluzione dei problemi generati dal bullismo ai danni degli omosessuali.

Stando a quanto sin qui riportato, il social network sembra avere un sistema efficientissimo e quasi infallibile per contrastare il cyberbullismo, che comprende sia misure specifiche per il fenomeno sia implementazioni dei servizi offerti per proteggersi dagli altri abusi.

Tuttavia, nonostante si cerchi di assicurare un'esperienza sicura ai più giovani, i rischi rimangono ancora persistenti considerando che la piattaforma, nell'ottobre 2012, ha raggiunto un miliardo di utenti con un conseguente aumento delle segnalazioni da gestire che hanno diluito i tempi di risoluzione.

Insomma, mentre la piattaforma cerca di promuovere l'utilizzo corretto dei suoi servizi, agendo direttamente all'interno delle scuole e delle famiglie si necessita di un'implementazione a livello tecnico che possa andare a snellire le procedure e ad aumentare i membri dei diversi team che si occupano di rispondere alle segnalazioni.

[192] A Thin Line, The Gay and Lesbian Alliance Against Defamation, The Gay, Lesbian and Straight Education Network, The Human Rights Campaign, The Trevor Project, Parents, Families&Friends of Lesbians and Gays.

Nel 2012, comunque, un portavoce di Facebook aveva dichiarato all'Huffington Post[193] che la rete di report si occupava di molestie dando ad esse elevata priorità, lavorando con squadre di indagine che mettono in atto interventi rapidi. In realtà, però, la possibilità per tutti i minori di rendere pubblici i propri profili, attivata ad ottobre 2013, non fa altro che acuire il problema e aumentare il numero delle segnalazioni. La maggior parte dei ragazzi, infatti, non si rende conto dei rischi che corre sul web, tantomeno riesce a capacitarsi del fatto che chiudere un account se si è bersagliati non significa non poter essere presi di mira tramite pagine o gruppi appositi.

Per questa ragione, alla fine di maggio del 2014, la piattaforma ha deciso di rivoluzionare la sua politica in termini di privacy, impostando come opzione di default quella di condivisione esclusiva con gli "amici". Ciò significa che, dopo aver creato un nuovo account, l'utente avrà la possibilità di scegliere esplicitamente di rendere pubblici i suoi contenuti, ma finché non deciderà di farlo, i suoi post e le sue attività resteranno visibili solo agli "amici".

Per tutti coloro che posseggono già un profilo non sono previsti cambiamenti, ma apparirà nella loro *home page* l'indicazione di "*privacy check-up*" con la quale essi verranno esortati a rivedere le loro opzioni di condivisione.

Unitamente a queste novità, vi è anche quella della piccola mascotte a forma di dinosauro blu, che comparirà nonappena gli utenti saranno in procinto di pubblicare un post, chiedendogli di assicurarsi che essi non condividano i contenuti con più persone di quelle che effettivamente desiderino (vedi Immagine 1).

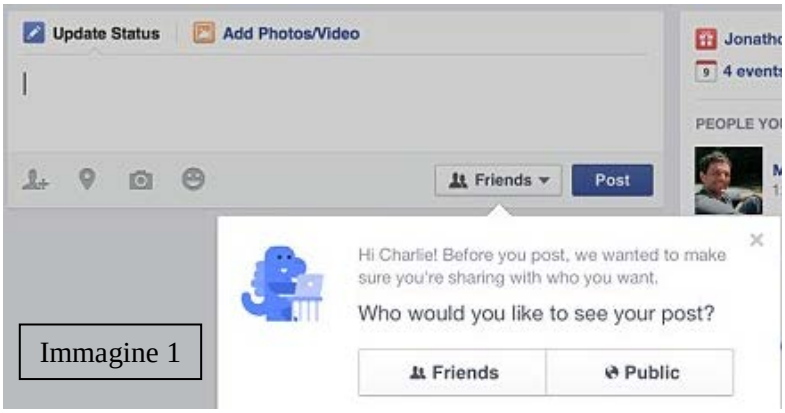


Immagine 1

[193] Sara Gates, *U.K. High Court Rules In Nicola Brookes' Favor: Facebook Must Turn Over Cyberbullies' Identities*, The Huffington Post, 6/8/2012.

Insomma, dal momento che il cyberbullismo si configura in fattispecie estremamente diverse tra loro e che spesso vanno a sommarsi in un unico abuso, è necessario un intervento immediato e in grado di interrompere l'attività dannosa. In tal senso, è fondamentale il primo passo compiuto per insegnare ai giovani e alle loro famiglie il corretto utilizzo della piattaforma e le modalità di difesa in caso di bullismo elettronico. Tuttavia, per chi scrive, il lavoro preventivo ed educativo di Facebook non potrà considerarsi concluso finché suddetta azione non verrà implementata in modo da garantire un intervento tempestivo e repressivo dei team che rispondono alle segnalazioni.

3.3 – Twitter e le differenti tipologie di abusi ricondotte all'interno del fenomeno del cyberbullismo

Proprio come già visto nel caso di Facebook, anche Twitter ha aderito al progetto *Safe Harbor* per garantire agli utenti europei che i loro dati vengano trattati in base ai *Privacy Principles* dalle società di social networking con sede negli Stati Uniti[194].

In tal senso, nonostante vi sia un'approfondita Informativa sulla Privacy[195], la piattaforma si riserva il diritto di «conservare e divulgare» le informazioni personali dei suoi utenti qualora «sia ragionevolmente necessario per ottemperare a una legge, un regolamento o un ordine dell'autorità, per proteggere la sicurezza di una persona, per contrastare frodi, problemi tecnici o per la sicurezza oppure per tutelare i diritti o la proprietà di Twitter»[196]. Infatti, nei suoi *Terms of Service*, il social network, come già visto con Facebook, si riserva «il diritto (ma non avrà l'obbligo) di rimuovere o rifiutare, in ogni momento, la distribuzione di Contenuti sui Servizi, di sospendere o chiudere utenze e di richiedere la restituzione di alcuni nomi utente senza alcuna responsabilità nei confronti dell'utente. Twitter si riserva altresì il diritto di accedere, leggere, conservare e divulgare le informazioni che ritenga ragionevolmente necessarie per: (i) conformarsi a ogni legge, regolamento, procedimento legale o richiesta governativa applicabile, (ii) imporre l'osservanza delle Condizioni, anche

[194] twitter.com/privacy.

[195] Ibid.

[196] Ibid.

mediante l'accertamento di potenziali violazioni delle stesse, (iii) individuare, impedire o in altro modo affrontare frodi o problematiche inerenti la sicurezza o di natura tecnica, (iv) rispondere alle richieste di assistenza da parte degli utenti, o (v) proteggere i diritti, la proprietà o la sicurezza di Twitter, dei propri utenti e del pubblico»[197]. Dunque, anche in questo caso, vi è un bilanciamento tra tutela dei dati personali e sicurezza, che si pone come condizione fondamentale nel contrastare fenomeni quali quelli relativi al cyberbullismo, poiché spesso è necessario risalire ai colpevoli per interrompere le attività dannose. Parallelamente, però, come già visto nel caso di Facebook, anche questa seconda piattaforma esclude la sua responsabilità «per danni indiretti, incidentali, speciali, consequenziali o punitivi […] o altre perdite immateriali risultanti […] (ii) dalla condotta o dal contenuto di terzi sui servizi, ivi incluso a titolo esemplificativo ma non esaustivo, le condotte diffamatorie, offensive o illegali di altri utenti o di terzi; […] o (iv) dall'accesso, utilizzo o alterazione non autorizzati delle trasmissioni o dei contenuti dell'utente» poiché è quest'ultimo ad essere «responsabile del proprio utilizzo dei Servizi, dei Contenuti forniti e di ogni conseguenza che ne possa derivare»[198].

Posto questo quadro di riferimento che sottolinea le attribuzioni e gli oneri di chiunque attivi un account su Twitter, sia esso un adulto o un ragazzo, un'ulteriore similitudine tra le due piattaforme risiede proprio nel richiedere come requisito minimo per usufruire dei servizi i 13 anni di età. Infatti, nella sezione relativa alla privacy, Twitter dichiara: «I nostri Servizi non sono diretti a persone di età inferiore ai 13 anni. Se vieni a sapere che il tuo bambino ci ha fornito informazioni personali senza il tuo consenso, ti preghiamo di contattarci all'indirizzo privacy@twitter.com. Non raccogliamo consapevolmente informazioni personali su bambini di età inferiore a 13 anni. Se veniamo a sapere che un bambino di età inferiore ai 13 anni ci ha fornito informazioni personali, ci attiviamo per rimuovere tali informazioni e per cancellare l'account del bambino».

Infatti, nonostante si tratti di «un social network per la trasmissione di informazioni che consente a persone e aziende di diffondere pubblicamente e immediatamente brevi messaggi in tutto il mondo […] gran parte delle comunicazioni che avvengono

[197] twitter.com/tos.

[198] Ibid.

su Twitter può essere visualizzata da chiunque. Trattandosi di informazioni pubbliche, possono essere ritweettate sul sito da chiunque le visualizzi».

Nonostante i Tweet possano essere protetti in modo da renderli visualizzabili solo dai *followers* approvati, «la maggior parte degli utenti li condivide pubblicamente»[199] pertanto i più giovani sono esposti ad un alto rischio di esposizione a meno che non vengano settate le impostazioni necessarie a mantenerli protetti. Infatti, nei casi in cui un minore venga ripetutamente bersagliato da un altro utente, Twitter «consiglia in genere di bloccare l'utente in questione e di porre fine alla comunicazione. Ignorare un contenuto equivale a dimostrare alla persona che lo pubblica di non essere disposti a interagire e, nella maggior parte dei casi, quest'ultima perderà interesse». Tuttavia, impedire al cyberbullo di continuare a seguire la sua vittima non significa garantire l'interruzione del comportamento indesiderato. Ecco perché la piattaforma consiglia esplicitamente di «coordinarsi con gli insegnanti e gli altri genitori sulle azioni da intraprendere». Infatti, come si è detto più volte all'interno di questo lavoro, il contrasto al bullismo elettronico muove in primis dall'educazione ad un uso responsabile della rete, che parte dalla famiglia e dalla scuola, come ha dimostrato il recente intervento di Facebook relativo alla "Piattaforma contro il bullismo".

Comunque, qualora ciò non bastasse, Twitter offre un suo meccanismo di segnalazione nel caso in cui vengano violate le "Regole di Twitter"[200]. Queste ultime, in relazione al fenomeno indagato, riguardano l'impossibilità di praticare l'impersonificazione, di divulgare le informazioni private, di pubblicare minacce di violenza specifiche e dirette e di dar vita ad illeciti o a prenderne parte. Inoltre, anche l'attivazione di account seriali, la diffusione della pornografia e l'abuso mirato (invio di messaggi a un utente da più account, utilizzo di un account creato con il solo scopo di inviare messaggi offensivi ad altri e minacce)[201] costituiscono un illecito ai sensi delle regole stabilite per un corretto uso dei servizi offerti.

Tutte queste fattispecie caratterizzano la potenziale attività del cyberbullo, dunque, stando a quanto dichiarato, possono essere perseguite dalla piattaforma che, nei casi

[199] *Suggerimenti sulla sicurezza per i genitori*, in support.twitter.com/articles.

[200] *Le Regole di Twitter*, in support.twitter.com/articles.

[201] Ibid.

di violazione di suddette disposizioni, si offre di sospendere o eliminare i profili che le violano, pur precisando che essa «non si occupa della mediazione in caso di dispute tra utenti»[202].

Infatti, in quest'ultimo caso, il social network consiglia di «contattare le forze dell'ordine o un rappresentante legale se un conflitto personale degenera fino a determinare minacce reali, online o offline» e si offre «di collaborare e di fornire le informazioni necessarie per eventuali indagini» rispettando quanto previsto dalla legge in proposito.

Twitter, comunque, rispetto a Facebook, offre servizi ridotti e per lo più limitati alla possibilità di pubblicare brevi frasi, ritweettarle e commentarle. Solo di recente è stata introdotta la funzione di chat privata, poiché nel singolo *tweet* è sempre stato possibile, attraverso la "*mention*", citare l'utente con cui si desidera avviare la conversazione. Dunque, relativamente alle *best practices* suggerite dal sito, il riferimento è alle modalità di *following* attivate dagli utenti che non devono essere aggressive, cioè non devono essere volte a seguire migliaia di account solo per attrarre l'attenzione, pena la sospensione del profilo[203]. Twitter, infatti, a differenza di Facebook, permette alle persone di scegliere se ricevere o meno gli aggiornamenti di un utente, senza la necessità di un'amicizia reciproca. Dunque, nel caso del cyberbullismo, ciò significa che il bullo può entrare in contatto con la vittima e tutti i suoi *followers* ed ha la possibilità di citarli nei suoi post offensivi anche senza che essi siano suoi seguaci, finché non provvederanno a bloccare il profilo del colpevole. Inoltre, questi potrebbe creare un nuovo account con cui ripetere la persecuzione, il che andrebbe ad infrangere le Regole di Twitter relative all'abuso mirato. Tutto ciò costituisce sicuramente uno strumento più diretto dell'adesione ad un gruppo o ad una pagina Facebook, poiché l'azione è unilaterale e non necessita di una mutua accettazione.

Questo spiega perché tra i due social network sussista una differenza relativamente alle azioni intraprese a seguito delle segnalazioni. Infatti, mentre Twitter pone continuamente l'accento sulla possibilità agire sull'account e «si riserva il diritto di sospendere immediatamente il tuo account senza preavviso nel caso in cui, a suo

[202] *Suggerimenti sulla sicurezza per i genitori*, in support.twitter.com/articles.

[203] support.twitter.com.

giudizio, sia presente una violazione delle Regole o dei Termini di Servizio», l'altra piattaforma è molto più parsimoniosa nel parlare di interruzione dei servizi e ne fornisce una versione totale e parziale, proprio perché le amicizie, le adesioni ai gruppi e quelle alle pagine sono basate sulla "consensualità".

In effetti, nella sezione relativa alle norme[204] vi è una descrizione dettagliatissima di quali condotte costituiscono una violazione delle regole e dei termini di servizio. Per esempio, nel caso di impersonificazione, viene precisato che: «Un account non sarà rimosso se: l'utente condivide il nome, ma non ha altri punti in comune; il profilo afferma chiaramente di non essere affiliato o connesso a persone con nomi simili»[205] ma non è sufficiente che vengano clonate le foto del profilo e dello sfondo. Infatti, «affinché ci sia impersonificazione, [gli utenti] devono anche fingere di essere un'altra persona, al fine di indurre in errore o ingannare»[206], ecco perché, rispetto ai personaggi "pubblici", vi è un rimando alle previsioni relative alla parodia, che comunque viene tutelata se nella biografia o nel nome account viene dichiarata la "falsità" del profilo.

Comunque, come già visto nel caso di Facebook, è necessario fornire «prove effettive della propria identità (copia di un documento) e gli account giudicati come in violazione della politica di impersonificazione o non in conformità alla politica su commenti/parodia, potranno essere sospesi o potrebbe essere chiesto loro di apportarvi delle modifiche»[207].

Nei casi di pubblicazione di informazioni private, Twitter interviene solo qualora si tratti di dati non immessi altrove su internet, ma comunque se si tratta di comportamenti offensivi, minacciosi o ingiuriosi, le segnalazioni giudicate valide vanno «dall'avvertimento all'utente fino alla sospensione permanente dell'account».

[204] support.twitter.com.

[205] Ibid.

[206] Ibid.

[207] Ibid.

Come si vede dall'immagine riportata[208], nei casi di pericolo per l'incolumità fisica dell'utente Twitter invita a contattare le autorità, poiché la piattaforma è consapevole della necessità di un intervento tempestivo che argini il potenziale rischio. Questo aspetto è estremamente rilevante se si fa riferimento al cyberbullismo poiché viene anteposta la salvaguardia della persona all'adempimento delle procedure di segnalazione. Tuttavia, rimane insoddisfacente il requisito di "minaccia fisica" se si considera che spesso le persecuzioni sono interamente telematiche ma avvengono senza sosta. Questa contraddizione emerge anche al momento di definire quali documenti vadano presentati alle forze dell'ordine, quando il social network fa riferimento alla necessità di riportare «i messaggi violenti» ma anche quelli «molesti»[209] attraverso la stampa o gli *screenshot*. Ciò, infatti, indica che vi è un profilo relativo allo stress psicologico ed emotivo, oltre a quello dell'incolumità fisica, che contraddistingue le prepotenze via web e deriva dal loro carattere incessante.

Comunque, nei casi di "comportamento abusivo" sono inclusi, oltre alle minacce dirette e specifiche e alle molestie, anche i contenuti offensivi, autorizzati se

[208] support.twitter.com/forms/abusiveuser.

[209] *Abuso online*, in support.twitter.com/articles.

potenzialmente provocatori «purché non violino le Regole di Twitter e i Termini di Servizio»[210] poiché solo in questo caso potrebbero essere rimossi.

Come segnalare violazioni da parte di singoli Tweet

Puoi inoltre segnalare singoli Tweet che stanno violando le Regole di Twitter o i nostri Termini di Servizio. Ciò include spam, molestie, impersonificazione, violazioni di copyright o marchi.

1. Accedi al Tweet che desideri segnalare.
2. Seleziona l'•••icona per visualizzare il menu fuori schermo.
3. Seleziona **Segnala Tweet** e una delle opzioni.
4. Seleziona **Invia** (o **Avanti** per segnalare un abuso) o **Annulla** per completare la segnalazione o bloccare l'utente.

Nota: questa funzione è attualmente disponibile solo su Twitter per iOS e su mobile.twitter.com per browser di smartphone.

Immagine 2

Una volta segnalato il *tweet* (vedi Immagine 2), si può specificare una delle tre opzioni previste: in primo luogo può trattarsi di spam, ad esempio la creazione di contenuti offensivi di massa in grado di raggiungere molti utenti in breve tempo; in secondo luogo può esservi la possibilità di un account "compromesso", cioè di un profilo di cui il vero gestore ha perso il controllo; in ultimo, vi è, chiaramente, il caso di *tweet* offensivi o molesti.

Tuttavia, dal momento che Twitter è disponibile in un elevato numero di stati che posseggono giurisdizioni diverse, è possibile che un comportamento o un determinato tipo di affermazioni costituiscano una «violazione della legge locale»[211]. In questo caso, «se Twitter viene contattato direttamente dalle forze dell'ordine, [può] lavorare con loro e fornire assistenza per la loro indagine, nonché indicazioni sulle possibili opzioni»[212].

Dunque, anche se inizialmente la piattaforma richiedeva il supporto delle famiglie e degli insegnanti per l'educazione dei minori, essa ammette la possibilità che l'offesa possa costituire un reato ai sensi della legge, pertanto si pone in atteggiamento collaborativo con le autorità, così come già visto nel caso di Facebook.

A tal proposito, nel luglio 2012, Twitter ha dato vita al suo Transparency Report, nel quale, ogni sei mesi, vengono pubblicati i dati relativi ai singoli paesi riguardanti il

[210] support.twitter.com.

[211] Ibid.

[212] Ibid.

volume di richieste governative che la piattaforma riceve affinché essa fornisca informazioni sugli utenti nonché quelle riguardanti le richieste dei governi di bloccare l'accesso ai *tweet*. Per quanto riguarda le richieste di informazioni, esse fanno parte delle indagini penali e, pertanto, devono provenire necessariamente da un ordine giudiziario che impone al *provider* di fornire i dati che consentono l'identificazione dell'utente.

L'ultimo rapporto (1 luglio-31 dicembre 2013) ha palesato la situazione in 46 paesi, tra cui l'Italia, le cui 19 richieste non sono state accontentate, l'Inghilterra, che dei suoi 56 casi ha visto un accesso alle informazioni nel 50% delle volte o gli Stati Uniti, in cui sono state presentate 833 richieste, ma solo il 63% ha avuto esito positivo[213].

L'aspetto più interessante è nella distinzione tra questo tipo di dati e quelli relativi alle "richieste di informativa di emergenza". Infatti, Twitter nelle sue "*Guidelines for Law Enforcement*"[214] (disponibili solo in lingua inglese) precisa che le informazioni sugli utenti vengono rilasciate solo in risposta ad adeguati procedimenti legali, come un mandato di comparizione o un ordine del tribunale, ma anche in risposta a una richiesta di emergenza. In quest'ultimo caso, infatti, le forze dell'ordine possono ricevere i dati degli utenti in modo rapido qualora vi sia pericolo di morte o di gravi lesioni fisiche ad una persona, così da prevenire tale danno. Ciò è possibile sia via fax che con un apposito modulo di contatto da compilare online (vedi Immagine 3) messo a disposizione esclusiva della polizia e dei rappresentanti del governo.

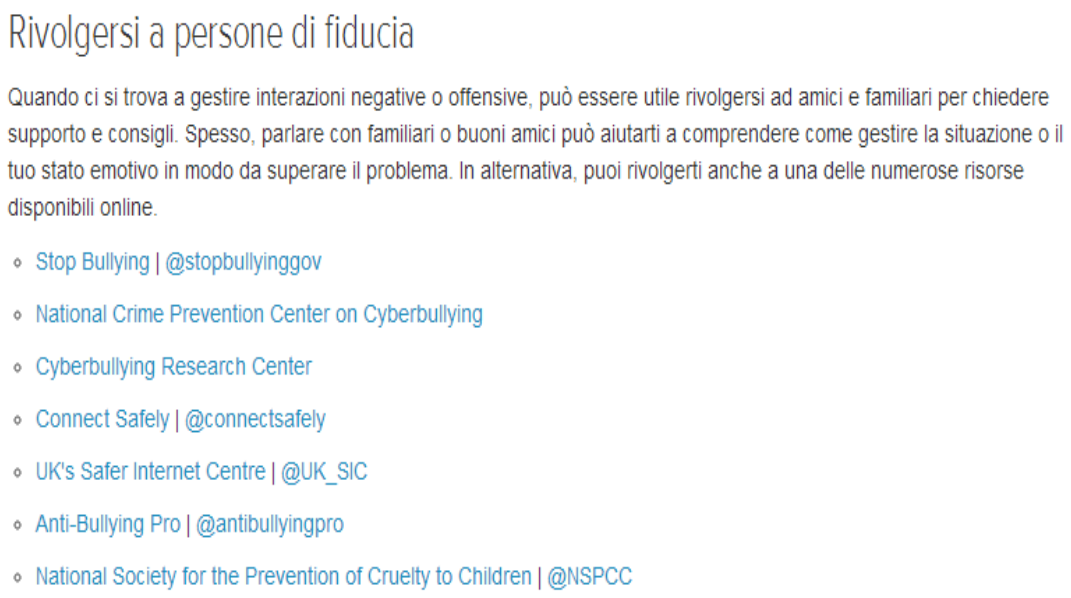
Immagine 3

[213] transparency.twitter.com/information-requests/2013/jul-dec.

[214] support.twitter.com/articles/41949#2.

Comunque, negli altri casi è bene ricordare che tutte le segnalazioni trattate possono avvenire soltanto a nome dell'utente o di un suo rappresentante legale, infatti nella sezione «Aiutare un amico o un familiare in caso di abusi online» si precisa che, qualora si noti un comportamento che costituisce abuso o molestia, è necessario suggerire al diretto interessato di segnalare suddetta condotta, a dispetto di quanto avviene su Facebook - ad esempio grazie alla "Segnalazione sociale". Ciò, probabilmente, è da attribuirsi all'assenza di opzioni che consentono di creare delle "comunità", il che mette il singolo al centro del sistema di servizi, rendendolo l'unico soggetto abilitato a contattare i gestori della piattaforma.

L'aspetto più interessante, comunque, è che i rimandi sotto alle sezioni relative a ciascuno degli argomenti sinora esposti sono relativi alle «numerose risorse disponibili online»[215]:



Come si vede dall'immagine, si tratta di "risorse" connesse del tutto o in parte con il fenomeno del cyberbullismo, a dimostrazione di quanto il problema sia diffuso e di come il social network costituisca uno dei suoi terreni più fertili.

In sostanza, nella maggior parte degli stati sono assenti disposizioni legislative che consentono di perseguire specificamente il fenomeno, quindi esso viene ricondotto a fattispecie simili, come la diffamazione o i crimini informatici (ad es. *identity fraud*). Twitter, invece, che è presente in un elevato numero di nazioni, adotta due approcci.

[215] Ibid.

Da un lato accoglie la possibilità di richiamarsi alle normative esistenti nei diversi territori, attraverso la censura selettiva e geografica dei *tweet*, che consiste nel rimuovere - successivamente alla segnalazione da parte delle autorità - quei post che infrangono la legge del paese che ne fa richiesta, oscurandoli soltanto all'interno dello stato in cui costituiscono un illecito, ma mantenendolo visibile nel resto del mondo[216]. Ovviamente, questi tipi di censura sono funzionali ad arginare eventuali problemi che potrebbero sorgere relativamente alla proprietà intellettuale o ai limiti posti, in certi paesi, al diritto di libera manifestazione del pensiero, per evitare conflitti con i governi esteri (vedi *supra* pag. 134). Dall'altro lato, però, per quello che riguarda il fenomeno in analisi, Twitter inverte l'approccio di quelle nazioni che non hanno una disciplina specifica per il bullismo elettronico, configurandolo non in modo "selettivo" e "geografico", ma come una categoria omnicomprensiva in grado di abbracciare contenuti e comportamenti che costituiscono abusi, minacce, molestie ed offese.

3.3 – La questione dell'anonimato e l'effettiva applicazione delle *policies* di Ask.fm

Domande e risposte sono al centro di un social network che sta spopolando in moltissimi stati e al primo posto tra di essi si colloca l'Italia, seguita da Brasile, Stati Uniti e Turchia. Si tratta di Ask.fm - Ask For Me - una piattaforma che ha origine in Lettonia e consente di porre interrogativi a chiunque attendendone poi la risposta, anche senza essere registrati, in forma anonima. L'unica differenza tra chi possiede un profilo e chi non lo possiede, infatti, è quella di poter dare la propria opinione al quesito posto da qualcun altro, facendolo così comparire sulla propria pagina. In realtà, vi è anche l'impossibilità di ricercare gli utenti iscritti direttamente all'interno della piattaforma, ma si tratta di un problema facilmente ovviabile attraverso l'uso di un qualsiasi motore di ricerca.

Questa "limitazione" di funzioni costituisce un tentativo di incoraggiare le persone a registrarsi per utilizzare il sito, ma, in ogni caso, anche senza possedere un account, si può decidere di non svelare la propria identità quando si pongono le domande,

[216] blog.twitter.com/2012/tweets-still-must-flow.

parallelamente al fatto che, come su Twitter, si possono avere dei *followers*, ma anch'essi restano anonimi pur avendo un profilo registrato.

Un contesto del genere, in cui neanche è necessario inventare nomi falsi o spacciarsi per qualcun altro, il cyberbullismo ha preso piede con forza ed ha contribuito al suicidio di oltre quindici ragazzi tra il 2012 e il 2014. Ciò è accaduto perché le domande non hanno limitazioni tematiche e possono andare dal semplice "Come stai?" al ben più temibile "Perché non ti uccidi?" o "Ti hanno mai detto che sei orrenda?".

Così, mentre l'amministratore delegato Ilja Terebin presenta il sito come un luogo in cui i giovani possono porre ad altri le questioni che fanno parte del loro mondo, condividere i pensieri, le idee e i sentimenti che queste domande ispirano[217], in realtà esso sta perdendo la sua funzione di spazio aperto ed onesto per trasformarsi in un potenziale nemico delle insicurezze tipiche dell'adolescenza.

Infatti, nonostante Terebin dichiari gli intenti della società di mantenere la piattaforma sicura e divertente, la sua caratteristica di garantire l'anonimato anche a chi è registrato l'ha resa lo strumento di attacco preferito dai cyberbulli.

Alla luce di ciò, sono state molte le richieste di modificare la funzione di domanda con mittente ignoto, soprattutto dopo il suicidio di Hannah Smith, una ragazza di 14 anni che viveva a Lutterworth. La giovane, infatti, si è impiccata il 2 agosto 2013 nella sua camera da letto dopo aver ricevuto per mesi "domande" da parte di altri utenti di Ask.fm che la esortavano ad uccidersi, a bere candeggina e persino a fare in modo di ammalarsi di cancro, poiché tanto a nessuno sarebbe importato della sua morte. A seguito di questi eventi, preceduti comunque già da altri suicidi, più di 15.000 persone hanno firmato una petizione online[218], sottoscrivibile fino al 5 agosto 2014, che richiede al governo britannico di agire per proteggere i più giovani dai social network come Ask.fm, affermando che il cyberbullismo è un problema in crescita nel Regno Unito e questa piattaforma, molto popolare tra i giovani, è diventata lo strumento tramite cui inviare messaggi in forma anonima, dando adito

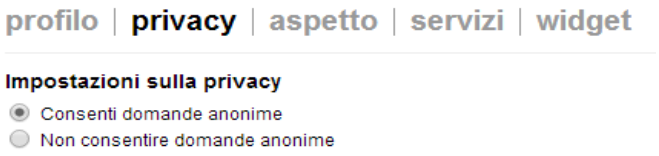
[217] «[…] young people could ask each other the questions that are shaping their world, and share the thoughts, ideas and feelings these questions inspire», *Letter from CEO, Ilja Terebin*, in ask.fm/about/safety.

[218] HM Government e-petition, *Goverment to take a Safeguarding Children position against sites like Ask.Fm*, in epetitions.direct.gov.uk.

non soltanto al bullismo e alle molestie, ma anche a problemi di salute mentale e ad intenzioni suicide, per la continuità e la segretezza che caratterizzano le attività del sito.

In effetti, stando così le cose, appare piuttosto inutile la previsione del sito secondo cui per creare un account bisogna avere almeno 13 anni dal momento che, oltre a non esservi adeguati meccanismi di verifica dell'età, vi è la possibilità di porre interrogativi in forma anonima senza alcun obbligo di registrazione.

Inoltre, anche se il profilo registrato è di un minore, le impostazioni di default non avviano le funzioni escludendo in automatico la possibilità di ricevere domande anonime, quindi a meno che l'utente non sia sufficientemente istruito e responsabile riceverà quesiti da chiunque e non soltanto da chi si dichiara apertamente:



Rimane ovviamente possibile la possibilità di bloccare un utente in particolare, di mettere un "*flag*" anziché un "*like*" se le domande risultano indesiderate oppure di segnalarne direttamente il contenuto, ma tutto questo non mette in alcun modo al riparo dalle domande anonime se esse non vengono manualmente escluse dalle impostazioni del proprio profilo - cosa che la maggior parte degli adolescenti non sa e non fa.

Comunque, anche se Ask.fm non fa parte del programma *Safe Harbor*, essendo la Lettonia un paese membro dell'Unione Europea dal 2004, ha dichiarato la sua totale disponibilità a collaborare con le autorità per rintracciare i colpevoli di cyberbullismo nei casi gravi come quello di Hannah Smith, fornendo le informazioni necessarie per risalire ad essi. Inizialmente, però, le posizioni dei due fratelli fondatori del social network erano radicalmente diverse, cioè attribuivano l'insorgere di "incidenti" alla mancanza di controllo da parte dei genitori, deresponsabilizzando totalmente lo strumento e non accennando minimamente al coinvolgimento della piattaforma nelle indagini. Più di recente, invece, oltre a mostrare un atteggiamento collaborativo, hanno anche sottolineato la disponibilità del team di moderatori a far sì che la

piattaforma resti un luogo sicuro, anche se il quotidiano Le Monde[219] ha scoperto che si tratta di circa cinquanta persone che devono vigilare su milioni di utenti in oltre 150 lingue[220], per un totale di trenta milioni di domande al giorno.

Insomma, il quadro è assolutamente insufficiente dal punto di vista delle tutele offerte contro il cyberbullismo e non più roseo è il *frame* che emerge analizzando direttamente le *policies* del sito.

All'interno dei suoi Termini di Utilizzo, infatti, si trova scritto che: «1. Non è consentito registrarsi su Ask.fm o utilizzare il sito ai minori di 13 anni. Si prega di non mentire sull'età. Iscrivendosi come membro, l'utente s'impegna a fornire ad Ask.fm informazioni veritiere e accurate. Nel caso in cui l'utente fornisca delle informazioni false, ci riserviamo il diritto di sospendere o rimuovere il suo account. 2. L'utente è il solo responsabile di tutto ciò che pubblica o dice su Ask.fm (non noi). Non monitoriamo tutto ciò che accade sul sito di Ask.fm perché impossibile. Non siamo responsabili di ciò che gli utenti pubblicano sul sito. Tuttavia, a volte inviamo notifiche quando le persone usano un linguaggio scurrile o parolacce, che non sono accettate sul nostro sito. Diamo anche seguito a tutte le denunce che riceviamo da parte di chi segnala una violazione di questi Termini e/o delle nostre politiche, soprattutto quelle riguardanti azioni che potrebbero aver sconvolto, angosciato o impaurito l'utente. Quindi, qualora l'utente pubblichi qualcosa che riteniamo inappropriato o inaccettabile, potremmo rimuoverlo dal sito e/o, dove possibile, bloccare il suo futuro accesso a quest'ultimo»[221]. Ma com'è possibile bloccare qualcuno se questo qualcuno non è registrato? Questa opzione rende totalmente inutile la previsione per cui: «Se l'utente decide di non accettare i Termini, allora non dovrà accedere o utilizzare il sito. Continuando ad utilizzare o accedere al sito di Ask.fm, l'utente dimostra di accettare i presenti Termini»[222]. Infatti, pur riconoscendo la deresponsabilizzazione degli ISPs derivante dalla direttiva sul commercio elettronico 2000/31/CE, non è possibile che un adolescente non registrato

[219] L. Belot, *Ask.fm affole les ados en quête de cyber-frissons*, Le Monde, 3/6/2013.

[220] V. Fraschetti, *"Fermate Ask, è il regno dei cyber bulli". Rivolta contro il social network dei ragazzini*, 9 agosto 2013 in www.repubblica.it.

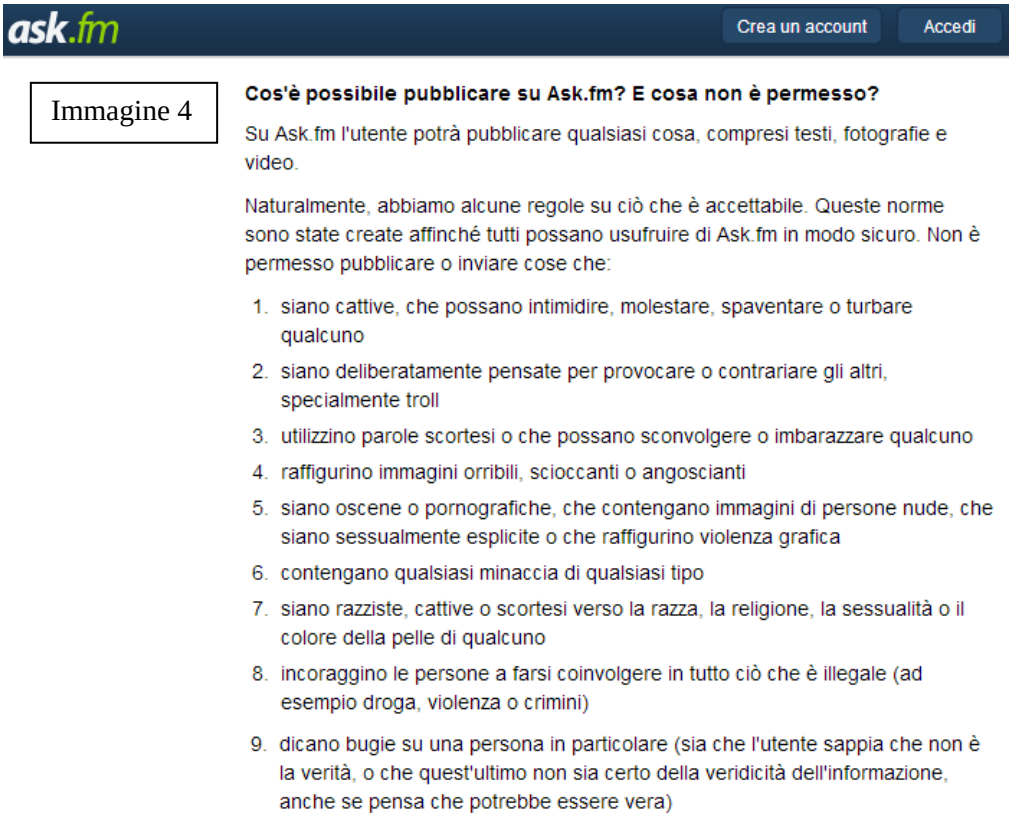
[221] ask.fm/about/policy/terms-of-service.

[222] Ibid.

possa insultare, offendere e minacciare il profilo di un altro utente senza che vi sia la possibilità di impedirgli di farlo proprio perché le prepotenze vengono eseguite in forma anonima senza possedere un account. Ovviamente ci si potrebbe rivolgere alle autorità competenti, ma a livello di risoluzione immediata della controversia (segnalazione-risposta da parte dei moderatori) non vi sono gli stessi strumenti messi a disposizione da Twitter che, basandosi su meccanismi simili a quelli di Ask.fm, è consapevole della potenziale unilateralità dei rapporti tra *followers* che comunque hanno l'obbligo di registrarsi.

La sezione relativa ai Termini di Utilizzo prosegue con l'elencazione delle pubblicazioni vietate sul sito (vedi Immagine 4), ma rimangono per esse gli stessi dubbi sovra esposti cui si aggiunge la totale assenza di riferimenti all'ammissibilità della satira o della libera manifestazione del pensiero, nonostante, come si diceva in precedenza, Ilja Terebin nella sua lettera parli di condivisione di idee, pensieri e sentimenti:

Immagine 4



Soltanto nella parte relativa alla "Cessazione di utilizzo" il sito dichiara che: «A volte le persone pubblicano cose che non sono ammesse sul sito. Quando pensiamo di trovarci davanti a uno di questi utenti, ci riserviamo il diritto in qualsiasi momento

(senza previo avviso) di: a. sospendere/rimuovere l'iscrizione (dove applicabile) e il diritto di accedere e/o utilizzare Ask.fm o di inoltrare qualsiasi contenuto su Ask.fm; b. fare qualsiasi altra cosa in nostro potere o controllo per far rispettare i nostri termini (tra cui bloccare indirizzi IP specifici o contattare la polizia)»[223]. Tuttavia rimane assolutamente indefinito se i provvedimenti della categoria "b." siano attuabili anche nei confronti di chi non ha un profilo registrato, rimanendo comunque in contraddizione con quanto più volte dichiarato, cioè che «l'utente è l'unico responsabile di tutto ciò che scrive o pubblica sul sito» e che «non saremo responsabili per eventuali danni di qualsiasi tipo derivanti dall'utilizzo del sito web di Ask.fm, compresi, ma senza limitarsi a, danni diretti, indiretti, incidentali, punitivi e consequenziali»[224].

Nella sezione riguardante le "Politiche di abuso"[225], poi, vengono elencate le «principali azioni che non sono permesse all'utente», collocando al primo posto il bullismo e ribadendo nuovamente, come nella parte "Cessazione di utilizzo", che: «Qualora […] un utente stia compiendo una qualsiasi di queste azioni (o qualcosa simile ad esse) su Ask.fm, prenderemo tutte le misure del caso per fermarlo e, se necessario, proveremo a bloccare la persona in questione sul nostro sito web. Qualsiasi comportamento di questo genere semplicemente non sarà tollerato»[226].

Ancora una volta viene sottolineata l'indeterminatezza degli interventi effettivi, non soltanto per quanto riguarda le azioni dirette ad utenti anonimi o a quelli con profilo visibile, ma soprattutto rispetto a coloro che non hanno un account, tant'è che l'espressione utilizzata è «proveremo a bloccare».

A questo punto, però, nella parte relativa al "Blocco utenti"[227], emerge un primo chiarimento per quanto riguarda la segnalazione di un utente che mette in atto uno dei comportamenti vietati da Ask.fm: «[…] è sufficiente cliccare sul pulsante Blocca utente. Questo impedirà all'utente in questione di inviarti altre domande qualora

[223] Ibid.

[224] Ibid.

[225] ask.fm/about/policy/abuse-policy.

[226] Ibid.

[227] Ibid.

accedesse ad Ask.fm dall'indirizzo IP usato originariamente. Anche se è impossibile per noi impedire agli utenti di accedere al sito da indirizzi IP diversi, il pulsante "Blocca utente" potrà limitare la loro capacità di farti domande, qualora non desiderassi essere contattato da loro»[228]. Dunque, da ciò si evince che l'intervento della piattaforma può determinare l'impedimento ad un determinato IP di effettuare l'accesso e di utilizzare le funzioni offerte dal sito, ma, ancora una volta, non è chiaro se ciò possa avvenire per coloro che hanno un profilo registrato o anche per quelli che accedono alla pagina senza avere un account. In questa seconda ipotesi, infatti, si avrebbe una maggior tutela delle vittime di abusi da parte dei cyberbulli e sarebbe coerente con quanto dichiarato nella parte relativa alla "Cessazione di utilizzo", quando il sito dichiara di voler agire in qualsiasi modo per far sì che i termini d'uso vengano rispettati «tra cui bloccare indirizzi IP specifici o contattare la polizia».

Tuttavia, a discapito di quanto potrebbe emergere mantenendo valida questa interpretazione, nella sezione relativa all' "Informativa sulla Privacy" viene spiegato chiaramente che Ask.fm non raccoglie informazioni sui membri non registrati, anche se sarebbe «in grado di monitorare il loro indirizzo IP »[229]. Infatti, continua il sito, «Se un utente dovesse visitarci senza essere membro, installeremo i *cookies* sul browser del suo computer (o di qualsiasi altro dispositivo) per la durata della visita»[230]. Dunque, stando a ciò, pur potendo intervenire contro coloro che non hanno un profilo registrato, la piattaforma non interverrà se non per ordine del tribunale in modo da reprimere gli abusi previsti dalla legge statale. Infatti, proprio nella sezione relativa alla privacy, Ask.fm precisa che, come risultato di queste richieste, il social network è tenuto «a dare alla polizia o ad altri organismi di regolamentazione, le informazioni personali dell'utente e tutto ciò che quest'ultimo ha pubblicato».

Tornando alla sezione relativa ai "Termini di Utilizzo", la conclusione enuncia che: «Per essere chiari, niente in questi Termini eviterà che Ask.fm sia responsabile di

[228] Ibid.

[229] ask.fm/about/policy/privacy-policy.

[230] Ibid.

tutto ciò per cui la legge prevede che sia ritenuta responsabile»[231]. Quindi, di fatto, la piattaforma non si pone limiti di responsabilità. Il problema, però, è che le leggi sono diverse a seconda dei paesi e non è detto che esse siano fornite di previsioni relative al cyberbullismo, pertanto per disciplinare le controversie che sorgono su siti come questo bisognerebbe avere specifiche disposizioni legislative, come auspicato nella petizione che circola in Gran Bretagna. Tant'è che la sezione si conclude così: «I presenti Termini e qualsiasi controversia o reclamo derivante da, o connesso a essi e al loro contenuto (comprese le controversie non contrattuali o i reclami) saranno regolati e interpretati in conformità alla legge lettone e saranno soggetti alla giurisdizione non esclusiva dei tribunali della Lettonia»[232]. Perciò il diritto lettone viene applicato in prima istanza, ma è ammesso l'intervento di "altri" giudici nei casi che coinvolgono utenti di altre nazioni, il che è coerente con la politica di Ask.fm di collaborare con le autorità competenti nei casi più gravi, poiché esse non necessariamente saranno di nazionalità lettone - come nel caso britannico di Hannah Smith (vedi *infra* pag. 178).

Nella pagina dedicata alle FAQs dei genitori[233], infatti, alla domanda relativa all'intervento del sito nei casi che prevedono un coinvolgimento legale, la piattaforma risponde che essa è ben disposta a collaborare qualora si sia rispettato il percorso di segnalazione corretto che va dalla polizia nazionale a quella lettone[234].

Comunque, pur non essendo effettivamente chiaro se si possa o meno agire sugli utenti senza profilo registrato, per «Limitare l'abuso di Ask.fm»[235] i gestori hanno «istituito filtri automatici per parole e frasi maleducate/offensive che non sono ammesse su Ask.fm»[236] grazie ai quali lo staff viene automaticamente avvisato e, in questo modo, può rimuovere suddetti contenuti abusivi. In questo caso, come già

[231] ask.fm/about/policy/terms-of-service.

[232] Ibid.

[233] ask.fm/about/safety/faqs-for-parents.

[234] «What do you do with legal requests? We take all legal requests extremely seriously provided they have gone through the correct reporting route from your national police to the Latvian police», in ask.fm/about/safety/faqs-for-parents.

[235] ask.fm/about/policy/abuse-policy.

[236] ask.fm/about/policy/abuse-policy.

accennato poco fa, tale previsione rimane di dubbia gestibilità se si considera che i moderatori sono circa cinquanta e si trovano a dover gestire non soltanto i meccanismi di filtraggio, ma anche le segnalazioni di altri due tipi, relative sia ai report di carattere generale sia a quelli dei contenuti, disponibili entrambi tanto per gli utenti registrati quanto per quelli senza un account. Innanzitutto, infatti, è possibile accedere alla "Pagina di Feedback" in cui si può inserire la propria e-mail ed allegarvi un messaggio (vedi Immagine 5) che verrà recapitato ai moderatori del sito, contenente qualsiasi tipo di lamentela o notifica relativa a questioni di molestie, minacce, atti di bullismo ecc… anche facendo riferimento al fatto che essi provengono da un utente che si mantiene anonimo e del quale, quindi, si è impossibilitati a bloccare il profilo - qualora ne abbia uno:

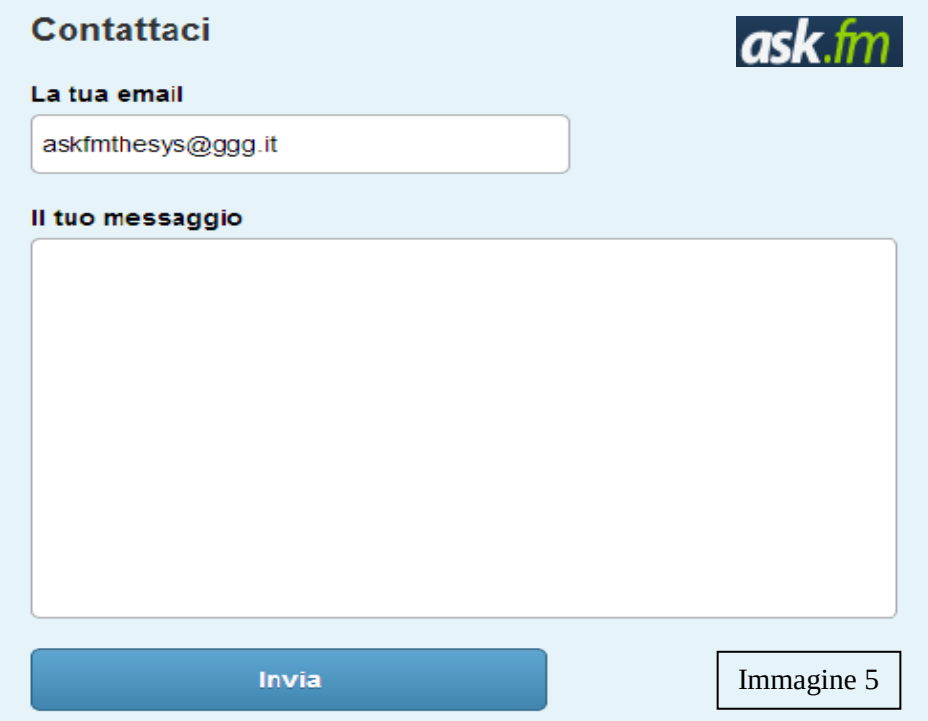


Immagine 5

In secondo luogo, invece, relativamente ai contenuti, si può agire direttamente dai box in cui sono elencate le domande e le risposte (siano esse proprie dell'utente o appartenenti ad un altro profilo), attraverso il click su un *flag* situato sulla destra. Questo meccanismo consente di segnalare la notizia come discorso denigratorio, come spam o frode, come contenuto che incita all'odio e/o alla violenza e, infine, come contenuto sessualmente esplicito.

Incrociando le disposizioni delle *policies*, insomma, emerge un quadro piuttosto ambiguo, di un ISP che non si prende la responsabilità sociale che gli spetta in quanto azienda che lavora per gli utenti e con gli utenti per offrire loro dei servizi. Inoltre, leggendo le diverse previsioni contenute nelle sezioni del sito (Termini di Utilizzo, Privacy, Politiche di Abuso ecc…) in realtà non emerge un quadro univoco, coerente e ben collegato, piuttosto si ha l'impressione che non vi sia un intervento tale da poter effettivamente porre fine alle prepotenze dei cyberbulli. Infatti, soltanto attraverso una comparazione delle diverse sezioni si riesce a comprendere quale sia effettivamente la posizione del social network relativamente alla tutela delle vittime di bullismo elettronico, mentre ben più chiara era quella di Facebook, seguita dalle previsioni di Twitter.

Non a caso, pochi giorni dopo il suicidio di Hannah Smith, i due fondatori del sito hanno avviato un'indagine auto valutativa condotta dallo studio legale Mishcon de Reya per vagliare l'effettivo livello di sicurezza del sito, sia dal punto di vista delle *policies* che da quello degli interventi concreti. Nel comunicato stampa che annunciava suddetta decisione[237] è stato garantito un successivo annuncio - previsto per la settimana successiva - di tutte le conclusioni e raccomandazioni realizzate dal team di avvocati e di specialisti di comunicazione.

Così, il 19 agosto 2013, a seguito dei risultati emersi dall'indagine, i rappresentanti del sito hanno dichiarato di voler cambiare le *policies* relative alle tre aree principali: *reporting*, moderazione e registrazione. Tra gli obiettivi ci sarebbe quello di rispondere alle segnalazioni su comportamenti abusivi entro 24 ore, grazie al reclutamento di più moderatori che sorveglino le attività del sito (funzione di filtraggio automatico) e i report degli utenti. A ciò, inoltre, si aggiunge il proposito di introdurre un "*bullying*/*harassment button*", cioè un pulsante di segnalazione appositamente dedicato al cyberbullismo e alle molestie.

I fratelli Terebin allora auspicavano che entro i successivi dodici mesi venissero introdotti i cambiamenti sovra descritti, inclusa l'assunzione di un responsabile della sicurezza a tempo pieno che si potesse assumere la responsabilità per la moderazione nel sito. Ebbene, come già spiegato poco fa, ad oggi è presente il "pulsante di segnalazione" sottoforma di *flag*, che consente di contrassegnare i contenuti che

[237] A. Rudd, *Hannah Smith suicide: Ask.fm hire law firm to carry out independent audit of safety features on site*, 9 agosto 2013, in www.mirror.co.uk.

costituiscono denigrazione, incitamento all'odio, spam ecc… ma non vi è traccia di espressioni quali "bullismo" e "molestie". Inoltre, nonostante i gestori del social network avessero annunciato ulteriori sforzi per incoraggiare gli utenti a registrarsi, tra cui la registrazione di indirizzi e-mail ed IP degli utenti, rimangono le previsioni ivi descritte relative all'assenza di monitoraggio se non per il tempo di mantenimento dei *cookies*, che comunque possono essere disattivati dagli utenti impedendo loro di fruire di alcune delle attività messe a disposizione dal sito. Inoltre, seppur vero che all'accesso viene immediatamente chiesto di registrarsi, senza possibilità di cercare gli utenti che già hanno un account così da incoraggiare l'iscrizione, Ask.fm consente di risalire ai diversi profili mediante un qualsiasi motore di ricerca. Infatti, basta conoscere il nome con cui la persona si è registrata e cercarlo su Google, accostandolo al nome del sito (ad es.: "@nomeutente ask fm") - procedura che su Facebook può essere impedita disabilitando l'opzione relativa alla possibilità dei motori di ricerca di rimandare al proprio diario.

Dunque, rimangono ancora piuttosto scarse le previsioni a tutela delle vittime di cyberbullismo, nonostante si attendesse per la primavera 2014 un nuovo sito rivolto ai genitori, che avrebbe dovuto informazioni sulle politiche di sicurezza di Ask.fm, similmente a quanto già attuato da Facebook nel maggio 2014 (vedi *supra* pag. 116). Questo ritardo nell'attuazione di *policies* più adatte a garantire la sicurezza degli utenti è da attribuirsi senz'altro alla minore pubblicità di questo social network rispetto agli altri due già analizzati. Infatti, come dichiarato dallo stesso padre di Hannah Smith, la maggior parte dei genitori neanche immagina l'esistenza di questo tipo di piattaforme che consentono una tale libertà di espressione, tanto da trasformarla in abuso. Ancora una volta, dunque, si tratta di coordinare l'intervento dell'ISP con quello delle forze dell'ordine, mettendo a disposizione, parallelamente, materiali che fungano da ausilio agli insegnanti e/o ai genitori, assieme ad una solida educazione relativa alle interazioni sui social network.

Comunque, oltre ai rischi derivanti da scarsi meccanismi di tutela, Ask.fm fa riemergere anche la già nota questione della necessità di adottare leggi che configurino il cyberbullismo come reato, in modo da rendere più efficiente la collaborazione tra i *providers* e i tribunali. Non serve, dunque, abolire l'anonimato, poiché la soluzione risiede nell'introdurre processi efficaci di autenticazione da parte

della piattaforma per coloro che commettono abusi senza possedere un profilo registrato, in modo da poter risolvere le controversie anche senza dover necessariamente ricorrere all'intervento delle forze dell'ordine. Oppure, sarebbe ancor più saggio consentire di nascondere la propria identità soltanto a quegli utenti che posseggono un account, il che garantirebbe maggiore coerenza con la responsabilità sociale di cui si è parlato spesso. A rafforzare questo quadro, poi, dovrebbe esservi una maggiore possibilità di controllo da parte del social network che si sostanzia nella definizione di *policies* più chiare, messe in atto da un vasto team di esperti che siano in grado di monitorare effettivamente le segnalazioni da parte degli utenti, proprio in virtù delle caratteristiche assolutamente peculiari del sito (usabilità senza profilo, *followers* anonimi ecc…) nonché nell'attuazione di modifiche alle impostazioni sulla privacy previste di default per i minori, così da rendere effettivamente «Ask.fm un luogo divertente e amichevole per tutti»[238].

In conclusione, se si volesse riflettere in generale sulla pluralità di social network oggi disponibili, da quanto detto in questo capitolo sembra chiaro che molti di essi necessitano di numerose migliorie a livello di *policies* e di interventi successivi, fermo restando che la tutela assoluta contro il cyberbullismo non è possibile, giacché la rete è e rimane uno spazio libero. Ciò, tuttavia, non esclude meccanismi di prevenzione realizzabili con un'educazione all'uso responsabile delle tecnologie di comunicazione, unitamente ad una disciplina legislativa funzionale alla repressione degli abusi da parte dei cyberbulli e applicata anche grazie all'assunzione di una "responsabilità sociale" da parte dei *providers*. Purtroppo, o per fortuna, infatti, i reati compiuti sul web ai danni dei minori non sono soltanto una responsabilità degli organi giurisdizionali o di quelli di polizia, bensì coinvolgono attivamente anche le famiglie e le scuole, ma soprattutto gli Internet Service Providers, che dovrebbero essere in prima linea nel garantire la sicurezza dei più giovani.

[238] ask.fm/about/policy/dos-and-donts.

Approfondimento 3a:

Atti di bullismo in onda su YouTube

Se fino ad ora si è descritto il cyberbullismo come fenomeno di persecuzioni, calunnie e prepotenze perpetrate tramite i social network e i nuovi strumenti di comunicazione, è bene precisare che queste configurazioni non esauriscono il panorama attuale delle sue manifestazioni.

Da qualche tempo, infatti, si è via via diffusa una nuova tipologia di molestia, resa possibile dalla creazione, nel 2005, della piattaforma di condivisione e di visualizzazione di video più diffusa al mondo: YouTube.

Esso è stato preceduto ed ha costituito l'evoluzione di Google Video, un servizio gratuito di Google per il caricamento dei filmati sul server di Google, attivo fino all'aprile 2011, oggi disponibile per la sola ricerca di materiale audiovisivo.

Tornando a YouTube, si tratta di un sito di *videosharing*, di proprietà della Google Inc., che non richiede la creazione di un profilo per accedervi e riprodurne i contenuti, ricercabili sia dalla sua *Home Page* che dalla stessa pagina iniziale di Google (nella sezione "video") o tramite qualsiasi altro motore di ricerca.

Chiaramente, per usufruire di alcune funzioni, quali l'*upload* o i commenti ai video, è necessario registrarsi ed accedere con il proprio account così da poter creare un "Canale" personale, ma la condivisione su altri social network (Facebook, Twitter, Pinterest ecc…) e la fruizione personale rimangono svincolate dal possesso di un profilo.

In questo contesto, come si diceva pocanzi, è nata una nuova tipologia di cyberbullismo, che consiste nella ripresa di atti di bullismo tradizionalmente intesi (prese in giro, violenze, minacce ecc…) che poi vengono pubblicati su YouTube dal "regista", dal bullo o da terzi, con profilo personale autentico o con uno creato *ad hoc*.

Un simile fenomeno richiede la riflessione su due temi già affrontati in questo lavoro. In primis, è importante soffermarsi sulle *policies* della piattaforma per comprendere se e in che modo essa previene e reprime questo tipo di illeciti.

In secondo luogo, invece, è necessario riflettere sul problema della responsabilità degli Internet Service Providers per concorso nel reato di diffamazione, dal momento

che le piattaforme di *videosharing* non soltanto consentono l'atto di bullismo elettronico, cioè l'*upload* con fini denigratori, ma soprattutto mandano in onda il fatto stesso, agendo da cassa di risonanza rispetto all'umiliazione subita dalla vittima. Ciò significa che anche un solo file può generare danni psicologici e creare conseguenze notevoli per chi è oggetto delle prepotenze, poiché il link può essere condiviso da chiunque e visualizzato in qualsiasi momento. Tutto ciò ovviamente, non può prescindere dal considerare che potrebbero attivarsi provvedimenti interni alle scuole o intrapresi dagli stessi ISPs per fronteggiare la comparsa dei video.

In tal senso, dunque, si è deciso di analizzare le condizioni d'uso valide in Italia, così da comprendere i meccanismi di funzionamento di YouTube rispetto al fenomeno del cyberbullismo.

Successivamente, poi, si passerà all'analisi di alcuni casi concreti, con le relative giurisprudenze - quando disponibili - che dimostrano in che modo si è deciso di risolvere la questione della responsabilità del *provider* che fornisce contenuti video e in quali casi essa è stata sostituita da un intervento delle forze dell'ordine o del personale scolastico.

Si ritiene utile iniziare dal fatto che i Termini di Utilizzo della piattaforma siano introdotti così: «Il contratto tra l'utente e YouTube è costituito da (A) i termini e le condizioni indicati nel presente documento; (B) la Privacy Policy di YouTube […] e (C) Le Linee Guida della Community di YouTube[…] (complessivamente definiti i "Termini")»[239]. Dunque, le *policies* del sito si articolano in tre diverse sezioni, fermo restando che: «L'utente riconosce ed accetta di essere l'unico responsabile dei propri Contenuti e delle conseguenze del loro caricamento online o pubblicazione. YouTube non avalla Contenuti o opinioni, raccomandazioni o consigli in essi contenuti, e declina espressamente ogni e qualsiasi responsabilità in relazione ai Contenuti»[240]. Così, come già visto per i tre social network analizzati in precedenza, anche in questo caso vi è da parte del provider un'autoesclusione dal coinvolgimento nelle responsabilità degli utenti che devono rispettare diverse disposizioni al fine di poter utilizzare correttamente la piattaforma di *videosharing*. Infatti, «la condotta dell'utente sul Sito web si dovrà conformare (e il contenuto di tutti i Contenuti si

[239] www.youtube.com/t/terms.

[240] Ibid.

dovrà conformare) alle Linee Guida della Community di YouTube» il quale «nel momento in cui dovesse venire a conoscenza di qualsiasi potenziale violazione dei presenti Termini, […] si riserva il diritto (ma non ha l'obbligo) di decidere se i Contenuti si conformino con i requisiti previsti nei presenti Termini e potrà rimuovere tali Contenuti e/o inibire l'accesso di un utente al caricamento dei Contenuti che siano in violazione dei presenti Termini in qualsiasi momento, senza preavviso ed a sua esclusiva discrezione». Insomma, alla responsabilità totale a carico dell'utente si affianca la gestione arbitraria degli illeciti da parte del sito poiché esso si assume la licenza gratuita di riprodurre i contenuti caricati e pertanto ha a disposizione il potere di disciplinarne la presenza e la rimozione, per questo dichiara: «Quando un video è segnalato come non appropriato, lo passiamo in rassegna per stabilire se vìoli i nostri Termini e condizioni d'utilizzo: i video segnalati non vengono automaticamente rimossi dal sistema. Se rimuoviamo un tuo video dopo averlo esaminato, puoi stare certo che l'abbiamo fatto intenzionalmente»[241]. Parimenti, la piattaforma potrà sospendere la fornitura di servizi all'utente o eliminare i video da esso caricati se viola una delle disposizioni dei "Termini" o qualora sia la legge a richiederlo. Infatti, nonostante YouTube si dichiari non responsabile per i contenuti caricati, in realtà esso «in caso di dolo o colpa grave […] e per perdite che non possono essere legittimamente escluse o limitate ai sensi della legge applicabile»[242] diviene responsabile per i reati previsti dalle norme vigenti in Italia e, pertanto, dovrà rispondere agli ordini giudiziari che ne derivano.

Nelle "Norme della Community", poi, viene stabilito che nei video «non è permessa alcuna forma di violenza evidente o gratuita» e, anche se YouTube incoraggia la libera manifestazione del pensiero, «è vietato l'incitamento all'odio (linguaggio che attacchi o umilii un gruppo in base a razza o origine etnica, religione, disabilità/invalidità, sesso, età, condizione sociale o orientamento sessuale/identità di genere)», così come lo sono «minacce, molestie, violazioni della privacy o la rivelazione di informazioni personali di altri membri»[243]. In ciascuna di queste

[241] www.youtube.com/t/community_guidelines?hl=it&gl=IT.

[242] www.youtube.com/t/terms.

[243] www.youtube.com/t/community_guidelines?hl=it&gl=IT.

condizioni, dunque, ai sensi di quanto dichiarato nei Termini di Servizio precedentemente analizzati, YouTube ha il diritto di rimuovere i contenuti che violino suddette norme e/o di impedire all'utente di accedere ai servizi della piattaforma.

In questo senso, già dalle disposizioni generali emerge un quadro di tutela nei confronti di coloro che divengono vittime dei cyberbulli mediante la pubblicazione di video che testimoniano atti di discriminazione per le categorie previste o di violenza nei confronti di qualsiasi destinatario.

Detto ciò, in caso vi siano problemi derivanti da un comportamento illecito, è possibile contattare i moderatori del sito passando attraverso il "Centro Norme e Sicurezza"[244], che consente di capire quali siano concretamente gli abusi e in che modo essi possano essere segnalati così da applicare le disposizioni previste dal sito.

Le sezioni del Centro sono in tutto tre, riguardanti le norme, la sicurezza e i rapporti, e rimandano alla guida fornita da Google per i servizi ad esso affiliati (Maps, Chrome, Gmail ecc…) tra cui, ovviamente, vi è anche YouTube e per il quale vengono stabilite specifiche previsioni riguardo al cyberbullismo e gli altri fenomeni che potrebbero connettersi ad esso (violazione della privacy, minacce, incitamento all'odio, molestie, violenza e diffamazione).

Innanzitutto, per comprendere cosa è consentito e cosa invece non lo è, si può visitare la sezione "Centro norme"[245]. Al suo interno sono contenute le *policies* relative a diversi argomenti del tutto o in parte connessi al bullismo elettronico perpetrato nelle forme che si descrivevano poco fa. In primo luogo, infatti, vi è l'ipotesi di violazione della privacy, ad esempio, qualora un utente carichi un video senza il consenso della persona ripresa, ferma restando la necessità «che un individuo sia identificabile in maniera univoca»[246]. In tal caso, «YouTube offre all'autore del caricamento l'opportunità di rimuovere o modificare le informazioni private nel suo video» entro 48 ore, attraverso «una notifica relativa alla potenziale violazione»[247]. Se a seguito dell'arco di tempo previsto «la causa della potenziale violazione della

[244] www.youtube.com/yt/policyandsafety/it.

[245] www.youtube.com/yt/policyandsafety/it/policy.html.

[246] support.google.com/youtube/answer/2801895.

[247] www.youtube.com/t/privacy_guidelines.

privacy è ancora presente sul sito […] il reclamo verrà esaminato dal team di YouTube»[248]. La segnalazione può essere presentata solo dall'interessato giacché per effettuarla è necessario accedere con il proprio account, a meno che egli non sia in grado di utilizzare un computer o qualora si tratti di «una persona vulnerabile». Infatti, in quest'ultimo caso, può intervenire anche «il genitore o il tutore legale»[249], ferma restando la possibilità per chiunque di farsi rappresentare da un legale, che in quanto tale può agire per conto del suo cliente.

Comunque, per effettuare il cd. "reclamo per la violazione della privacy" è sufficiente seguire i sei passaggi previsti nell'omonimo modulo[250] disponibile nella terza sezione del Centro Norme e Sicurezza, chiamata "Centro rapporti"[251]. Questa scheda è molto interessante poiché inizia i suoi diversi *step* assimilando alla violazione della privacy tutti i comportamenti molesti, che si concretizzano «se qualcuno ti sta rivolgendo degli insulti o sta pubblicando dei video malevoli su di te»[252]. Proprio questa considerazione contiene un rimando diretto alla seconda sezione del Centro, quella relativa alla sicurezza (Centro Sicurezza[253]), nella parte intitolata "Molestie e Cyberbullismo"[254]. L'aspetto di notevole rilevanza è quello per cui si assimila la violazione della privacy al bullismo elettronico, identificandolo come "attacco dannoso" che si sostanzia nei seguenti comportamenti:

«- video, commenti e messaggi offensivi;
- pubblicazione di informazioni personali di altri;
- riprese intenzionali di una persona senza il suo consenso;
- pubblicazione volontaria di contenuti con lo scopo di umiliare qualcuno;
- video o commenti negativi o crudeli riguardanti altri utenti»[255].

---

[248] Ibid.

[249] Ibid.

[250] support.google.com/youtube/answer/142797.

[251] www.youtube.com/yt/policyandsafety/it/reporting.html.

[252] support.google.com/youtube/answer/142797.

[253] support.google.com/youtube/topic/2803240?hl=it&ref_topic=2676378.

[254] support.google.com/youtube/answer/2802268.

[255] Ibid.

Dunque, YouTube prevede espressamente la possibilità di segnalare i contenuti di cui si diceva pocanzi, che stanno iniziando a costituire un vero e proprio strumento d'attacco nelle mani dei cyberbulli, al punto che la piattaforma ha ritenuto necessario assimilare il fenomeno in analisi ad altre configurazioni, ricomprendendolo in un'unica categoria che abbraccia la privacy, le offese e le molestie, così da evidenziare il potenziale raggio di azione degli atti di bullismo elettronico.

A questo punto, dunque, l'utente viene invitato, nella parte a ciò riferita del Centro norme[256] - "Molestie e Cyberbullismo" - a segnalare suddetti episodi e/o a bloccare l'utente che ha caricato il video, poiché «quando un contenuto viola le […] norme sulle molestie, l'utente che ha pubblicato il contenuto riceverà un avvertimento sul proprio account YouTube»[257] secondo le modalità descritte nei Termini di servizio, precisando che «gli account concepiti per molestare un determinato utente o l'intera community saranno chiusi»[258].

Nei casi di molestie e di bullismo, il "Centro Rapporti"[259] consente di segnalare un video, «una serie di video o commenti o un intero account di un utente [cd. Canale]»[260] (cfr. Immagine A). All'interno di questa sezione, YouTube dichiara quanto segue: «Ogni minuto gli utenti caricano su YouTube più di 72 ore di video. Con così tanti contenuti sul sito, sarebbe impossibile controllare tutto. È per questo che ci affidiamo ai membri della community di YouTube affinché segnalino i contenuti che trovano inappropriati. Lo staff di YouTube esamina i video segnalati 24 ore al giorno, sette giorni alla settimana, e i video che violano le Norme della community vengono rimossi dal sito. Ai video che potrebbero essere inappropriati per alcuni degli spettatori più giovani viene applicato un limite di età. I video segnalati non vengono rimossi automaticamente dal sistema di segnalazione. Se un video non viola le nostre linee guida, non importa quante segnalazioni riceveremo, il video resterà sul sito».

[256] support.google.com/youtube/answer/2801920?hl=it&rd=1.

[257] Ibid.

[258] Ibid.

[259] support.google.com/youtube/topic/2803138?hl=it&ref_topic=2676378.

[260] support.google.com/youtube/answer/2801920?hl=it&rd=1.

Immagine A

Nonostante le previsioni relative alla violazione della privacy siano di per sé esaustive rispetto al fenomeno del cyberbullismo e benché suddetti meccanismi di segnalazione del Centro rapporti siano applicabili anche ai casi di minacce, incitamento all'odio, contenuti violenti, espliciti, dannosi o pericolosi, esistono altre disposizioni nel Centro norme, relative proprio a queste fattispecie, che possono essere applicate agli abusi connessi al bullismo elettronico.

Oltre ad avere il potere di rimuovere «i video che contengono gravi minacce di danni fisici»[261], infatti, YouTube precisa che, pur incoraggiando la libertà di espressione e rispettando i «punti di vista impopolari», non è consentito l'incitamento all'odio, inteso come quel tipo di contenuti che inneggiano alla violenza o al disprezzo «nei confronti di individui o gruppi sulla base di determinati attributi, come ad esempio: razza o etnia, religione, disabilità, sesso, età, orientamento/identità sessuale». Questa previsione è interessante poiché molto spesso gli episodi di cyberbullismo si

[261] support.google.com/youtube/answer/2801927?hl=it&ref_topic=2803176.

sostanziano nel caricamento di video che ritraggono persone affette dalla sindrome di Down (cfr. caso Google-Vividown pag. 159) o di etnie diverse da quella del bullo che vengono insultate e malmenate di fronte alla telecamera. Quest'ultimo caso si identifica proprio in ciò che è avvenuto a Grosseto, sulle cui mura è stato girato un video, caricato su YouTube il 17 febbraio 2013, in cui un gruppo di adolescenti si accanisce su una ragazza di etnia diversa, insultandola per il colore della sua pelle e malmenandola finché essa riesce finalmente a scappare.

I materiali erano stati rimossi dal sito di *videosharing* il 20 febbraio, mentre la la *task force* della Polizia di Stato "Codice rosa" (contro la violenza sulle donne) si era attivata per ricercare i colpevoli. Si trattava di bullismo a sfondo razzista tramutatosi, nel tempo dell'*upload*, anche in cyberbullismo poiché la diffusione in rete delle riprese era finalizzata chiaramente ad esaltare le ingiurie e le violenze contro "la negra" che "le busca". Nonostante ciò, comunque, il questore di Grosseto, Michele Laratta, aveva dichiarato al Messaggero che non c'era stata alcuna denuncia da parte della vittima poiché la lite era dovuta a "questioni di cuore"[262]. Per le autorità, i commenti razzisti, secondo quanto emerso dopo aver ascoltato la giovane, erano da attribuirsi ai ragazzi che guardavano e riprendevano la scena, ma la ragazza non si era offesa e non li aveva considerati discriminatori.

L'allora ministro dell'Integrazione, Andrea Riccardi, invece, aveva definito il fatto come estremamente grave ed aveva demandato all'UNAR di indagare sulla vicenda, ma nonostante ciò, il caso è stato chiuso ancor prima di essere costruito e il video, pur non presente su YouTube, è ancora disponibile e visibile su molti siti a partire dal quotidiano "Il Tirreno", che ha consentito il rimbalzo del link sulle migliaia di pagine del web.

Nel rapporto redatto nel 2014 da Ipsos Public Affairs per Save the Children Italia Onlus[263], del quale si è fatta più volte menzione in questo lavoro, è emerso che il cyberbullismo avviene ai danni di ragazzi "diversi" per la loro origine etnica nel 43% dei casi, il che si colloca al terzo posto dopo la discriminazione per caratteristiche fisiche (67%) e per l'orientamento sessuale (56%).

[262] www.ilmessaggero.it/primopiano/cronaca/grosseto/notizie/253499.shtml.

[263] Safer Internet Day Study – Il Cyberbullismo, 2014.

Comunque, a prescindere dalle statistiche, è chiaro che l'episodio non rappresenta una semplice bravata, ma si tratta di un atto che, se fosse avvenuto all'interno del cortile, del corridoio o di una classe della scuola sarebbe stato classificato come atto di bullismo tradizionale e i colpevoli sarebbero stati quantomeno ammoniti. Allora viene da chiedersi per quale motivo il bullismo tradizionale ripreso e diffuso sul web non meriti le stesse forme di tutela. Infatti, pur non potendo stabilire immediatamente o con certezza la data di accadimento concreto dell'evento, le sue conseguenze si perpetuano nel tempo grazie alla continua disponibilità del materiale online finché il provider o il giudice non ne dispongono la rimozione.

Sicuramente, questo tipo di avvenimenti differiscono dalle forme di cyberbullismo sinora analizzate, che si sostanziano in atti persecutori e/o intimidatori piuttosto continuativi e che possono essere poi contornate da danno fisico oppure rimanere "semplici" prepotenze telematiche. In questi casi, infatti, è indubbio il danno psicologico - prima ancora che corporeo - ed è per questo che si è più volte sostenuta la necessità di una disposizione legislativa che tuteli le vittime parallelamente all'azione dei *providers* e all'educazione nelle scuole. Tuttavia, non si può restare indifferenti alla questione del bullismo ripreso e postato sulla rete poiché anch'esso dovrebbe costituire un reato, sia che si tratti di parte della strategia messa in atto dal cyberbullo per perseguitare la sua vittima, sia che rappresenti un caso isolato come quello esposto poco fa.

A seguito della vicenda, infatti, la direttrice dei programmi Italia-Europa di Save The Children, Silvia Milano, ha dichiarato: «Di fronte al dilagare di questi episodi, che dimostrano una interconnessione così stretta tra la vita reale e quella "virtuale", né le scuole né le famiglie possono essere lasciate da sole. Abbiamo davanti a noi una sfida educativa dove ogni soggetto, istituzioni comprese, deve giocare la sua parte»[264].

Comunque, tornando a YouTube, il Centro Norme[265] pone l'accento anche sui contenuti violenti o espliciti proprio perché in alcuni casi il materiale caricato dagli utenti potrebbe essere dannoso non soltanto per chi lo visualizza, ma anche per chi ne

[264] *"E la negra se le busca": video choc su Youtube di una rissa tra ragazzine*, 20/02/2013, in www.lanazione.it.

[265] support.google.com/youtube/answer/2802008?hl=it&ref_topic=2803176.

è protagonista. E' chiaro che se si tratta di materiale giornalistico o documentaristico, di spezzoni cinematografici, ma anche di semplici immagini che ritraggono fatti della vita quotidiana, non può esservi limitazione alla libertà di espressione. Per questo vengono applicati limiti di età nella fruizione di alcuni video ed è possibile, come spiegato nel Centro Sicurezza[266], attivare la cd. "modalità di protezione" cioè «un'impostazione attivabile dall'utente per escludere potenziali contenuti sgradevoli»[267] che preferisce non visualizzare o che vuole evitare di far trovare «per caso da altri membri della famiglia durante l'utilizzo di YouTube». Infatti, in questi casi la piattaforma suggerisce «di pubblicare più informazioni possibili nel titolo e nei metadati per rendere gli spettatori consapevoli di quello che stanno per vedere»[268]. Tutto questo, però, non dovrebbe costituire in alcun modo uno strumento dietro cui mascherare i video che raffigurano atti di bullismo, poiché in questo caso si tratterebbe di un illecito che si rifà a quanto precedentemente visto in relazione alla violazione della privacy. Inoltre, non può considerarsi libera manifestazione del pensiero il caricamento di riprese contenenti violenze fisiche e verbali ad un minore, siano esse relative alle origini etniche della vittima o a qualunque altro tipo di caratteristica che la connota.

A tal proposito, infatti, il Centro Norme, fermi restando gli scopi educativi, documentaristici, scientifici o artistici, vieta «i contenuti concepiti per incitare alla violenza o incoraggiare attività pericolose o illegali che comportano il rischio di gravi infortuni o di morte»[269] così come «i video che istigano altre persone a commettere atti di violenza sono severamente proibiti su YouTube»[270]. In quest'ultimo caso, infatti, se il video «istiga altre persone a commettere azioni violente o contiene minacce di azioni violente nei confronti di altre persone sarà rimosso dal sito»[271]. Tutto ciò, ovviamente, è in gran parte ricollegabile al caso in cui un atto di bullismo venga ripreso e postato sulla piattaforma qualora esso contenga

[266] support.google.com/youtube/answer/174084.

[267] Ibid.

[268] Ibid.

[269] support.google.com/youtube/answer/2801964?hl=it&ref_topic=2803176.

[270] Ibid.

[271] Ibid.

gli incoraggiamenti di cui sopra, anche perché, come dichiarato dagli stessi moderatori del sito, essi sono «molto attenti ai contenuti pericolosi o dannosi che coinvolgono i minorenni»[272].

Un altro aspetto estremamente interessante del Centro Norme è che, nella parte in cui esso si riferisce alle previsioni "legali"[273], si fa riferimento alla diffamazione e alla possibilità per l'utente e per il suo legale di segnalare i contenuti denigratori attraverso un apposito modulo da compilare online[274], diverso da quello previsto per la violazione della privacy ed utilizzabile soltanto dal diretto interessato o dal suo avvocato, ma anch'esso riconducibile al fenomeno del cyberbullismo. Infatti, nonostante il primo suggerimento in caso di «molestie, violenza esplicita o azioni dannose o pericolose» sia quello di fare click sugli appositi pulsanti di segnalazione illustrati poco fa (cfr. Immagine A), è possibile procedere al riempimento del modulo, fermo restando che vi è «la possibilità che YouTube invii il reclamo legale a Chilling Effects Clearinghouse». Si tratta di un'organizzazione statunitense composta da diversi studenti e professori di giurisprudenza che raccolgono e analizzano i reclami legali derivanti dalle attività in rete per aiutare gli utenti a conoscere i propri diritti e a capire la legge. In realtà, i report possono essere presentati anche dai *providers* - oltre che dalle persone - ed hanno tra gli scopi principali non solo la tutela della proprietà intellettuale, ma soprattutto il bilanciamento di due importanti diritti: quello di esercitare la libertà di parola e, al tempo stesso, quello di essere protetti da attacchi non veritieri sulla reputazione, agendo prima che la querela (o la minaccia di querela) per diffamazione diventi uno strumento per limitare anche le osservazioni legittime postate in rete.

A tal proposito, tenendo presente tutto ciò che è stato spiegato relativamente al cd. *false statements of fact* (vedi *supra* pag. 21) e alle previsioni di esclusione di responsabilità degli ISPs negli Stati Uniti (vedi *supra* pag. 48), il sito dell'organizzazione[275] spiega che può esservi diffamazione anche nelle opinioni se in esse vi è "malizia" cioè l'intento, senza giustificazioni o scuse, di commettere un

[272] Ibid.

[273] support.google.com/youtube/answer/2801979?hl=it&ref_topic=2803176.

[274] support.google.com/youtube/answer/140536.

[275] www.chillingeffects.org/defamation.

illecito. Dunque, proprio come nel caso del caricamento dei video che ritraggono la vittima presa di mira e spesso insultata dai bulli, vi è la coscienza e la volontà di fare del male e ferire la vittima attraverso l'*upload*. Quindi, stando a quanto esposto, sembra plausibile per l'utente il ricorso anche al modulo per la diffamazione giacché, implicitamente, le immagini vengono caricate per gli scopi appena descritti.
Affrontato il tema della segnalazione finalizzata alla rimozione dei contenuti, è bene precisare che comunque per motivi legali, le Norme sulla Privacy[276] della piattaforma prevedono la cessione alle autorità dei dati personali nel caso in cui essa sia funzionale a «soddisfare eventuali leggi o norme vigenti, procedimenti legali o richieste governative applicabili» e per «Applicare i Termini di servizio vigenti, compresi gli accertamenti in merito a potenziali violazioni». Dunque, da ciò si evince che, su richiesta delle autorità competenti, gli utenti potranno essere rintracciati grazie alle informazioni di cui è in possesso il provider, mantenendo viva la previsione del *Safe Harbor* relativamente all'utilizzo di suddetti dati, così come dichiarato nella sezione Accordi di Autoregolamentazione[277], disponibile nella guida di Google.

Tutte le previsioni sinora analizzate sono coerenti sia con la deresponsabilizzazione degli ISPs prevista dalla direttiva europea sul commercio elettronico 2000/31/CE, sia, più in generale, con quanto previsto in proposito dalle altre normative (statunitensi, neozelandesi, canadesi ecc…) già esaminate in precedenza. Per altro, le *policies* della piattaforma appaiono piuttosto soddisfacenti anche rispetto alla tutela dei minori nei casi di bullismo e rispettano gli standard di tutela della privacy nel trattamento dei dati personali.
Dunque, ora non rimane che verificare in che modo la giurisprudenza italiana e quella extraeuropea abbia applicato suddette previsioni attraverso l'analisi di diversi casi di cyberbullismo.
Il primo di essi che si intende affrontare costituisce un exemplum a livello internazionale nonostante abbia coinvolto Google Italia e l'associazione Vividown Onlus. Quest'ultima, infatti, il 9 novembre del 2006 aveva denunciato, mediante

[276] www.google.it/intl/it/policies/privacy.

[277] www.google.it/intl/it/policies/privacy/frameworks.

querela, gli amministratori[278] del più celebre provider di ricerca a seguito del caricamento e della diffusione[279] su Google Video (oggi equivalente alla piattaforma di YouTube[280]) di un video di 191 secondi in cui Francesco De Leon, un ragazzo affetto dalla sindrome di Down, veniva sbeffeggiato, insultato e malmenato da alcuni compagni di classe nella sua scuola di Torino. Nonostante nelle immagini comparissero anche scritte e saluti nazisti, mentre la stessa associazione veniva derisa, il video appariva tra i primi risultati della ricerca avente per parole chiave "video divertenti".

A seguito dell'upload, dunque, Vividown Onlus e i rappresentanti legali di De Leon avevano sporto denuncia contro Google Italia per il filmato ritenuto lesivo della reputazione sia del ragazzo che di quella dell'associazione. L'accusa faceva leva sul concorso omissivo in diffamazione a mezzo internet, in particolare per il fatto che il video non aveva subito alcun controllo preventivo da parte dei gestori di Google Video. A ciò, appellandosi alla policy sulla privacy della piattaforma di *videosharing*, si aggiungeva l'illecito trattamento dei dati personali in violazione degli artt. 13[281] e 26[282] del D. Lgs. 196/2003[283], stando ai quali l'informativa sulla privacy era insufficiente e le immagini costituivano dati idonei a rivelare lo stato di salute della persona inquadrata. Inoltre, il decreto risultava violato anche nelle previsioni dell'art. 17[284], relativo ai rischi specifici derivanti dal tipo di trattamento omesso, giacché anche dopo essere stata contattata dall'Autorità Garante per la

[278] Carl David Drummond – Presidente del CdA di Google Italy s.r.l. e amministratore delegato dal 2004 al 2007.
Peter Andrew Fleischer – Responsabile per l'Europa della policy sulla privacy di Google Inc.
George de los Reyes – Membro del CdA di Google Italy s.r.l. e amministratore delegato dal 2004 al 2007.
Arvind Desikan – Responsabile per l'Europa del progetto Google Video.

[279] Settembre 2006.

[280] Google Video consentiva l'upload e la ricerca di video all'interno della rete di Google fino all'acquisizione di YouTube da parte della società, nel 2005. A seguito di ciò, Google Video è rimasto funzionale alla ricerca, ma il caricamento dei file video può avvenire solo su YouTube.

[281] Art. 13 del D. Lgs. 196/2003 – "Informativa".

[282] Art. 26 del D. Lgs. 196/2003 – "Garanzie per i dati sensibili".

[283] Codice in materia di protezione dei dati personali.

[284] Art. 17 del D. Lgs. 196/2003 – "Trattamento che presenta rischi specifici".

Privacy, Google Italia aveva mantenuto disponibile il video, danneggiando la persona interessata.

Per quanto riguarda il primo reato, quello relativo alla diffamazione, i Pm sostenevano che il provider avrebbe dovuto impedire il configurarsi dell'evento, per cui sarebbe dovuta sorgere una responsabilità per mancato controllo preventivo sul contenuto del video. Se quest'ultimo vi fosse stato, infatti, il danno alla persona offesa sarebbe stato evitato o comunque avrebbe potuto avere un'entità minore.

Con riferimento alla violazione delle previsioni del D. Lgs. 196/2003, invece, i Pm avevano rilevato un reato nella violazione dell'art. 167[285] per omissione del corretto trattamento dei dati personali e sensibili dell'interessato, giacché il video che lo ritraeva era stato caricato e mantenuto sulla piattaforma al fine di ricavarne un profitto. Infatti, in relazione a ciò, non è da sottovalutare il fatto che Google Italia beneficia degli introiti pubblicitari derivanti dalla vendita agli inserzionisti di spazi disponibili su Google Video. Comunque, nell'effettuare tali osservazioni, i Pm avevano fatto riferimento alla distinzione tra *host* provider e *content* provider[286], dalla quale era risultato che Google Italia apparteneva alla seconda categoria, essendo un soggetto che immette i contenuti sulla rete. Pertanto, diversamente dai prestatori di servizi di *hosting*[287], esso doveva essere soggetto a responsabilità nel trattamento dei dati personali relativamente al controllo obbligatorio e preventivo sul contenuto del video in questione.

Dal momento che Google Italia ha sede a Milano, ad essere competente per il caso era proprio il Tribunale di Milano – Quarta Sezione Penale, nella sua composizione monocratica. Il giudice Oscar Magi, con sentenza 1972/2010[288] partì proprio dall'analisi di quest'ultimo capo di imputazione, considerato più grave. Secondo il magistrato, non esisteva alcun obbligo di legge codificato che imponesse agli ISPs un controllo preventivo sui materiali caricati in rete, ai sensi dello stesso D. Lgs.

---

[285] «[…] 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 nocumento, con la reclusione da uno a tre anni», art. 167 comma 2 del D. Lgs. 196/2003.

[287] Ex art. 16 D. Lgs. 70/2003.

[288] Sentenza n. 1972 del 24 febbraio 2010, Tribunale Ordinario di Milano in Composizione Monocratica, Sezione Quarta Penale, composta dal magistrato Oscar Magi .

70/2003. Tuttavia, il *provider*, ai sensi degli artt. 13 e 17 del D. Lgs. 196/2003, avrebbe dovuto ottemperare all'obbligo di corretta informazione agli utenti per ciò che riguarda i loro oneri e i rischi che si corrono a non adempierli, nonché al dovere di immediata cancellazione dei materiali indicati come criminosi.

Così, la voluta disattenzione nell'applicazione delle politiche societarie finalizzata a scopi di lucro e relativa allo scorretto trattamento dei dati personali e sensibili riguardanti De Leon e la conseguente sussistenza del cd. dolo specifico erano state giudicate punibili ai sensi dell'art. 167 D. Lgs. 196/2003. Seguendo quanto previsto da quest'ultimo, dunque, gli imputati erano stati condannati a sei mesi di reclusione ciascuno e al pagamento delle spese processuali[289].

Con riferimento al capo di imputazione relativo alla diffamazione, invece, proprio perché non esisteva un obbligo di controllo preventivo codificato dalla legge, non era da considerarsi plausibile l'osservazione dell'Autorità Garante per la protezione dei dati personali secondo cui il provider avrebbe dovuto impedire l'evento diffamatorio, che comunque sarebbe stato perpetrato anche se l'informativa sulla privacy fosse stata esaustiva e comprensibile all'utente, giacché nulla gli avrebbe impedito di caricare ugualmente il video in questione. Dunque, per questa ipotesi di reato, gli imputati vennero assolti[290].

I due capi di accusa dimostrano ancora una volta gli aspetti multiformi del cyberbullismo, che, quindi, si configura come un fenomeno complesso nel quale, per la giurisdizione italiana, la corretta informazione preventiva nelle *policies* delle piattaforme della web prevale sul controllo dei materiali caricati in rete, proprio perché non sussiste alcuna responsabilità per i *providers* ai sensi del D. Lgs. 70/2003. Tuttavia, il 27 febbraio 2013 è stata depositata in Cancelleria la sentenza n. 8611/2012, nella quale la Corte d'Appello di Milano - Sezione Prima Penale - ha assolto gli imputati stabilendo che «il fatto non sussiste»[291].

La decisione rivede completamente quanto previsto dal Tribunale Ordinario poiché la sola mancanza di informativa sulla privacy è stata considerata insufficiente a generare una responsabilità penale, la quale, piuttosto sarebbe stata da attribuirsi al

[289] Ibid.

[290] Ibid.

[291] Sentenza n. 8611 del 21 dicembre 2012, Corte d'Appello di Milano, Sezione Prima Penale.

soggetto che ha caricato il video sulla piattaforma di proprietà di Google Inc. Infatti, il titolare del trattamento dei dati personali è solo l'*uploader*, poiché esso, caricando il video, se ne assume la responsabilità, dovendo chiedere previo consenso al soggetto ripreso. A quest'ultimo sicuramente spetta il diritto di ricevere l'informativa sugli obblighi in capo a colui che ha caricato il video, ma ciò non significa che il *provider* debba rispondere dell'illecito commesso da terzi.

Con riferimento al dolo specifico relativo alla violazione dell'art. 167 del D. Lgs. 196/2003, invece, si sovverte la decisione del Tribunale Ordinario poiché quanto previsto da suddetta norma non è riscontrabile nel caso specifico giacché non vi era stato alcuno scopo di lucro nel mantenimento del video sulla piattaforma. Infatti, il servizio offerto non solo era gratuito, ma la pagina su cui si visualizzavano le immagini era anche sprovvista dei link pubblicitari negli spazi vendibili agli inserzionisti.

Inoltre, la Corte d'Appello approfondisce la decisione del Tribunale Ordinario definendo il provider come un "*hoster* attivo", in quanto esso ha la possibilità di filtrare, rimuovere ed indicizzare i contenuti, nonché di selezionarli e raccoglierli per fini pubblicitari.

Tuttavia, nonostante suddetta figura non sia contemplata dal Decreto Legislativo 70/2003 - probabilmente ormai troppo antiquato - non può sussistere per essa alcuna responsabilità di controllo preventivo sulla vasta quantità di materiale caricata dagli utenti. Infatti, nelle motivazioni della sentenza si afferma che: «Va esclusa per il prestatore di servizi che fornisca hosting attivo la possibilità ipso facto di procedere a una efficace verifica preventiva di tutto il materiale immesso dagli utenti»[292]. Inoltre, nell'affermare che «Non può non vedersi come l'obbligo del soggetto Web di impedire l'evento diffamatorio imporrebbe allo stesso un filtro preventivo su tutti i dati immessi in rete, che finirebbe per alterarne la sua funzionalità»[293], la Corte d'Appello pone l'accento sul fatto che richiedere meccanismi di controllo preventivo al provider significherebbe minacciare l'apertura del web e trasformarsi in un potere arbitrario di censura. Per questo «demandare ad un internet provider un dovere/potere di verifica preventiva appare una scelta da valutare con particolare

[292] Ibid.

[293] Ibid.

attenzione in quanto non scevra da rischi, poiché potrebbe finire per collidere con forme di libera manifestazione del pensiero»[294].

Nonostante l'assoluzione, comunque, si è giunti al terzo grado di giudizio che ha posto fine alla vicenda confermando quanto stabilito dalla Corte d'Appello. La Corte di Cassazione, infatti, a seguito del ricorso da parte della Procura Generale della Repubblica, con la sentenza 5107/2013, depositata il 3 febbraio del 2014[295], ha ricostruito i riferimenti normativi utilizzati nel corso dei processi precedenti, soffermandosi su diversi punti e rafforzando la decisione presa nel secondo grado di giudizio.

Innanzitutto, ai sensi del D. Lgs. 70/2003, è stata sottolineata l'assenza di qualunque obbligo di sorveglianza da parte del provider. In secondo luogo, si è affermato che anche qualora l'utente abbia caricato un video che infrange le norme sulla privacy, non spetta all'ISP riportare la violazione all'*uploader*. In terzo luogo, è stato ribadito che il titolare del trattamento dei dati personali è colui che ha potere decisionale rispetto ai fini e ai modi di suddetto trattamento, perciò non è una figura assimilabile a Google Italia, ma piuttosto all'utente che ha immesso il video in rete. Infatti, la società rappresenta un *hosting* provider, il quale diventerebbe "titolare del trattamento" solo gestendo direttamente gli indici di ricerca - ad esempio, attraverso impostazioni che rendono più o meno facile l'individuazione di una pagina web[296]. Per la Cassazione, dunque, la definizione di *host* provider "attivo" non ha alcuna rilevanza, visto che il Considerando n. 42 della direttiva sul commercio elettronico[297] prevede che: «Le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il

[294] Ibid.

[295] Sentenza n. 5107 del 17 dicembre 2013, Corte Suprema di Cassazione, Terza Sezione Penale.

[296] Cfr. Sentenza della Corte di Giustizia, causa C-131/12.

[297] 2000/31/CE.

che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate»[298].

In ultimo, viene precisato che non vi è il dolo specifico previsto dall'art. 167 del D. Lgs. 196/2003 poiché, vista l'assenza di un obbligo generale di controllo preventivo, non è possibile attribuire al provider il dovere di essere a conoscenza dei dati sensibili presenti nei video caricati in rete.

Dopo sette anni, dunque, il caso si è concluso ponendo l'accento più sulla disciplina relativa agli Internet Service Providers che sul cyberbullismo, il quale è decisamente passato in secondo piano. L'aspetto interessante di questa traslazione dell'attenzione risiede nel fatto che si tratta di uno dei tanti esempi - cui si farà riferimento più avanti (vedi Approfondimento 3b: Le indagini degli inquirenti e le decisioni dei giudici, pag. 171) - in cui il bullismo elettronico ha portato a considerare moltissimi altri aspetti della *governance* di internet, quali la privacy, la responsabilità del provider, la libera manifestazione del pensiero, la diffamazione ecc…

Comunque, fermo restando il pieno accordo con quanto stabilito dalla Cassazione, appare del tutto insensato che non vi siano stati (e non vi siano) provvedimenti spendibili nei confronti di chi compie tale abuso, inteso non come la piattaforma, ma individuato nell'utente che agisce diffamando o offendendo la vittima. Infatti, come sottolineato da Alan Johnson, segretario inglese all'Educazione, grazie alle piattaforme di *videosharing* il bullo si accanisce in modo molto più efficace e pervasivo, mandando in onda le prepotenze anche sul web, il che rende necessario prendere provvedimenti per chi esercita questo tipo di attività, anche attraverso la collaborazione dei *providers*.

Ciò che emerge è il fatto che la giustizia viene esercitata nei confronti dei colpevoli errati, poiché vi è un errore di fondo che risiede nel colpevolizzare i soggetti che forniscono servizi online piuttosto che gli utenti che abusano di suddette opportunità. Ciò che è giusto pretendere dagli ISPs è sicuramente la massima collaborazione possibile nella tutela dei minori che si sostanzia nel garantire che le azioni dei cyberbulli abbiano delle conseguenze anche in rete (rimozione del video, temporanea sospensione dell'account ecc…).

[298] Ibid.

Dunque, come più volte si è sostenuto nel corso di questo lavoro, emerge la necessità di coordinare le risorse e far sì che i *providers* possano esercitare la loro attività attraverso l'autoregolamentazione mediante *policies* chiare e puntuali, forti di una maggiore educazione e consapevolizzazione dei giovani attraverso strumenti educativi, pur rimanendo spendibili delle "sanzioni" in rete per coloro che attuano comportamenti illeciti. Unitamente a ciò, per reprimere gli abusi, appare necessario adottare una disposizione normativa che vada a punire i colpevoli di bullismo elettronico o quantomeno a scoraggiare le prepotenze via web per il fatto stesso di sapere che esse comporterebbero sanzioni gravi. In questo modo, l'ordinamento statale e le condizioni d'uso dei social network, assieme agli strumenti educativi, andrebbero ad agire sia sul livello preventivo che su quello successivo, diminuendo i reati ma mantenendo il più possibile invariata la libertà di espressione sul web.

Nel resto del mondo, non tutti gli interventi da parte di Google o di YouTube hanno avuto la stessa prontezza di quelli attuati nella rimozione del video che vedeva protagonista il ragazzo affetto da sindrome di Down, il che ha messo in discussione il ruolo dei *providers* nella risoluzione delle controversie.

In Spagna, ad esempio, José Martín Roldán, nel 2007, ha dovuto lottare affinché la piattaforma di *videosharing* rimuovesse i *files* in cui suo figlio quarantaseienne affetto da schizofrenia, Román, veniva messo in ridicolo e vessato durante uno dei suoi attacchi da una banda di ragazzi che, contemporaneamente, insultavano anche la famiglia del malcapitato. Ad accorgersi dei video era stato il secondo figlio dell'uomo, che aveva esortato immediatamente il padre a contattare YouTube, chiedendogli di rimuovere il video. Tuttavia, non ottenendo alcun riscontro da parte della piattaforma, l'uomo aveva cercato su Wikipedia i diversi recapiti di contatto dei media statunitensi in lingua spagnola, chiedendo aiuto a ciascuno di essi, ma senza esiti positivi. Qualche mese dopo aveva deciso di rivolgersi alla corte di Móstoles (Madrid) facendo una petizione verbale affinché i video venissero eliminati. Inizialmente l'utente rimosse i video, ma due settimane dopo ne apparve un altro, caricato da un diverso profilo, il che indusse Roldán a sporgere denuncia per individuare le persone che avevano registrato e postato il filmato e affinché YouTube venisse punito per la reiterata presenza dei video diffamanti.

A quel punto, mentre la Guardia Civil si occupava del caso, un portavoce di Google España dichiarò che il genitore avrebbe potuto chiedere che il video fosse rimosso compilando il modulo relativo alla violazione della privacy. Inoltre, aggiunse che la piattaforma avrebbe rivelato le informazioni personali degli utenti che avevano caricato i video solo quando fosse pervenuto un ordine del tribunale.

Sicuramente il fatto che si tratti di un uomo di quarantasei anni rende il caso diverso da quello che ha coinvolto l'associazione Vividown, tuttavia i bulli in questione erano tutti ragazzi e la vittima, affetta da schizofrenia, non era in grado di provvedere da sola a contattare Google o le autorità competenti e per questo può essere tranquillamente paragonata ad un soggetto debole minore di diciotto anni.

Infatti, questa riflessione pone di fronte anche ad un'altra annosa questione, cioè al fatto che i giovani, così come coloro che sono incapaci di intendere e di volere, necessitano assolutamente di un intervento pronto ed efficace da parte di tutti i soggetti coinvolti.

Così, ferma restando la deresponsabilizzazione dell'ISP, è inaccettabile il suo mancato intervento nella rimozione successiva alla segnalazione, giacché essa avrebbe avuto la funzione di tutelare qualcuno collocato in posizione svantaggiata. Infatti, la Agencia Española de Protección de Datos, nell'ottobre dello stesso anno, aveva posto l'accento sul fatto che la diffusione delle immagini costituiva una grave violazione della *Ley Orgánica de Protección de Datos*[299] poiché si trattava di scene raffiguranti la salute della persona, che, per di più, in questo caso aveva una disabilità.

Inoltre, il fatto che le risorse fossero disponibili solo in lingua inglese aveva rallentato non poco le capacità di Roldán di segnalare l'accaduto. Ciò dimostra, ancora una volta, la necessità per i *providers* di fornire in modo puntuale e facilmente comprensibile gli strumenti di risoluzione delle controversie, senza costringere gli utenti a ricorrere a strumenti alternativi come Wikipedia. Infatti, se si fosse trattato di un minore, magari meno motivato di un padre settantenne, probabilmente il giovane non avrebbe proceduto con le segnalazioni poiché non avrebbe saputo cosa fare.

Soltanto il 10 ottobre del 2007 il video venne rimosso da YouTube grazie all'insistenza dell'uomo nell'andare a fondo alla questione, poiché il supporto degli

[299] Legge 15/1999 del 13 dicembre.

avvocati condusse ad un rapido esame del video da parte della piattaforma che eliminò il video per violazione dei termini di utilizzo.

Comunque, proprio perché il reato di cyberbullismo non è previsto in nessuna delle sue manifestazioni (video, persecuzioni via web, pagine web, gruppi d'odio ecc…) recentemente, a Pavia, non è stata sporta alcuna denuncia quando su YouTube è comparso il video di un'aggressione da parte di una minorenne ai danni di una sua coetanea, ripreso da un compagno di scuola. Questo è quanto è successo il 17 gennaio 2014 per risolvere "questioni di cuore", come dichiarato da alcuni presenti.

Si tratta dell'ennesimo caso in cui un gruppo, radunato attorno alla scena di violenza, incita la bulla a continuare mentre qualcuno filma tutto per poi postarlo su YouTube. L'aggravante, però, sta nel fatto che la vittima non ha sporto denuncia perché ricattata da alcuni coetanei in possesso di un video privato di cui essa è protagonista.

Dunque, è chiaro che la mancanza di strumenti di tutela contro il cyberbullismo, qualunque forma esso prenda, sta mietendo vittime molteplici e per le ragioni più disparate. E' un reato che formalmente non esiste e che, anche laddove possa essere arginato con leggi già esistenti, non è abbastanza conosciuto né riconosciuto dai ragazzi o dalle loro famiglie, che non sanno come difendersi. Così, nuovamente compare la necessità per i rappresentanti legali di potersi avvalere di previsioni definite che consentano la corretta difesa del proprio assistito, ma soprattutto emerge l'esigenza di tutelare i minori dalle patologie del web, che si sostanziano ormai troppo spesso nelle prepotenze "elettroniche" perpetrate dai bulli.

In California, alla fine del 2009, una Corte Distrettuale ha dovuto affrontare un caso in cui una bambina delle elementari si era ritrovata ad essere vittima di cyberbullismo tramite la pubblicazione di un video su YouTube, creato da coetanei, in cui essa non solo appariva, ma veniva denigrata ed insultata. Riferito l'accaduto al consigliere scolastico, questi aveva discusso la questione con l'amministrazione e con gli avvocati dell'istituto, classificando il comportamento come "bullismo" e disponendo la sospensione per due giorni della ragazza che aveva postato il video online. La famiglia di quest'ultima decise di citare in giudizio la scuola presentando il caso alla corte federale sostenendo la violazione del Primo Emendamento. Così, nella celebre causa *J.C. v. Beverly Hills Unified School District*[300] venne stabilito che

[300]Federal Court Case n. 08-cv-03824.

gli istituti degli Stati Uniti, pur potendo disciplinare i comportamenti *off-campus* e intervenire contro le manifestazioni del pensiero degli studenti che interferiscono con la sicurezza dell'ambiente scolastico e le condizioni di istruzione, hanno l'obbligo di distinguere tra i discorsi meramente offensivi e quelli realmente dannosi che potrebbero compromettere il diritto di un altro studente di sentirsi al sicuro all'interno dell'ambiente scolastico.

In questo caso ha prevalso il Primo Emendamento e la famiglia della cyberbulla ha vinto la causa, ma non è possibile considerare il caricamento di un video denigrante su YouTube al pari di un insulto a voce, essendo esso disponibile e condivisibile da chiunque in qualsiasi momento, il che contribuisce ad alimentare il danno indotto dalla prepotenza, che non si esaurisce nel solo caricamento del *file*. Infatti, per quanto ammirevole la decisione di intervenire per correggere il comportamento della cyberbulla, l'intervento della scuola non solo è stato "punito", ma non ha neanche risolto il problema della presenza del video sulla piattaforma, che è passata in secondo piano nonostante costituisca il cardine dell'illecito.

Il problema è che non si possono ignorare gli aspetti emotivi e psicologici del fenomeno, poiché gli atti di bullismo elettronico hanno una risonanza di gran lunga maggiore rispetto a quelli tradizionali e sono perfettamente in grado di compromettere il diritto di uno studente di sentirsi al sicuro all'interno dell'ambiente scolastico giacché spesso ne consegue lo scherno e l'isolamento della vittima proprio all'interno dell'istituto.

Anche in Gran Bretagna, nel 2007, tre alunni dell'Hayling College (Hampshire), erano stati sospesi dopo aver postato su YouTube un video ripreso con il cellulare che raffigurava una rissa tra due ragazze. Il preside del college, in questo caso, aveva invece dovuto fronteggiare la grande difficoltà, proprio come José Martín Roldán, di ottenere che il video fosse tolto dalla piattaforma, tanto che alla fine aveva dovuto rivolgersi alla polizia.

Il parallelo tra i diversi episodi dimostra che l'intervento su più livelli è l'unico possibile, poiché a seconda della prospettiva da cui si guardano gli eventi, viene chiamato in causa tanto il personale scolastico quanto la piattaforma, che deve dare

una risposta immediata alle segnalazioni, collaborando con le autorità, ma cercando anche di risolvere le questioni prima che diventino di competenza della polizia.

Insomma, ciò che emerge da questo approfondimento è una grande confusione nell'attribuire le responsabilità e la potestà di intervento, che non sono definite dalla legge e spingono gli utenti a pensare che la risoluzione dei problemi sia compito esclusivo della scuola o degli ISPs. Per chi scrive, invece, il rigido rispetto delle *policies* da parte di YouTube, connesso ad un intervento rapido anche coordinabile con quello delle forze dell'ordine, unito ad eventuali previsioni di legge in grado di arrivare laddove il semplice *provider* non può - come nel caso dell'impossibilità di rilasciare spontaneamente le informazioni dell'account per individuare il cyberbullo - costituiscono gli unici strumenti che consentono di fronteggiare il fenomeno in analisi, da accostarsi ad una corretta educazione all'uso di internet.

Bisogna superare l'approccio classico al bullismo poiché nel mondo del web esso assume una molteplicità di configurazioni che necessitano di un *toolkit* nel quale si collocano strumenti governativi, scolastici e relativi alle aziende che operano nel settore, i quali a loro volta necessitano di essere coordinati mediante accordi nazionali ed internazionali, autoregolamentazioni e norme in grado di prevenire e reprimere il fenomeno.

Dunque, per quanto si possano deresponsabilizzare gli ISPs, ciò non può e non deve corrispondere ad una mancanza di assistenza agli utenti, siano essi insegnanti, alunni o genitori, poiché questo è l'unico modo per consentire ai più giovani di beneficiare della tecnologia e di difendersi dalle umiliazioni tanto diffuse sul web. Parallelamente, qualora l'intervento della piattaforma non fosse sufficiente ad arginare la questione, si dovrebbe avere una previsione legislativa funzionale all'individuazione e alla repressione degli illeciti relativi al cyberbullismo. Infatti, anche se nessuno mette in dubbio la presenza dei team e le loro capacità di risposta alle segnalazioni, emesse 24 ore al giorno, sette giorni alla settimana, probabilmente questa risorsa non è ancora sufficiente ad ottenere una rapida interruzione dei danni che può provocare un video la cui presenza in rete è continuativa e sempre riproducibile.

Approfondimento 3b:

Le indagini degli inquirenti e le decisioni dei giudici

Nonostante ogni stato abbia le sue leggi ed ogni social network abbia le sue *policies*, negli ultimi dieci anni il fenomeno del cyberbullismo ha invaso le sezioni di cronaca dei giornali e le scrivanie dei giudici, che si sono trovati a fare i conti con i casi più diversi. Infatti, non si parla soltanto di prese in giro e di tormento telematico, ma spesso ci si trova di fronte anche alla diffusione di materiale pedopornografico o all'istigazione al suicidio.

A causa della varietà di disposizioni normative a livello mondiale e della differenza di reazione alle condizioni d'uso dei social network nei singoli stati, si è deciso di prendere in esame alcuni dei fatti di cronaca più eclatanti per analizzare in che modo la giustizia abbia deciso di fare fronte al problema e, soprattutto, per comprendere se essa abbia effettivamente deciso di intervenire, riflettendo, a partire dai casi concreti, sui diversi aspetti del fenomeno sinora esposti.

Nel Regno Unito, il 21 agosto del 2009, per la prima volta è stata pronunciata una sentenza che ha visto una cyberbulla, Keeley Houghton (18 anni), finire in carcere per aver commesso un reato.

La Worcester Magistrates Court, infatti, ha accusato la ragazza di aver svolto attività di bullismo elettronico su Facebook ai danni di Emily Moore (18 anni), preceduta da due episodi di bullismo tradizionale ("*physical assault*"[301] nel 2005 e "*criminal damage*"[302] nel 2007). La vittima ha denunciato Houghton il 12 luglio, a seguito della pubblicazione di minacce di morte[303] come "*status*" di Facebook della cyberbulla. Le due ragazze, infatti, si erano incontrate due giorni prima in un pub di Malvern, dove Houghton aveva avvicinato Moore, la quale aveva intimato la sua persecutrice di lasciarla in pace altrimenti avrebbe chiamato la polizia, ottenendo

[301] Oggi rinvenibile nella Section 22 dello UK Borders Act del 2007, applicata nella fattispecie in quanto la vittima era stata assalita mentre tornava a casa da scuola.

[302] Criminal Damage Act del 1971, applicato nella fattispecie in quanto Houghton aveva preso a calci la porta di casa della vittima.

[303] "Keeley is going to murder the bitch. She is an actress. What a fucking liberty. Emily Fuckhead Moore".

come risposta che se non stava attenta le avrebbe dato un buon motivo per telefonare ai soccorsi, postando poco dopo la frase incriminata.

Così, nonostante l'indagata avesse eliminato lo *status* il giorno successivo alla sua pubblicazione - postato mentre quest'ultima era in stato alterato derivante dall'abuso di alcool - la denuncia ha assunto comunque rilevanza in quanto le frasi immesse sul web erano state precedute da intimidazioni verbali non soltanto la sera del 10 luglio, bensì negli ultimi quattro anni, sin da quando le ragazze avevano quattordici anni. Inoltre, a seguito dell'analisi dei registri dei Facebook, è risultato che in realtà le minacce erano state pubblicate alle quattro del pomeriggio - non la notte stessa - e, per di più, mantenute per 24 ore sul profilo di Houghton.

Gli avvocati della difesa hanno più volte dichiarato che la ragazza ha ammesso di essere coinvolta nel fatto, ma questo non ha contribuito a diminuire la pena stabilita dal giudice Bruce Morgan, pari a tre mesi di detenzione, unitamente a cinque anni di validità per l'ordine di restrizione da mantenere nei confronti di Moore e all'interdizione dall'uso di Facebook fino al gennaio del 2010.

Ovviamente, la sentenza ha soddisfatto pienamente le aspettative della vittima, che dopo molti anni di soprusi fisici e telematici ha potuto liberarsi del suo persecutore. Tuttavia, ai fini dell'argomento trattato è interessante riflettere su due punti fondamentali. Innanzitutto, il fatto che sia stato applicato il *Protection from Harassment Act* (1997) in quanto si è trattato di minacce credibili che fanno parte di una serie di molestie specificamente destinate ad un individuo, il che mostra la tendenza a tutelare le vittime di cyberbullismo attraverso leggi preesistenti e riguardanti fenomeni ad esso simili (vedi *supra* pag. 71).

In secondo luogo, collegato a quanto appena affermato, vi è il fatto che suddetta pena sia stata comminata solo perché preceduta da intimidazioni concrete e da danni fisici e materiali già perpetrati. C'è da chiedersi, infatti, se il giudizio della corte sarebbe stato lo stesso qualora si fosse trattato di mero bullismo elettronico, senza precedenti di bullismo tradizionale. Ciò confermerebbe quanto sinora affermato, cioè che il vuoto normativo porta all'applicazione di norme che regolano fattispecie simili, ma che finiscono per avere esiti diversi nonostante i casi siano riconducibili allo stesso fenomeno.

Sicuramente, il fatto che ci fossero dei precedenti ha contribuito ad alimentare i sospetti su Houghton ed ha condotto ad una pena che è in grado di tutelare Moore prevenendo ulteriori illeciti. Tuttavia, per un unico post su Facebook, se si fosse trattato di un caso senza precedenti di bullismo tradizionale, la decisione del tribunale sarebbe apparsa piuttosto eccessiva, giacché vi sono stati casi in cui la persecuzione è andata ben oltre il singolo commento, diventando un'attività di molestia continuativa, eppure non è stato disposto niente di simile.

Sembra, dunque, che si sia fermi ad una concezione di cyberbullismo come "accessorio" del bullismo tradizionale, poiché senza lesioni fisiche non viene data credibilità ai danni psicologici che il fenomeno può creare. A tal proposito infatti, il 15 aprile 2014 a Venaria, in provincia di Torino, una quattordicenne si è tolta la vita lanciandosi dal sesto piano del suo palazzo dopo aver ricevuto insulti e frasi crudeli su Ask.fm per lunghissimo tempo.

Aurora Cerullo, questo il nome della vittima, era affetta da una malattia ai reni che la rendeva molto esile e fisicamente diversa dai suoi coetanei, il che ha spinto un gran numero di utenti o forse un piccolo manipolo di individui, in ogni caso nascosti dietro l'anonimato, ad insultarla per il suo aspetto sulla piattaforma di *question and answer*.

Il giorno dopo il tragico evento, gli inquirenti avevano dichiarato che per poter parlare di cyberbullismo si necessitava di un'analisi approfondita, pertanto si riservavano di rivedere le loro conclusioni a seguito delle indagini. Infatti, i carabinieri avevano sequestrato sia il cellulare che il computer della ragazza, mentre la procura di Ivrea si accingeva a nominare un perito per analizzare le "domande" inviate sul social network e quella dei Minori cercava di fare luce sulla vicenda per comprendere, insieme, se si trattasse o meno di istigazione al suicidio.

Ebbene, a seguito dell'analisi dei messaggi inviati alla ragazza e nonostante la polizia postale abbia identificato tutti i minorenni che la tormentavano in forma anonima su Ask.fm, è risultato che nessuno si è accanito con continuità tale da potersi intraprendere un'accusa per istigazione al suicidio. Inoltre, gli inquirenti hanno aggiunto che la ragazza presentava una leggera forma di depressione, derivante non solo dalle sue condizioni di salute ma anche da un amore non corrisposto, pertanto le

ragioni del gesto sarebbero da attribuire a queste circostanze più che agli insulti ricevuti.

Insomma, il 29 aprile 2014 le forze dell'ordine hanno consegnato la loro relazione contenente suddette osservazioni al pm della Procura di Ivrea e a quello della Procura dei minori affinché i magistrati valutino le conclusioni delle indagini e decidano l'esistenza o meno delle ipotesi di reato.

In attesa di sapere se il caso verrà archiviato o meno, si può certamente elogiare la prontezza di reazione delle autorità competenti, che hanno immediatamente sequestrato il materiale utile (computer e cellulare) per vagliare tutti i messaggi ricevuti e inviati dalla ragazza, ma soprattutto per identificare gli utenti che pubblicavano commenti anonimi su Ask.fm.

Tuttavia, riflettendo sul fenomeno del cyberbullismo come evento dannoso per la persona che lo subisce, appare piuttosto ingiusta la soluzione degli inquirenti di escludere qualsiasi conseguenza solo perché i commenti erano stati postati da persone diverse e senza continuità. Infatti, se fossero stati insulti pronunciati a scuola - bullismo tradizionale - allora gli insegnanti sarebbero intervenuti e comunque le prepotenze sarebbero state limitate nel tempo e nello spazio. Su internet, invece, questi confini non esistono e non è possibile che non vi siano colpevoli anche se chiaramente un illecito è stato commesso, trattandosi di maltrattamenti e violenze psicologiche perpetrate 24 ore al giorno, 7 giorni su 7 ed eseguibili da chiunque.

Dunque, per quanto non si voglia suggerire un processo penale ai danni dei minori che hanno compiuto suddette azioni, è assolutamente insoddisfacente il fatto che non esistano misure da spendere per punire chi in rete commette qualcosa che nel mondo reale verrebbe sanzionato almeno a livello scolastico e familiare. Per questo si rinnova ancora una volta la necessità di adottare una legislazione che tuteli a livello civile e penale le vittime di cyberbullismo, affinché quantomeno i colpevoli ricevano delle ammonizioni, come la sospensione dell'account o l'interruzione parziale dei servizi offerti dalle piattaforme di social networking.

In questi casi, comunque, appare imprescindibile la collaborazione tra le forze dell'ordine e i *providers*, che rimangono gli unici in grado di inibire con un intervento repressivo la possibilità per il cyberbullo di continuare le sue attività

aggressive, fermo restando che dovrebbe sempre essere previsto un piano di prevenzione consistente nell'educare i più giovani al corretto uso del web.

Un altro caso in cui la persecuzione è stata frutto dell'attività incrociata di più utenti, ma senza l'immediato intervento da parte della piattaforma o della autorità, è quello di Flora, massacrata di insulti su Twitter, dopo aver vinto un biglietto omaggio per il concerto degli One Direction nel dicembre del 2012. La ragazza di 17 anni, infatti, ha partecipato al concorso BringMeTo1D, grazie al quale si è potuta recare gratuitamente a New York per assistere all'esibizione del suo gruppo preferito e poi conoscerne i membri.
Quello che all'inizio sembrava il realizzarsi di un sogno è diventato ben presto un terribile incubo, poiché il profilo Twitter di Flora è stato letteralmente invaso da insulti e minacce (vedi Immagine B), che si sono intensificati a seguito del suo rientro in patria a causa della pubblicazione delle fotografie che la ritraevano in compagnia degli One Direction.

Immagine B

Così, mentre i suoi *followers* passavano da 200 a 13000, le offese andavano dai commenti sul suo aspetto fisico al tipo di vestiario indossato durante l'incontro, ma soprattutto premevano sul fatto che fosse stata raccomandata e che non si era

emozionata abbastanza vedendo i membri della band, fino ad arrivare, progressivamente, ai suggerimenti e agli incoraggiamenti relativi alla sua morte.
Il fatto ha avuto immediatamente vasta copertura mediatica, in particolare grazie al quotidiano Repubblica e al telegiornale di Italia Uno, Studio Aperto. Questo evento ha generato moltissima solidarietà in rete, al punto che nel gennaio del 2013 sono nati due *hashtag* su Twitter, #IoStoConFlora e #StayStrongFlora, per dimostrare alla ragazza che il popolo della piattaforma la affiancava nella lotta contro i cyberbulli, ma questo non ha impedito che gli insulti telematici si trasformassero in realtà. Infatti, la situazione è degenerata fino al punto che, anche nei luoghi pubblici e per la strada, Flora ha cominciato ad essere derisa e offesa. Così, mentre inizialmente la diciassettenne fronteggiava con relativa serenità la situazione, ha cominciato a spaventarsi quando si è resa conto che le prepotenze scritte si sono trasformate in minacce di morte e in commenti così pesanti da rasentare l'istigazione al suicidio.
Pertanto, il 10 gennaio 2013, la ragazza e la sua famiglia hanno deciso di recarsi alla Polizia Postale per presentare denuncia e cercare di arginare la valanga di insulti e intimidazioni che stavano ricoprendo la ragazza. Infatti, la cosa più terribile è stata che l'attività denigratoria non si è fermata in seguito all'incontro e al concerto, anzi, ha aumentato il suo volume e modificato le sue modalità, tanto da spingere la Sony, che aveva organizzato il concorso, a minacciare di sporgere denuncia contro chiunque avesse continuato scrivere che la manifestazione era stata truccata o che Flora avesse vinto grazie alle raccomandazioni.
In questo caso, come in quello di Aurora Cerullo, il numero dei cyberbulli è di gran lunga superiore alla norma e la loro attività, per quanto continuativa, non ha avuto la costanza di cui sembra dover essere munito il bullismo elettronico per essere perseguito, tanto che lo scandalo è scoppiato solo dopo aver ricevuto copertura mediatica. Tuttavia, per chi scrive, appare di dubbia ragionevolezza pensare che si possa omettere un intervento soltanto perché l'attività è intrapresa da un numero indeterminato (ma determinabile) di utenti e i loro insulti non hanno carattere metodico.
Di fatto, alla base c'è sempre la volontà di denigrare la persona e arrecarle un'offesa, tant'è che la Polizia Postale ha immediatamente raccolto la deposizione e la denuncia di Flora, attivandosi tramite la Procura Ordinaria per reperire tutto il materiale

necessario a presentare il caso di fronte ai magistrati. Così, anche se ovviamente le indagini vengono condotte contro ignoti, il fatto che si tratti di Twitter può garantire che vengano reperiti i nomi di coloro che hanno insultato e/o minacciato Flora, lasciando alla Procura dei Minori l'intervento nei casi in cui i *followers* che hanno pubblicato i commenti siano minorenni.

I capi di imputazione sarebbero da individuarsi nella diffamazione aggravata (art. 595 c.p.) e nelle minacce gravi (art. 612 c.p.), ma ad oggi ancora non sono stati diffusi i risultati delle indagini, anche se il profilo della ragazza su Twitter, seppur finalmente privato, ha ancora tutti i *followers* e i *tweet* necessari alla conclusione degli accertamenti della Polizia Postale (vedi Immagine 6).

Immagine 6

Ancora una volta, è inaccettabile il fatto che le tempistiche necessarie a prendere provvedimenti e ad agire per arginare il fenomeno siano così elevate, praticamente pari a quelle utilizzate nei casi di diffamazione a mezzo stampa, nonostante la natura del web sia totalmente diversa e necessiti di interventi diretti ed immediati. Inoltre, emerge nuovamente la difficoltà di identificare il cyberbullismo senza una base normativa che consenta di individuare le modalità con cui esso si configura (frequenza, durata, carattere dei contenuti, profili dei cyberbulli ecc…), il che ostacola sia la capacità delle autorità di intraprendere celermente azioni che tutelino la vittima, sia l'intervento cooperativo con il *provider*, poiché, fermo restando quanto

stabilito dal D. Lgs. 70/2003, è comunque necessario che si attivino meccanismi collaborativi che impediscano il protrarsi delle offese e della persecuzione.

Un altro esempio che testimonia la scarsità di prontezza nella reazione agli illeciti perpetrati dai cyberbulli sul web è quello della quattordicenne Hannah Smith, trovata impiccata nella sua camera da letto dalla sorella maggiore, il 2 agosto del 2013. La decisione di togliersi la vita è stata presa non soltanto dopo essere stata vittima di episodi di bullismo scolastico a causa del suo eczema - questo è ciò che riferisce il padre - ma soprattutto dopo aver ricevuto per settimane insulti crudeli su Ask.fm, che, tra le altre cose, la invitavano a togliersi la vita.
A seguito dell'evento, gli amministratori del social network avevano rilasciato alla BBC un comunicato stampa[304] in cui annunciavano di voler collaborare con le indagini della polizia di Leicestershire, ricordando che tutte le segnalazioni vengono tutt'ora lette dal team di moderatori per garantire che i problemi di cyberbullismo siano affrontati celermente, provvedendo a rimuovere i contenuti dannosi segnalati qualora essi violino i termini di servizio.
Proprio perché rimane piuttosto difficile pensare all'efficacia di tali misure considerando che Ask.fm conta circa 200'000 nuovi membri al giorno, il sito ha accettato di apportare modifiche per rendere più sicuri gli utenti (vedi *supra* pag. 145) subito dopo il suicidio della ragazza.
Comunque, inizialmente la morte della giovane è stata oggetto di inchiesta da parte del coroner Catherine Mason, poiché in Gran Bretagna ciò accade ogniqualvolta una morte è improvvisa, violenta o innaturale. Dal momento che il ruolo di questo ufficiale giudiziario indipendente è quello di indagare e registrare le cause e le circostanze di questo tipo di decessi, la polizia non ha potuto indagare da subito sugli eventi nonostante l'offerta di collaborazione da parte di Ask.fm. Una simile procedura appare piuttosto contrastante con il mondo di internet, considerando che, come già visto in precedenza, i tempi di memorizzazione dei file necessari all'ottenimento delle prove sono estremamente ristretti sul web, il che richiede un intervento rapido ed immediato.

[304] Sian Lloyd, *Hannah Smith death: Ask.fm 'to help police inquiry'*, 6/8/2013, in www.bbc.com.

Per lungo tempo si è discusso animatamente su questo aspetto, nonché sul fatto che le identità dei cyberbulli avrebbero dovuto essere immediatamente rese note agli inquirenti, affinché si potesse procedere nei loro confronti. Il padre della vittima, infatti, si era mosso da subito al fine di ottenere giustizia per la figlia, dando vita addirittura ad una petizione online contro i rischi per i minori presenti sulle piattaforme web (vedi *supra* pag. 137).

Sino alla primavera del 2014 il dibattito è rimasto piuttosto vivo ed ha contribuito ad alimentare i tentativi di fronteggiare il fenomeno del cyberbullismo, al punto che persino David Cameron era intervenuto per intimare il boicottaggio dei siti che, come Ask.fm, consentono che le minacce e le molestie siano perpetrate per lungo tempo ed in forma anonima prima di intervenire.

Tuttavia, per correttezza nella redazione del presente lavoro, è necessario precisare che i risultati delle indagini, resi noti il 6 maggio del 2014 dal detective Wayne Simmons durante una seduta di ascolto tenutasi al Leicester Coroner's Court[305], hanno rilevato che i messaggi offensivi provenivano dallo stesso IP della ragazza, la quale, dunque, con vasta probabilità si era auto inviata suddetti contenuti. Simmons, infatti, ha precisato che è del tutto improbabile che gli insulti e l'istigazione al suicidio siano stati postati dallo stesso indirizzo IP ma da una persona diversa da Hannah Smith, in quanto questa persona avrebbe dovuto possedere le credenziali di accesso della ragazza (account e password) nonché trovarsi nella stessa casa della giovane.

Alla luce di ciò, durante la seduta del 6 maggio, il coroner del Leicester e del South Leicestershire, ha interrogato Simmons circa la presenza di prove che Hannah Smith fosse stata oggetto di cyberbullismo, ottenendo come risposta dall'uomo che non ve ne sono. Dunque, Catherine Mason ha confermato il verdetto di suicidio senza alcun tipo di istigazione perpetrata da terzi, aggiungendo che nessun intervento preventivo (del social network, dei giudici o della polizia) avrebbe potuto evitare che la ragazza compisse l'insano gesto.

Comunque, prima di questa svolta inaspettata nelle indagini, è stata dimostrata la necessità di collaborazione tra ISP e forze dell'ordine, grazie alla quale è stato comunque possibile risolvere il caso seppur in senso totalmente diverso da quello

[305] coroners.leicester.gov.uk/completed-inquests/?EntryId78=131046.

originario. Infatti, solo grazie alla memorizzazione e alla messa a disposizione dei file relativi ai messaggi e all'accesso è stato possibile ottenere l'IP di provenienza degli insulti e delle istigazioni al suicidio. Tuttavia, restano assolutamente discutibili i tempi di azione e di intervento della polizia poiché anche in questo caso, come in quello di Emily Moore, vi erano stati precedenti di bullismo tradizionale che potevano indurre a sospettare di cyberbullismo qualche coetaneo di Hannah Smith. Nel 2013, però, nessun giudice è intervenuto nell'immediato per stabilire che venissero subito reperiti i dati relativi agli indirizzi IP poiché gli accertamenti sul suicidio hanno sovrastato le indagini per bullismo elettronico.

Dunque, a prescindere dai risultati delle indagini, il caso di Leicestershire fa riflettere sulle tempistiche e le modalità di reazione agli illeciti perpetrati dai cyberbulli sul web. Il fatto che la vittima sia ancora viva e il colpevole sia identificabile, come nel caso di Moore, hanno comportato un'immediata azione di prevenzione sulla base di abusi già commessi in passato. Nella vicenda di Hannah Smith, invece, pur essendo stata vittima di bullismo ed essendosi uccisa presumibilmente (prima degli imprevedibili risultati) per lo stesso motivo, non è stato adottato alcun intervento immediato, se non quello di approdare ad una conclusione un anno dopo, sovvertendo, tra l'altro, le ipotesi iniziali - cosa che sarebbe potuta realizzarsi ben prima, se si fosse proceduto prontamente.

Come già affermato spesso nel corso di questo lavoro, sicuramente non è semplice distinguere i casi di cyberbullismo da tutta una serie di altri fenomeni, tra cui l'autolesionismo, a causa delle caratteristiche intrinseche del web, come l'anonimato e la possibilità di creare profili *fake*. A ciò, poi, si aggiunge il processo di vittimizzazione che si innesca in chi subisce gli insulti e si somma a delle evidenti difficoltà pregresse che spingono i più giovani a togliersi la vita.

Tuttavia, è impossibile pensare che si possa trovare una soluzione al fenomeno se non se ne organizza legislativamente la regolazione e se non viene realizzato che l'approccio al bullismo elettronico deve essere molto più rapido di quello che si ha nei confronti del bullismo tradizionale, poiché nel mondo del web le minacce possono portare ad una escalation di violenza non soltanto verbale ed emotiva, ma anche fisica o auto inflitta.

Infatti, nonostante l'inaspettata conclusione del caso di Hannah Smith, Ask.fm ha continuato a mietere vittime tra i più giovani, alimentando il fenomeno del cyberbullismo. E' il caso, ad esempio di Ciara Pugsley, ritrovata il 29 settembre del 2012 nel bosco vicino alla sua casa di Leitrim (Irlanda). La ragazza di quindici anni si è tolta la vita a seguito delle numerose offese ricevute sulla piattaforma di *question and answer*, così come la tredicenne Erin Gallagher, anche lei irlandese, ritrovata dalla madre il 27 ottobre del 2012 nella loro abitazione a Ballybofey. In quest'ultimo caso, la giovanissima vittima aveva più volte pubblicato su Ask.fm che si sarebbe tolta la vita a causa di un'autentica "campagna" di cyberbullismo, che la vedeva protagonista degli insulti sul suo aspetto fisico ritenuto troppo "grasso" dai suoi anonimi *followers*. La rapida successione di questi due casi ha portato tutto il Regno Unito a riflettere sul potenziale dannoso della piattaforma, nominata espressamente nel biglietto di addio di Erin Gallagher, che, scusandosi, affermava di doversi uccidere poiché stufa degli atti bullismo subiti[306].

Il social network ha rimosso il profilo delle due ragazze quasi un anno dopo la loro morte e non ci sono state denunce o cause intraprese per scoprire l'identità dei cyberbulli, tanto che il Children's Ombudsman ha richiesto espressamente mediante l'*Emily Logan's Bullying Report*[307], che vengano quantomeno intraprese, a livello scolastico, le iniziative necessarie per prevenire il fenomeno, riconoscendo il ruolo determinante dell'educazione nell'arginamento del bullismo elettronico.

Di recente, 19 febbraio del 2014, è stata la volta di Nadia, una quattordicenne di Cittadella (Padova) che ha deciso di buttarsi dal tetto di un hotel, chiedendo scusa ai genitori in una lettera per averli delusi, dopo aver già compiuto atti autolesionisti a seguito delle numerose offese ricevute sul suo profilo di Ask.fm, dove le si chiedeva di tagliarsi le vene, di rendersi conto di quanto faceva schifo come persona e di quanto fosse patetica.

Insomma, anche in questo caso, come in tutti quelli già analizzati, si tratta senza dubbio di episodi di cyberbullismo, ma a differenza di quanto accaduto in Irlanda, la Procura di Padova ha deciso immediatamente di aprire un'inchiesta, pur non

[306] "I'm sorry I have to do this but I'm fed up of the bullying".

[307] Children's Ombudsman Office, Dealing with Bullying in Schools: A Consultation with Children & Young People, novembre 2012, in www.oco.ie.

essendoci indagati precisi, a partire dall'ipotesi di reato consistente in maltrattamenti e istigazione al suicidio. La Polizia Postale, a tal fine, si occuperà di collaborare con la polizia lettone per risalire all'identità di coloro che hanno pubblicato i messaggi anonimi sul profilo della ragazza.

Dunque, anche se ci sono norme in tutto il mondo che possono essere estese per dare copertura al fenomeno, esse non regolano l'intervento delle autorità, le modalità di denuncia, le pene previste per i cyberbulli né tutto ciò che sarebbe necessario per arginarne l'espansione, che invece viene deciso caso per caso, in modo diverso in ogni stato, nonostante le caratteristiche e le conseguenze degli abusi siano pressoché le stesse ovunque.

Allora, sembra sempre più opportuno pensare a disposizioni che consentano di prendere provvedimenti seri e concreti nei confronti di chi abusa della libertà del web, soprattutto considerando che si tratta di minori, ma è chiaro che ciò non può essere fatto solo in un'ottica nazionale. Infatti, appare imprescindibile contrastare gli illeciti perpetrati online a livello internazionale, visto il carattere a-territoriale della rete che necessita di vaste cooperazioni per essere gestito. Nel caso di Nadia, per esempio, la piattaforma lettone ha dovuto decidere spontaneamente di sospendere l'account poiché la ragazza ha continuato ad essere insultata sul suo profilo di Ask.fm anche dopo il suicidio, tanto che il Codacons ha presentato un esposto al Garante della privacy «per accertare se nella modalità di utilizzo del sito, vi siano eventuali profili di illegittimità o di violazioni dei dati»[308].

Interessante è stata la risposta statunitense al caso di Rebecca Sedwick che, pur dimostrando tempistiche estremamente incalzanti, ha visto ribaltarsi completamente le conseguenze inizialmente derivanti dalle azioni delle cyberbulle che hanno spinto al suicidio la ragazza di Lakeland (Florida).

La vittima, di soli dodici anni, il 10 settembre del 2013 ha deciso di suicidarsi gettandosi da un fabbricato industriale dopo aver subito due anni di bullismo elettronico, messo in atto da un gruppo di coetanee. I motivi dichiarati alle autorità nelle diverse sedute di ascolto erano relativi a questioni di cuore, che avevano visto una compagna di scuola ingelosirsi dell'ex fidanzato di Rebecca Sedwick, portandola

[308] www.codacons.it.

dapprima ad aggredire fisicamente la ragazza, poi a cercare supporto in una dozzina di coetanee affinché isolassero la vittima.

Questi fatti avevano indotto la madre della giovane a decidere di farla studiare in casa per gli ultimi mesi delle elementari, in attesa del passaggio alla scuola media, dove comunque Rebecca Sedwick aveva continuato a subire prepotenze telematiche, nonostante non lo avesse riferito ai genitori.

Ad occuparsi delle indagini è stato lo sceriffo di Polk County, Grady Judd, che insieme ad alcuni colleghi ha controllato i molteplici account della ragazza sui social media, scoprendo che la giovane era costantemente vittima di cyberbullismo, perpetrato non soltanto tramite messaggi offensivi, ma anche attraverso un continuo incitamento alla morte.

A metà ottobre, le indagini hanno portato ad individuare due sospettate, Guadalupe Shaw (quattordici anni) e Katelyn Roman (dodici anni), le quali avevano iniziato a perseguitare la vittima per questioni di cuore. I loro nomi sono stati resi noti quasi subito dallo stesso sceriffo in quanto le accuse per stalking aggravato hanno condotto immediatamente al loro arresto il 15 ottobre. Nell'*Arrest report*[309], infatti, viene sottolineato che, secondo il Titolo 46 dei *Florida Statutes*[310], le ragazze sono perseguibili poiché si tratta di un illecito che costituisce un crimine di terzo grado (punibile con un massimo di cinque anni di carcere), in quanto si tratta di azioni di stalking volontarie, maliziose e ripetute, perpetrate ai danni di una vittima di età inferiore ai 16 anni (*felony aggravated stalking of minor 16 years of age*)[311].

Dunque, nonostante all'interno dello stato non vi fossero (e non vi siano tutt'ora) leggi specifiche sul cyberbullismo, ad esso si è deciso di applicare una disposizione già presente che ha consentito di incriminare due minorenni per il suicidio della vittima.

Tuttavia, con un evidente colpo di scena, il 20 novembre il giudice Michael McCarthy della *Circuit Criminal Divisions* ha fatto cadere le accuse per insufficienza di prove, che gli avvocati difensori hanno descritto come mancanza di leggi che

[309] Sheriff's Office – Polk County – Winter Haven, FL , Shaw and Roman Affidavits (Incident number 130042926), in archive.org.

[310] Title XLVI – Chapter 784 (Crimes: assault; battery; culpable negligence), par. 048, Stalking; definitions; penalties.

[311] Ibid.

individuino un illecito nelle azioni delle loro assistite. Questo ribaltamento repentino dimostra che, per quanto le norme esistenti siano già molte e possano essere estese al cyberbullismo, se questo reato non viene minimamente menzionato nelle disposizioni legislative è molto semplice trovare delle scappatoie che consentano ai legali di scagionare i loro clienti, nonostante sia fuori dubbio il loro coinvolgimento nei fatti.

A ciò si aggiunge la più volte citata complessità del reperimento delle prove, la cui natura assume le peculiarità delle tecnologie digitali rendendole rimovibili e rintracciabili solo con analisi mirate. Nel caso Sedwick, per esempio, Guadalupe Shaw aveva postato sulla sua pagina di Facebook l'ammissione di bullismo, aggiungendo che non le importava nulla del suicidio della ragazza. Poco dopo, però, interrogata dalla polizia, aveva dichiarato che il suo account era stato hackerato e che non era stata lei a pubblicare lo status.

Inoltre, gli avvocati delle due ragazze incriminate hanno criticato insistentemente il comportamento dello sceriffo, sottolineando che il rilascio delle foto e dei nomi delle giovani aveva causato la loro sospensione scolastica e, soprattutto, che ciò era stato effettuato a seguito dell'arresto senza che vi fosse motivo di dichiararle colpevoli.

Dunque, a differenza dei casi già citati, i presunti colpevoli sono stati identificati, ma non è stato possibile, come nella vicenda che ha coinvolto Aurora Cerullo, punire in alcun modo i cyberbulli. Non si tratta, quindi, di intraprendere solamente un'azione legale, che comunque nei diversi paesi è sempre possibile a partire dall'estensione al fenomeno in analisi di norme già esistenti. Piuttosto, ciò che lascia perplessi è l'assenza totale di qualunque tipo di conseguenza, proprio perché non esiste il cyberbullismo come reato e non esistono neanche punizioni di lieve entità (ad esempio l'interdizione momentanea dai siti di social networking o il richiamo scolastico) tali da scoraggiare il ripetersi delle azioni dannose.

Insomma, il paradosso è che, avvalendosi di strumenti già esistenti che tutelano le vittime di crimini ben precisi, ci si trova a fronteggiare un illecito che non è considerato un reato. Questo tipo di approccio sembra una contraddizione in termini, poiché equivale a dire che in via ufficiosa si può pensare di difendere coloro che subiscono il cyberbullismo, ma in via ufficiale non esiste alcuna disposizione che lo configuri come misfatto tale da meritare delle conseguenze concrete.

Una volta puntualizzate le suddette osservazioni, è necessario spostare l'attenzione sul fatto che, come si è detto più volte, il fenomeno in esame comprende molte fattispecie differenti, che vanno dal furto di identità all'istigazione al suicidio, ma possono anche riguardare la pedopornografia quando si tratta di *sexting* o di *revenge porn*. A tal proposito, rimane celebre lo sfortunato caso di Amanda Todd, sedicenne di Vancouver, suicidatasi il 10 ottobre del 2012 a seguito di un ricatto sessuale trasformatosi in una vera e propria campagna di cyberbullismo ai danni della sua persona.

Il 7 settembre 2012, la giovane aveva pubblicato un video di quasi 9 minuti su YouTube, intitolato "*My Story: Struggling, bullying, suicide and self-harm*", nel quale narrava la sua esperienza personale che oggi conta più di nove milioni di visite. Durante le immagini, Amanda Todd racconta che nel 2010 si era trasferita con il padre e, non conoscendo la nuova città, aveva usato una video chat per incontrare nuove persone su internet.

Per oltre un anno, uno sconosciuto aveva tentato di persuaderla affinché si fotografasse i seni e, una volta convinta, la ragazza si era scattata delle foto con cui l'uomo iniziò a ricattarla dopo averla aggiunta su Facebook affinché si mostrasse nuda in webcam, altrimenti avrebbe diffuso le immagini a tutti i suoi amici.

Essendo amici sulla piattaforma social, l'uomo conosceva il suo indirizzo, il suo nome, dove andava a scuola e chi fossero i suoi familiari nonché i suoi conoscenti. La ragazza, rifiutandosi di mettere in piedi lo "show" che le era stato richiesto, vide l'uomo postare pubblicamente le fotografie, il che scatenò numerosi atti di bullismo tradizionale ed elettronico da parte dei compagni di scuola, conducendola ad una grave depressione fatta di ansia, autolesionismo e abuso di droghe.

Il padre, a conoscenza dell'accaduto perché informato dalla polizia locale durante le vacanze di Natale del 2010, decise di trasferirsi nuovamente. Un anno dopo, però, nonostante la ragazza avesse nuovi amici e una vita diversa, l'individuo riapparve creando un nuovo account di Facebook - che aveva come immagine del profilo la fotografia dei seni di Amanda Todd - e contattando tutti i nuovi compagni di scuola della ragazza. Subite ancora una volta le persecuzioni scolastiche da parte dei coetanei, dovette cambiare scuola per la seconda volta.

Nel frattempo, un vecchio amico l'aveva ricontattata e si erano visti mentre la sua ragazza era in vacanza, consumando un rapporto sessuale. Qualche giorno dopo, la fidanzata del ragazzo e un gruppo di altri 15 persone, compreso il giovane, assalirono la vittima nella nuova scuola, con insulti, calci e pugni, lasciandola agonizzante in un fossato. L'episodio spinse la ragazza a tentare il suicidio bevendo candeggina, ma sopravvisse grazie al tempestivo intervento dell'ambulanza.

Nuovamente, nel marzo 2012, la madre decise di prenderla con sé in un'altra città e, evitando di sporgere denuncia per farle ricominciare una nuova vita altrove, fu in quell'occasione che Amanda Todd pubblicò il suo video su YouTube.

Tuttavia, gli atti di cyberbullismo non si fermarono, anzi, divennero sempre più frequenti, portandola alla decisione di togliersi la vita.

Meno di una settimana dopo la morte di Amanda, i legislatori canadesi hanno iniziato a prendere in considerazione una proposta di legge costituisca la base di una strategia nazionale di prevenzione del cyberbullismo, oggi il già citato Bill C-13: "*The Protecting Canadians from Online Crime Act*" (vedi *supra* pag. 93).

Infatti, nonostante i coetanei l'avessero derisa, offesa, incitata a riprovare a togliersi la vita e ripostato le foto dei suoi seni per decine di volte su moltissimi siti, nessuno di loro era stato soggetto ad alcuna conseguenza.

L'uomo dall'identità nascosta è stato identificato ed arrestato in Olanda solamente il 18 aprile 2014. Si tratta di un tedesco di 35 anni, accusato di estorsione, adescamento e molestie, nonché di possesso di materiale pedopornografico a fini distributivi.

Il caso ha fatto particolarmente scalpore perché oltre a riguardare un reato gravissimo, quello di pornografia minorile, ha accentrato l'attenzione internazionale sul problema del bullismo in tutte le sue forme grazie al video che la ragazza aveva pubblicato su YouTube. Infatti, nonostante i numerosi cambi di scuola, nulla, grazie all'a-territorialità del web, ha impedito ai compagni di Amanda Todd di bersagliarla continuamente e, per quanto essi fossero stati quasi tutti contattati tramite Facebook dall'uomo arrestato, nessuno aveva mai fatto in modo che cessassero le prepotenze e smettessero di insultarla o postare le fotografie dei suoi seni.

Sull'onda di quanto avvenuto a Vancouver, in Italia è stato accolto con enorme preoccupazione il suicidio di Carolina Picchio, la quattordicenne di Novara che si è gettata dal balcone di casa sua il 5 gennaio 2013. La giovane ha deciso di togliersi la

vita in seguito alla pubblicazione di un video su Facebook che la ritraeva durante atti sessuali di gruppo ad una festa.

Avviate immediatamente le indagini, è stato scoperto che Carolina quella sera aveva bevuto molto ed era stata abusata da più ragazzi che poi avevano postato le immagini sulla piattaforma web, dando il via a ben 2600 offese telematiche solo nelle prime 24 ore.

In questo tragico caso, proprio perché il mondo era già stato scosso dalla vicenda canadese, a maggio del 2013 si è deciso di aprire due diverse inchieste. La prima, seguita dai magistrati di Torino e coordinata dal pm Valentina Sellaroli, vede iscritti al registro degli indagati della procura dei minori ben sei ragazzi: cinque per "violenza sessuale di gruppo", uno per "diffusione di materiale pedopornografico online" e, in realtà, quest'ultimo, insieme al fidanzato di Carolina Picchio è indagato anche per il suicidio come conseguenza di altri reati.

La seconda inchiesta, invece, indaga su Facebook per "omissione di controllo sui contenuti pubblicati" ed è diretta dalla Procura di Novara che si sta muovendo parallelamente al Movimento italiano dei genitori (Moige), il quale ha presentato una denuncia contro il social network per "concorso in istigazione al suicidio della minore".

Alla luce della già citata sentenza 5107/2013 della Corte di Cassazione[312] (vedi s*upra* pag. 164), appare piuttosto difficile pensare che vi sia e che venga ammessa un effettivo coinvolgimento del provider nell'accaduto, giacché esso non può essere ritenuto responsabile dei contenuti diffusi in rete ai sensi del D. Lgs. 70/2003. Tuttavia, l'accusa ipotizza che la ragazza sia stata istigata al suicidio dagli atti di bullismo perpetrati sul web attraverso i commenti e le immagini con cui i cyberbulli l'hanno perseguitata.

Entrambi i casi, quello canadese e quello italiano, dimostrano in modo lampante quanto l'umiliazione telematica possa essere nociva e pervasiva, tanto da spingere gli adolescenti a togliersi la vita. Chiaramente, il fatto che si sia trattato di avvenimenti che hanno coinvolto la pornografia minorile li ha resi ben più facilmente tutelabili dalla legge canadese e italiana, ma questo sarebbe successo ovunque, proprio perché,

[312] Sentenza n. 5107 del 17 dicembre 2013, Corte Suprema di Cassazione, Terza Sezione Penale, depositata il 3 febbraio 2014, caso Google-Vividown.

come si diceva poco fa, il cyberbullismo viene combattuto attraverso previsioni normative già esistenti.
Tuttavia, ciò che sembra emergere da quanto detto sinora, è che, come nel caso delle minacce e delle violenze fisiche perpetrate da Keeley Houghton ai danni di Emily Moore, il fenomeno viene combattuto solo se esistono dei reati considerati "gravi" che vanno a costituire parte integrante del bullismo elettronico, quasi come se da solo esso non bastasse ad essere considerato una potenziale minaccia ai diritti della persona. Infatti, non bisogna dimenticare i casi sin qui affrontati in cui il fenomeno si è configurato come attività denigratoria continuativa e nei quali non è stato preso alcun provvedimento se non in rare occasioni e per un tempo limitato.

Rimane aperta, dunque, la questione relativa agli strumenti di tutela messi a disposizione dalla legislazione nei diversi stati, poiché le misure per fronteggiare l'ondata di insulti e di offese sembrano essere insufficienti sia a prevenire che a reprimere gli illeciti.
Ciò appare con maggiore chiarezza se si osserva quanto accade, invece, nei territori che posseggono specifiche normative volte a tutelare le vittime di cyberbullismo.
E' il caso, ad esempio, di una ragazza di Issaquah di soli dodici anni, perseguitata da due compagne di classe nell'aprile del 2011. Infatti, nello stato di Washinghton il *Senate Bill 5288* del 2007 ha modificato il *Code of Washinghton* (*§28A.300.285*) aggiungendo il cyberbullismo al *Bullying Act* (cfr. pag. 16) e considerandolo un reato che può assumere anche una configurazione penale grazie alla *Cyberstalking Law*[313].
Si è trattato di una storia che ha visto coinvolte due ragazze, rispettivamente di undici e dodici anni, che hanno perseguitato la loro compagna di classe, Leslie Cote, prima a scuola e poi in rete. La vittima ha dichiarato che, dopo aver accidentalmente salvato la password di Facebook sul computer di una delle due amiche, le sue coetanee le hanno rubato l'account a seguito di una lite ed hanno iniziato a pubblicare immagini oscene e offensive sul suo profilo, come quelle che la ritraevano con un coltello puntato alla testa e con le corna da diavolo insieme alla didascalia "*I'm a slut*". Inoltre, le ragazze hanno anche inviato messaggi ai suoi

[313] Revised Code of Washinghton 9.61.260, Cyberstalking.

“amici” a nome della vittima, parlando di parti intime e invitandoli ad avere rapporti sessuali.

Leslie Cote ha raccontato l’accaduto a sua madre, che ha immediatamente sporto denuncia assieme alla figlia affinché le cyberbulle venissero fermate. Queste ultime, infatti, sono state accusate di cyberstalking e di violazione del computer (*computer trespassing*), poiché l’accusa ha sostenuto che l’utilizzo della password della vittima aveva lo scopo di accedere alla sua pagina Facebook con l'intento preciso di imbarazzarla e tormentarla. Se condannate, le ragazze avrebbero potuto scontare fino a 30 giorni di carcere minorile, ma mentre la dodicenne è stata chiamata in giudizio il 10 maggio, l’imputata più giovane è stata sottoposta ad un'audizione che ha determinato la sua incapacità di comprendere appieno i crimini di cui è stata accusata e le è stato dato da assolvere semplicemente un periodo di servizio civile.

Comunque, nel luglio 2011, la King County Juvenile Court ha condannato l’altra ragazza con una “*suspended sentence*”, cioè una sentenza che, in questo caso, ha sospeso la pena per sei mesi affinché la colpevole potesse essere messa alla prova e potesse essere testato il suo effettivo rispetto della legge. Si è trattato di un periodo di “libertà vigilata” in cui la ragazza, oltre a dover svolgere 20 ore di servizio civile, non ha potuto contattare la vittima in nessun modo e il suo utilizzo di internet è stato supervisionato costantemente da un adulto.

Avendo rispettato le suddette condizioni, al termine dei sei mesi il giudice ha fatto cadere le accuse di cyberstalking e di *computer trespassing*.

Si tratta di un risultato estremamente soddisfacente, perché l’intero procedimento ha chiamato in causa sia la legge che la rieducazione, attraverso decisioni che si addicono perfettamente alla giovane età dell’imputata e che hanno avuto come obiettivo quello di correggere i suoi comportamenti così da reprimere gli abusi. Per chi scrive, questo è ciò che dovrebbe essere fatto in tutti i paesi, infatti la tesi sin qui sempre sostenuta è quella che i mezzi debbano essere proporzionati all’entità del crimine e all’età del cyberbullo, affinché possano attivarsi meccanismi di cooperazione tra la legge, le scuole e le famiglie, esattamente come in questo caso. L’obiettivo, infatti, non deve essere necessariamente quello di provocare la detenzione dei colpevoli o di compromettere la loro fedina penale - a meno che non si tratti di illeciti gravi che solo una legge potrebbe distinguere da quelli meno

complessi. In effetti, il semplice fatto di stare in piedi davanti a un giudice ed essere ritenuti responsabili delle proprie azioni - per cui si potrebbe rischiare di non poter salire sullo stesso scuolabus della vittima o di non poter usare il computer senza la supervisione di un adulto - è già un enorme passo verso la rieducazione poiché consente di reprimere gli abusi e prevenire le azioni illecite dimostrandone le conseguenze.

Anche in North Carolina, grazie al *Senate Bill 707*[314], il cyberbullismo viene considerato un illecito punibile sia come comportamento diretto verso i minori, che nel caso in cui venga perpetrato ai danni dei genitori di un minore. Il reato è di classe 1 se l'imputato è maggiore di 18 anni al momento in cui il reato è stato commesso. Se egli, invece, ha un'età inferiore, viene punito come un reato di classe 2. Nel primo caso, il colpevole sconterà da 1 a 120 giorni di «*active, intermediate, or community punishment*»[315], mentre nel secondo, da 1 a 60 giorni.

Nel rispetto di queste previsioni, a Graham (Alamance County, North Carolina), sono stati sanzionati i commenti di Robert Bishop ai danni di Dillion Price. Si è trattato di una serie di dichiarazioni offensive sul compagno di classe allora sedicenne, postate su Facebook da almeno altri cinque studenti della *Southern High School* tra settembre del 2011 e febbraio del 2012. Il 5 febbraio 2014, l'ormai diciottenne Bishop, all'epoca coetaneo di Price, è stato dichiarato colpevole dall'*Alamance County Superior Court* in quanto i suoi post erano destinati a molestare e isolare l'amico.

Ciò si deve al fatto che, oltre a quanto sopra descritto, la legge del North Carolina vieta anche la pubblicazione di informazioni private, personali o sessuali che riguardino i minori, con l'intento di intimidire o tormentare la vittima[316].

Nel caso in esame, infatti, Price aveva erroneamente inviato un messaggio di testo esplicito a un compagno di classe di sesso maschile, in realtà destinato ad una ragazza. Il destinatario sbagliato ha quindi postato uno *screenshot* del messaggio di testo su Facebook, taggando altri studenti e invitandoli a ridicolizzare l'accaduto. Nei

[314] Amends 14-458,1.

[315] Ibid.

[316] Ibid.

commenti, Bishop aveva definito la vicenda come "estremamente omoerotica", affermando pubblicamente sul social network che la vittima era solita praticare attività omosessuali. A ciò aveva fatto seguito una foto modificata di Price impegnato in atti osceni, caricata da un altro compagno di classe della vittima, cui molti ragazzi avevano risposto con link di pagine volgari, imprecazioni e offese.

La madre di Price, Angela Kelly, preoccupata per la quantità di messaggi ingiuriosi diretti al figlio, alla fine del 2011 aveva sporto denuncia all'ufficio dello sceriffo, causando l'arresto di cinque cyberbulli nel novembre 2012.

Delle indagini si è occupato l'*Alamance County Sheriff's Office* e il detective David Sykes, che il 4 febbraio ha presentato ai giurati i post e i *thread* delle attività incriminate, mentre l'assistente del procuratore distrettuale di Alamance County, Brooks Stone, ha affermato che Bishop ha violato la legge statale sul cyberbullismo cercando di prendersi gioco intenzionalmente di Price tramite internet.

Al contrario, l'avvocato difensore, Dan Monroe, ha sottolineato che il suo assistito non ha avuto il "*criminal intent*" necessario affinché vi sia violazione di legge. Inoltre, egli ha sostenuto che alcune delle impostazioni sulla privacy di Facebook consentono agli utenti di bloccare i commenti delle persone che non sono tra gli amici, pertanto visto che i due giovani non avevano stretto amicizia sulla piattaforma, Bishop non si aspettava che Price potesse leggere i suoi post.

Nonostante queste osservazioni, comunque, l'*Alamance County Superior Court* ha condannato l'imputato a 48 mesi di libertà vigilata, durante i quali egli deve pagare 2100 dollari di spese legali e giudiziarie aggiuntive, vietandogli inoltre di utilizzare Facebook o altri siti di social networking per un anno. Anche in questo caso, come in quello di Leslie Cote, il giudice ha emesso una *suspended sentence* di 30 giorni, cui si aggiunge l'impedimento per Bishop di avere alcun contatto con Price o con la sua famiglia. Se nei successivi 12 mesi egli rispetterà quanto stabilito, compreso il fatto di non utilizzare alcuna piattaforma social, potrà essere sottoposto a libertà condizionata senza supervisione.

Gli altri cinque imputati nel caso in esame, che erano già stati dichiarati colpevoli nel 2012 in seguito all'arresto, hanno visto respingere le loro accuse dopo aver scontato un anno di libertà vigilata, grazie ad un "*deferred prosecution agreement*" con il quale il giudice si è impegnato a concedere loro l'amnistia in cambio del

soddisfacimento di determinati requisiti, come quello di scrivere saggi sui pericoli del cyberbullismo o quello di effettuare tra le 36 e le 96 ore di servizi civili, lavorando contemporaneamente con l'ufficio del procuratore distrettuale per parlare di cyberbullismo nelle scuole.
Nella Contea di Alamance, Bishop è stato il primo cyberbullo ad essere processato davanti ad una giuria e il risultato voluto dalla corte è probabilmente lo stesso che si diceva nel caso di Leslie Cote, cioè quello di rieducare e correggere i comportamenti scorretti, così da reprimere gli abusi e scoraggiare il ripetersi di suddetti reati. In questo caso, infatti, oltre ai servizi socialmente utili sono stati comminati anche dei saggi scritti e una collaborazione con la procura, il che dimostra quanto peso viene dato all'istruzione sia nella repressione che nella prevenzione del cyberbullismo.
Nello stesso senso può essere interpretato anche quanto accaduto nel caso di Andrea Paul (vedi *supra* pag. 88), in cui, pur essendo coinvolti due adulti, la *Supreme Court* ha imposto al cyberbullo un ordine preventivo ai sensi del *Cyber-Safety Act* del 2013.
In ogni caso, è evidente che senza una precisa disposizione normativa probabilmente le accuse sarebbero cadute come nel caso di Rebecca Sedwick, in cui Guadalupe Shaw è stata assolta per insufficienza di prove, intesa come mancanza di leggi che individuino un illecito nelle azioni delle loro assistite.

Dunque, Da tutti i casi analizzati, qualunque sia stato il loro esito, emerge la necessità di intervenire su più livelli, così da coinvolgere tutti i settori della società, dall'istruzione e le famiglie alle imprese che si occupano di fornire servizi sul web, affinché l'intera comunità si assuma la responsabilità sociale di tutelare i minori vittime del bullismo elettronico. Tutto questo, ovviamente, deve avvenire all'interno di un quadro di regolamentazione sia nazionale che internazionale, il cui obiettivo non deve essere quello di frenare la libera manifestazione del pensiero su internet, bensì di individuare quali fattispecie costituiscano un reato e di provvedere ad impartire sanzioni che consentano la sospensione scolastica, la cessazione momentanea della disponibilità dei servizi in rete e qualsiasi altro metodo correttivo che potrà essere individuato anche nell'incarcerazione per i casi più gravi.
Si tratta, quindi, di specificare con chiarezza le modalità di configurazione dell'illecito per far sì che ad esso consegua ciò che è giusto e in modo da scoraggiare

le azioni dei cyberbulli, bilanciando la libertà di espressione in rete con la tutela dei diritti della persona. A ciò, poi, per rendere ancora più efficaci le misure repressive, dovrà aggiungersi la previsione di appositi programmi scolastici che insegnino ai giovani, anche in accordo con le più popolari piattaforme di social networking, quali siano i comportamenti da seguire o da evitare nel mondo del web.

Conclusione

L’obiettivo del lavoro svolto era quello di prendere in esame tutte le disposizioni legislative e non, per capire quali fossero gli strumenti di tutela contro il cyberbullismo negli ordinamenti contemporanei e nelle *policies* dei social network, ma soprattutto per riflettere su cosa possa realmente essere intrapreso per evitare questo tipo di abusi online.

Sotto il primo punto di vista, è apparsa estremamente chiara la volontà di organizzazioni sovrannazionali, quali l’Unione Europea e il Consiglio d’Europa, di agire congiuntamente con i governi dei singoli stati, coordinando un intervento di arginamento del fenomeno su più livelli (governativo, scolastico, aziendale).

Parimenti, anche gli enti federali, come quello degli Stati Uniti o quello del Canada, stanno tentando di rispondere a questo tipo di esigenze attraverso la definizione di normative che possano essere omogenee all’interno dei diversi paesi che li compongono.

Tirando le fila dell’intero discorso, le tendenze che appaiono maggiormente condivise a tutti i territori esaminati sono, in primo luogo, quelle che implicano la definizione di unità operative di azione (*task forces*) il cui obiettivo è monitorare ed arginare il fenomeno, come brillantemente eseguito in Nuova Scozia, sullo sfondo di una legge specifica che tutela le vittime del cyberbullismo. Tuttavia, a dimostrazione della necessità di agire anche sul livello educativo oltreché su quello normativo, nei paesi come il Regno Unito e la Nuova Zelanda, queste sono state costituite per fornire gli strumenti necessari a garantire ad adulti e bambini un’alfabetizzazione mediatica che li renda più responsabili e per capire in che modo prevenire e contrastare il bullismo elettronico, lavorando con le agenzie governative, i fornitori di servizi ICT e i rappresentanti del settore dell'istruzione.

In secondo luogo, è impossibile non notare un approccio alla questione del coinvolgimento degli Internet Service Providers che tende da un lato a deresponsabilizzarli, ma dall’altro a richiedergli forti meccanismi collaborativi che si sostanziano sia nelle previsioni contenute nei Termini di Servizio dei social network come YouTube, Facebook, Twitter e Ask.fm che nelle disposizioni normative europee (Direttiva 2000/31/CE). Comunque, anche negli Stati Uniti, in cui si tende

molto di più ad evitare di chiamare in causa i fornitori di servizi e a tutelare le libertà di cui al Primo Emendamento, rimane aperta la possibilità per essi di collaborare su richiesta delle autorità affinché vengano forniti gli elementi necessari alla risoluzione dei casi più gravi.

Questa riflessione porta con sé altre due questioni. La prima, più tecnica, riguarda il reperimento delle prove elettroniche per il quale via via si stanno configurando nuovi scenari all'interno dei singoli stati, come stabilito dalla Convenzione di Budapest sul Cybercrimine e come auspicato nel Regno Unito e in Canada, dove le diverse proposte di legge analizzate hanno anche l'obiettivo di modificare i tempi e le modalità delle indagini di polizia. Infatti, come già visto nei diversi casi di cronaca riportati, è necessario superare un approccio "tradizionale" al crimine giacché la natura del web richiede interventi tempestivi sia nei provvedimenti repressivi che nella racconta delle prove "virtuali" estremamente meno durature di quelle presenti nel mondo "reale".

La seconda questione, invece, riguarda la cooperazione internazionale necessitata dall'a-territorialità della rete, che rende impossibile definire i confini spaziali di azione a disposizione dei singoli stati. Da ciò derivano non soltanto le intese internazionali - come la sovra citata Convenzione di Budapest - ma anche gli accordi presi tra enti sovrannazionali e *providers*, come quello del Safe Harbor, che consente agli utenti di essere tutelati dalle proprie normative nazionali, emanate in virtù delle direttive europee, anche se i server sono allocati in stati esteri che non fanno parte dell'Unione Europea.

In ultimo, si è notato come in tutti i territori la questione del cyberbullismo evochi molti aspetti patologici della rete, che vanno dalla libera manifestazione del pensiero alla pedopornografia, chiamando in causa anche le disposizioni relative alla privacy e agli Internet Service Providers, il che ha dimostrato la complessità e la vastità delle configurazioni del fenomeno.

Proprio per questo si è proposta, nel corso di tutto il lavoro sinora svolto, una maggiore chiarezza relativamente alle *policies* dei social network che molto spesso si riferiscono a disposizioni normative statunitensi pur essendo disponibili nei portali europei. Google, ad esempio, nel rinvio al sito di Chilling Effect, relativamente alla diffamazione cita i codici statunitensi in materia di *false statements of fact*, rendendo

molto complessa per l'utente la comprensione degli strumenti di tutela a sua disposizione negli stati diversi da quelli americani. Ancora, anche Ask.fm rimane piuttosto vago nello specificare se il blocco dell'IP segnalato sia valido per tutti gli utenti (anche quelli anonimi) o unicamente per coloro che posseggono un profilo registrato.

Comunque, in virtù della a-territorialità della rete e delle conseguenze che ciò comporta, si è poi auspicato che venissero adottati provvedimenti il più possibile internazionali, affinché il cyberbullismo potesse essere definito con chiarezza a prescindere dal paese in cui esso avvenga, come già è accaduto per la pedofilia e la pedopornografia grazie alla Convenzione di Lanzarote del 2007. Infatti, mentre ad esempio la Nuova Scozia ha introdotto una legge in proposito che si applica anche agli adulti, negli stati europei e in quelli americani si tende ad identificare il fenomeno come relativo ai rapporti tra minori. Questa confusione sui soggetti rischia di accentuarsi se si tiene conto del fatto che i social network sono attivi nella maggior parte dei territori e devono poter redigere delle *policies* che siano applicabili in modo omogeneo proprio perché gli utenti di tutto il mondo devono essere egualmente tutelati.

Connesso all'aspetto dell'accordo internazionale vi è, poi, l'annosa questione dell'adozione di leggi specifiche all'interno dei singoli stati, affinché il cyberbullismo venga effettivamente riconosciuto come un crimine perseguibile a livello civile e penale. Come spesso si è detto, infatti, ad esso vengono estese le norme già esistenti e relative ad altri reati, sia tradizionali (bullismo, minacce, istigazione al suicidio…) che tipici del web (violazione della privacy, cyberstalking, pedopornografia…), ma ciò si rivela un'arma a doppio taglio, poiché se da un lato consente di garantire almeno un minimo di tutela alle vittime di bullismo elettronico, dall'altro spesso le indagini si risolvono in un nulla di fatto. La vicenda di Rebecca Sedwick, ad esempio, ha dimostrato come l'assoluzione per insufficienza di prove sia sinonimo di mancanza di leggi che individuino un illecito nelle azioni del cyberbullo, a meno che non vi siano dei precedenti di bullismo tradizionale, come nel caso di Emily Moore, o degli illeciti gravi che coinvolgono la pornografia minorile, come nel caso di Carolina Picchio.

Quanto accaduto in North Carolina e nello stato di Washinghton, invece, ha dimostrato gli effetti positivi dell'adozione di disposizioni normative in grado di perseguire il cyberbullismo, poiché in questi casi la presenza di una legge specifica ha consentito di condannare e rieducare i colpevoli per il semplice fatto di stare in piedi davanti a un giudice ed essere ritenuti responsabili delle proprie azioni. Ciò che si è sempre cercato di proporre, infatti, è che attraverso una norma si individuino le modalità di configurazione del fenomeno (durata, tipi di comportamenti illeciti, chi è stato coinvolto, area di accadimento *in/off-campus* ecc…) e le conseguenze ad esso connesse in termini di sanzioni e di intervento scolastico, affinché nei casi più gravi vi possa essere la giusta pena, mentre in quelli meno complessi si possa garantire quantomeno lo scoraggiamento a ripetere l'abuso. Ad esempio, qualora si tratti di un caso isolato, come un video su YouTube o un'immagine offensiva su Facebook, che comunque possono scatenare i commenti negativi o lo scherno della vittima anche a scuola, gli istituti dovrebbero poter applicare una disciplina appropriata: non si tratta solo di prevedere conseguenze legali per il cyberbullo, ma di far sì che ogni scuola abbia un codice di comportamento che regoli i casi di bullismo elettronico prima ancora di rivolgersi alle forze dell'ordine o alle autorità competenti. Sarebbe quindi opportuno coinvolgere un consulente legale, oltre ai genitori e ai professori, nel processo di definizione delle politiche scolastiche, in modo da creare collaborazione, mediazione ed informazione tra la famiglia, la scuola e la legge, così come auspicato dal fortunato esempio della "Piattaforma contro il bullismo" di Facebook (vedi pag. 116).

Comunque, è bene sottolineare che il fatto stesso che vi fosse una norma determinerebbe di per sé il ridursi di questo tipo di attività abusive, proprio perché chi le commette sa che verrebbe punito. Inoltre, le disposizioni, attraverso una definizione chiara e precisa di cyberbullismo, indicherebbero i tempi e i modi che lo rendono tale, così da evitare di sconfinare in provvedimenti meramente censori ed incostituzionali, presi in virtù delle leggi già esistenti e riguardanti altre fattispecie di reati.

Negli Stati Uniti, ad esempio, dove su tutto domina il Primo Emendamento, il fatto che a livello federale non vi sia una legge contro il cyberbullismo ha comportato spesso che non venisse intrapresa alcuna azione - come nel caso di Rebecca Sedwick

- o che, addirittura, la scuola venisse punita per aver limitato la libertà di espressione di uno studente, nonostante essa consistesse in atti offensivi e diffamatori commessi a discapito di un compagno di classe (cfr. causa *J.C. v. Beverly Hills Unified School District* pag. 169).

Parallelamente a ciò, comunque, appare imprescindibile un intervento da parte dei *providers* che dovrebbero assumersi una responsabilità sociale di impresa, intesa come implementazione delle unità che si occupano della risposta alle segnalazioni e dei meccanismi di *report* a disposizione degli utenti, che in alcuni casi, come in quello di Ask.fm, rimangono del tutto insoddisfacenti. Inoltre, una maggiore chiarezza negli strumenti a disposizione (condizioni d'uso, centri per la sicurezza, link ai siti partner ecc…) potrebbe consentire agli utenti di comprendere quali strumenti possano essere utilizzati per tutelarsi, senza doversi necessariamente rivolgere alle autorità competenti, come dimostra la recente ed efficace innovazione della "Piattaforma contro il bullismo" di Facebook (vedi pag. 116) evidenziando ancor più le mancanze degli altri social network analizzati.

Insomma, trattandosi di aziende, esse debbono rispondere a degli standard minimi di qualità per i servizi offerti ed assumersi i rischi d'impresa che non sono da individuarsi nella responsabilizzazione - giacché è impossibile pensare ad un controllo costante di tutti i materiali caricati sul web - piuttosto nell'aumento delle garanzie offerte ai diritti della persona affinché la rete non si tramuti in un territorio affetto da anomia.

Oltre a osservare suddetti strumenti di tutela all'interno delle *policies* e degli ordinamenti, si diceva pocanzi che l'obiettivo del lavoro era anche quello di comprendere in che modo si potessero prevenire gli abusi dei cyberbulli.

Ebbene, a tal proposito, nelle diverse riflessioni condotte è emerso che solamente un intervento coordinato su più livelli può garantire una protezione effettiva dei più giovani rispetto al bullismo elettronico. Infatti è impossibile pensare che una legge basti a scoraggiare gli abusi, poiché essa, per agire sulla prevenzione, dovrebbe essere insegnata affinché ve ne sia un'effettiva conoscenza. Ecco perché, in mancanza di specifiche disposizioni normative, i siti di social networking si rivolgono alle scuole e alle famiglie (vedi Immagine 4), esplicando non solo quali

siano i segnali comportamentali che caratterizzano la vittima di cyberbullismo, ma anche fornendo apposite indicazioni di contatto relative alle autorità competenti.

Immagine C

In Italia, a dimostrazione della necessità di un coinvolgimento delle famiglie, l'articolo 2048 del codice civile definisce le responsabilità genitoriali stabilendo che: «Il padre e la madre, o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi […]». Ciò significa che, ad esempio, una mancata educazione al corretto uso della rete potrebbe comportare una citazione in giudizio dei genitori del cyberbullo a causa dell'omessa vigilanza o della carenza di istruzione. La Corte di Cassazione, con le sentenze 26200/2011 e 20322/2005 ha infatti stabilito che, anche qualora il genitore non abbia potuto impedire il fatto materialmente, ciò non esclude le sue responsabilità. Esse, infatti, si attivano comunque per i genitori dei minori capaci di intendere e di volere, se vi è omissione di vigilanza adeguata e di un'educazione idonea all'età e alla personalità del figlio. Questo tipo di osservazioni sono state applicate anche nei casi di cyberbullismo, come dimostra il Tribunale di Teramo attraverso la sentenza n. 18 del 2012. Nella fattispecie in esame, su Facebook era stato creato da una minorenne un gruppo "Per tutti quelli che odiano L.C." ai danni di una coetanea, i cui genitori avevano sporto denuncia per l'accaduto giacché gli abusi erano stati perpetrati su per 3 giorni consecutivi. A seguito delle audizioni da parte dei legali, si è poi scoperto che il gruppo ingiurioso era stato creato a seguito di una frase offensiva pubblicata dalla stessa L.C.

Così, il giudice ha sentenziato che l'evento dimostrava come entrambe le famiglie avessero omesso il controllo sul recepimento dei valori e dell'educazione da parte dei figli, poiché l'attività offensiva era stata persistente e continua.

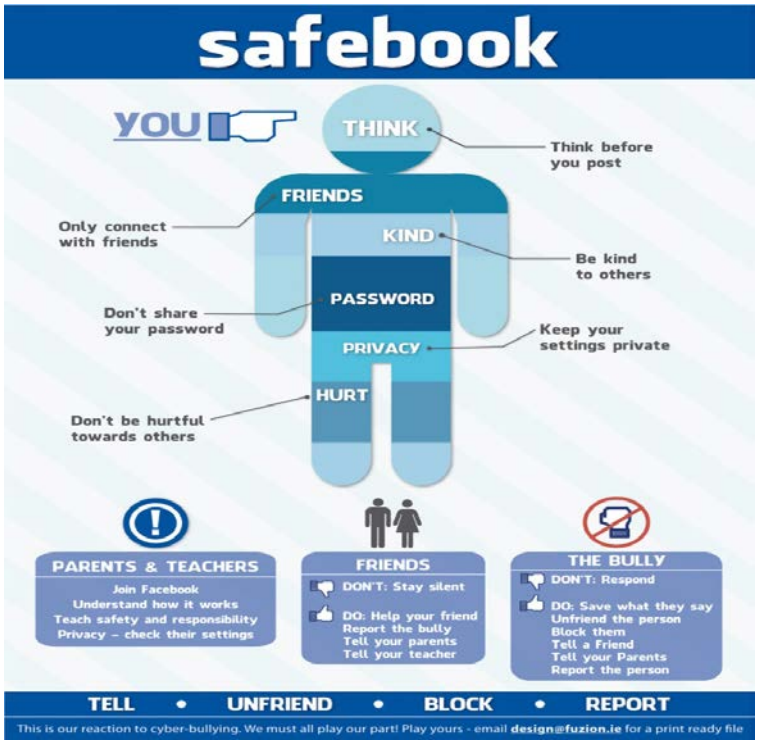
Il fatto che vi fosse stata "provocazione" ha indotto il tribunale a imporre il risarcimento del danno patrimoniale, ma non ha disposto alcuna sanzione per il danno morale soggettivo arrecato. Comunque, il fatto che i genitori siano stati puniti

evidenzia l'effettivo coinvolgimento delle famiglie e dell'educazione cui si faceva riferimento poco fa.

Inoltre, come si è visto, anche le disposizioni scolastiche italiane, statunitensi e canadesi fanno riferimento ai comportamenti degli studenti rispetto sia all'uso di applicazioni mobili, sia riguardo ai comportamenti che negli Stati Uniti vengono definiti "*off-campus*". Ciò dimostra come non si possano trascurare le conseguenze che il bullismo elettronico ha nell'ambiente di apprendimento, che è il motivo per cui, ad esempio, nello stato di Washinghton, in Italia, in Florida, in Ontario, in Québec e in molti altri stati si è imposto un intervento scolastico sia nella prevenzione (istruzione) che nella repressione (richiami o sospensioni) dei reati.

La fondamentale importanza della famiglia e degli insegnanti emerge anche quando si considera l'eventualità dell'adozione di una legge specifica, poiché essa dovrebbe essere insegnata affinché si scoraggino i comportamenti dannosi. Pertanto, è imprescindibile pensare che una modifica nell'ordinamento normativo si dovrà tradurre in un'implementazione della programmazione scolastica, ad oggi ancora insufficiente nell'impartire la cd. "alfabetizzazione digitale". In effetti, gli episodi di bullismo elettronico possono essere il risultato di una mancanza di consapevolezza delle caratteristiche della rete e delle conseguenze che ciò comporta, per cui dire qualcosa di negativo su un coetaneo pubblicamente e sul web significa dare la possibilità a moltissime persone di inoltrare o visualizzare le offese, alimentandole e dando vita ad una vera e propria persecuzione ventiquattro ore al giorno, sette giorni su sette.

Per questo motivo, il sito www.thejournal.ie, ad esempio, ha dato vita ad un infographic molto interessante:



Si tratta di una serie di consigli ai familiari, agli insegnanti, agli amici e alle vittime di cyberbullismo che intendono porre l'accento sulla necessità, innanzitutto, di educare i più giovani al corretto uso della rete attraverso l'istruzione che deve provenire dalla famiglia e dalla scuola in quanto luoghi di socializzazione primaria di ciascun individuo. Ovviamente, visto che come si è affermato spesso, anche i *providers* hanno un ruolo fondamentale nel contrasto al fenomeno, l'immagine si conclude con le parole "*tell*", "*unfriend*", "*block*" e "*report*", che indicano la possibilità del ricorso agli strumenti messi a disposizione del social network.

A livello europeo, a dimostrazione della necessità di un intervento congiunto tra istituzioni ed istruzione, è stato varato il progetto Impact of Relationship[317], finanziato tramite il già nominato *Daphne III Funding Programme*, gestito dall'Associazione AGreenment e da altri 27 partner europei. L'obiettivo principale è quello di insegnare ai ragazzi tra i 10 e i 17 anni l'uso corretto dei social network, sottolineandone l'importanza affinché si possa usufruire della rete senza dover fare i conti con i suoi rischi (furto di identità, cyberbullismo, adescamento ecc…).

[317]Progetto I.O.R. (Impact Of Relationship), JUST/2011/DAP/AG/3255, in www.provincia.rimini.it.

A tal fine, ogni paese europeo ha creato una pagina su Facebook, Twitter e numerose altre piattaforme con cui vengono raggiunti i ragazzi, utilizzando il loro linguaggio per fornire informazioni utili e per sensibilizzarli sulla questione.

Ancora, in Italia a partire da gennaio 2014 (fino al 25 maggio) è stato realizzato il progetto "Una vita da Social" che attraverso le sue 39 tappe, sarà rivolto ad un totale di 150000 studenti tra gli 8 e i 19 anni. Si tratta di un'iniziativa della Polizia di Stato, intrapresa in accordo con il Ministero dell'Istruzione dell'Università e della Ricerca (MIUR) e con numerose aziende che offrono servizi sul web, tra cui soggetti che operano su Internet Facebook, Google, Microsoft, Youtube, Fastweb, Telecom, Vodafone, Wind, Tre, Norton ecc… Lo scopo è quello di insegnare ai più giovani in che modo si possa navigare in rete in modo sicuro, così da sapere come ci si possa difendere dai cyberbulli e dalle attività di adescamento o di frode. Inoltre, all'interno di ogni singolo incontro, oltre al modulo indirizzato ai ragazzi ve ne sarà uno dedicato alle famiglie ed un altro per i docenti, al fine di promuovere il dialogo sul tema del bullismo elettronico e le iniziative didattiche in proposito[318].

Ancora una volta, dunque, si dimostra essenziale la collaborazione di tutti i livelli della società, che chiamano in causa il governo e le sue leggi, le responsabilità di impresa degli ISPs, l'istruzione e la cooperazione internazionale, a dimostrazione che, come si diceva introducendo il presente lavoro, l'offerta di strumenti di tutela contro il cyberbullismo è una questione che riguarda tutti.

[318] www.commissariatodips.it.

Bibliografia

B. A. Areheart, *Regulating cyberbullies through notice-based liability*, in www.yalelawjournal.org

L. Backman, *Traditional bullying and cyberbullying among swedish adolescents*, in kau.diva-portal.org

V. Barkoukis, L. Lazuras, H. Tsorbatzoudis, *A social cognitive perspective in cyberbullying prevention*, in www.bullyingandcyber.net

B. Belsey, *Cyberbullying: an emerging threat to the "always on" generatio*, in www.cyberbullying.ca

P. Burger, *How to stop or remove cyberinfo*, in www.bullypolice.org

M. A. Campbell, *Cyber bullying: an old problem in a new guise?*, Australian Journal of Guidance and Counselling, 2005

M. Centorrino, *Bulli, pupe e videofonini*, Bonanno, Roma 2009

M. Cuniberti, *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Giuffrè, Milano 2008

R. Donegan, *Bullying and Cyberbullying: history, statistics, law, prevention and analysis*, in www.elon.edu

Eurispes, Telefono Azzurro, *Indagine nazionale sulla condizione dell'infanzia e dell'adolescenza*, Roma 2011

European Union 2008 COST action IS0801, *Guidelines for preventing cyber-bullying in the school environment: a review and recommendations*, in www.bee-secure.lu

A. Ferguson, *Online bullying*, The Rosen Publishing Group, 2013

G. Gardini, Le *regole dell'informazione. Principi giuridici, strumenti, casi*, Mondadori, Milano 2009

M. L. Genta, A. Brighi, A. Guarini, *Bullismo elettronico. Fattori di rischio connessi alle nuove tecnologie*, Carocci, Roma 2009

M. L. Genta, A. Brighi, A. Guarini, *Cyberbullismo. Ricerche e strategie di intervento*, Franco Angeli, Milano 2013

B. High, *Bullycide*, JBS Publishing, Washington 2007

S. Hinduja, J. W. Patchin, School *climate 2.0: preventing cyberbullying and sexting one classroom at a time*, Sage Publications, 2012

S. Hinduja, J. W. Patchin, *Cyberbullying prevention and response: expert perspectives*, Routledge, 2012

S. Hinduja, J. W. Patchin, *Bullying beyond the schoolyard: preventing and responding to cyberbullying*, Sage Publications, 2010

S. Hinduja, J. W. Patchin, *Cyberbullying: An exploratory analysis of factors related to offending and victimization*, Deviant Behavior, 2008 (129–156)

S. Hinduja, J. W. Patchin, *Offline consequences of online victimization: school violence and delinquency*, Journal of School Violence, 2007 (89–112)

S. Hinduja, J. W. Patchin, *State cyberbullying laws*, 2014 in cyberbullying.us

S. Hinduja, J. W. Patchin, *Cyberbullying Research Summary. Emotional and psychological consequences*, Cyberbullying Research Center, 2009 in www.cyberbullying.us

S. Hinduja, J. W. Patchin, *Preventing cyberbullying: top ten tips for teens*, Cyberbullying Research Center, 2009 in www.cyberbullying.us
N. Hunter, *Cyber Bulling (Hot topics)*, Heinemann Educational Books, 2011

N. Iannaccone, *Stop al Cyberbullismo*, La meridiana, Molfetta 2009

IPSOS per Save the children, *Report: Safer Internet Day Study – Il cyberbullismo*, Italia 2014

iSafe America, 2004 Survey of students nationwide, *Cyber Bullying: statistics and tips*, in www.isafe.org

C. Kim, *CDA §230 and its influence in shaping the role of Internet service providers: implications for the future of cyber-bullyin*, in legalstudies.lscrtest.com

A. V. King, *Constitutionality of cyberbullying laws: keeping the online playground safe for both teens and free speech*, in www.vanderbiltlawreview.org

R. M. Kowalski, S. P. Limber, P. W. Agatston, *Cyber bullying: bullying in the digital age*, John Wiley&Sons, 2010

Q. Li, D. Cross, P. K. Smith, *Cyberbullying in the global playground: research from international perspectives*, Blackwell Publishing Ltd., Chichester 2012

S. Livingstone, L. Haddon, A. Görzig, K. Oláfsson, *Risks and safety on the Internet: the perspective of European children*, LSE London, 2011

Ministerial Briefing Paper, Law Commission, *Harmful digital communications: the adequacy of the current sanctions and remedies*, Wellington, New Zealand, August 2012, in www.lawcom.govt.nz

Ministero dello sviluppo economico, Bozza del codice di autoregolamentazione per la prevenzione e il contrasto del cyberbullismo, 8 gennaio 2014 in www.sviluppoeconomico.gov.it

M. B. Morano, D. Valentino, *Più scuola meno mafia e cyberbullismo. Contrasto alle nuove forme di devianza giovanile*, Annali della pubblica Istruzione, 6/2012

D. Olweus, *A useful evaluation design and effects of the Olweus bullying prevention program*, Psychology, Crime & Law, 2005

B. O'Neill, E. Staksrud, S. McLaughlin, *Towards a better internet for children? Policy pillars, players and paradoxes*, Nordicom, 2013

G. Pascuzzi, *Il diritto dell'era digitale*, Il Mulino, Bologna 2010

L. Petrone, M. Troiano, *Dalla violenza virtuale alle nuove forme di bullismo*, Magi, 2008 Roma

C. Pickering, *The jury has reached its verdict ... Or has it? Cyberbullying in the canadian legal arena*, in www.teachers.ab.ca

G. Pini, *Un computer per i giochi di nostro figlio*, Intruso, Roma 2001

N. Pinna, M. E. Saturno, L. Pisano, *Prevenire il cyberbullismo e la navigazione online a rischio - Linee guida per genitori*, in www.cyberbullismo.com

N. Pinna, M. E. Saturno, L. Pisano, *Prevenire il cyberbullismo e la navigazione online a rischio - Linee guida per docenti*, in www.cyberbullismo.com

N. Pinna, M. E. Saturno, L. Pisano, *Prevenire il cyberbullismo e la navigazione online a rischio - Linee guida per studenti*, in www.cyberbullismo.com

Research by J. W. Patchin, S. Hinduja, A. Schafer, *Cyberbullying and Sexting: Law Enforcement Perceptions*, 2010-2011

M. E. Saturno, L. Pisano, *Differenze tra bullismo e cyberbullismo*, in www.cyberbullismo.com 2008

S. Shariff, *Confronting cyber-bullying*, Cambridge University Press, 2009

P. K. Smith, *An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying*, 2006 in www.anti-bullyingalliance.org.uk

C. Sunstein, *Republic.com*, Princeton University Press, 2001

S. M. Taylor, *Cyberbullying penetrates the wall of traditional classroom*, in circle.adventist.org

T. Tedford, D. Herbeck, *Freedom of speech in the United States*, Strata Publishing Inc., State College 2009

The Report of the Byron Review, *Safer Children in a Digital World*, Department for Children, Schools and Families, and Department for Culture, Media and Sport, in www.dcsf.gov.uk

G. Titley, *Realities And Threats Of Hate Speech Online For Young People Today*, Oral presentation during the European Online Youth Campaign Against Hate Speech Preparatory Seminar (Eycs), Strasbourg, October 2012

E. Volokh, *First Amendment and Related Statutes: Problems, Cases and Policy Arguments*, Foundation Press, 2008

Various participants, *Workshop: The legal aspects of cyberbulling*, University of Antwerp, 2010

N. E. Willard, *Cyberbullying and cyberthreats: responding to the challenge of online social aggression, threats and distress*, Research Pr Pub, 2007

Wired Safety, *Reporting Terms of Service Violations*, 2010, in www.wiredsafety.org

Sitografia

antibullying.novascotia.ca

anti-bullyingalliance.org.uk

apps.leg.wa.gov

archive.org

ask.fm

assembly.coe.int

blogs.edweek.org

books.google.it

brage.bibsys.no

bullying.about.com

coroners.leicester.gov.uk

definetheline.ca

dev.twitter.com

dirittodigitale.com

dubestemmer.no

ec.europa.eu

edition.cnn.com

emsoc.be

eur-lex.europa.eu

export.gov

feedback-form.truste.com

fundforcivility.org

globalnews.ca

help.instagram.com

hub.coe.int

inchieste.repubblica.it

it.norton.com

it.wikipedia.org

laws-lois.justice.gc.ca

loveourchildrenusa.org

mediasmarts.ca

news.nationalpost.com

nobullying.com

nohate.ext.coe.int

nslegislature.ca

o.canada.com

productforums.google.com

roma.corriere.it

safeharbor.export.gov

sites.google.com

stopcyberbullying.org

support.google.com

support.twitter.com

thechronicleherald.ca

thediplomat.com

tvnz.co.nz

wcd.coe.int

www.abc.net.au

www.aleteia.org

www.altalex.com

www.ansa.it

www.arkleg.state.ar.us

www.askthejudge.info

www.azzurro.it

www.bbc.com

www.bullyfree.com

www.bullyfreealberta.ca

www.bullying.co.uk

www.bullyingandcyber.net

www.bullyingstatistics.org

www.bullyonline.org

www.canadainternational.gc.ca

www.cbc.ca

www.change.org

www.childline.org.uk

www.chillingeffects.org

www.cittadinanzattiva.it

www.codacons.it

www.coface-eu.org

www.coface-eu.org

www.commissariatodips.it

www.cps.gov.uk

www.criminaljustice.ny.gov

www.cyberbullying.ca

www.cyberbullying.org.nz

www.cyberbullying.se

www.cyberbullying.us

www.cyber-bullying-facts.com

www.cyberbullyingnews.com

www.cyberbullyingprevention.com

www.cyberscan.novascotia.ca

www.cybersmile.org

www.cybertraining-project.org

www.cyfernet.org

www.dcsf.gov.uk

www.deletecyberbullying.org

www.diritto.it

www.dirittoegiustizia.it

www.dosomething.org

www.endcyberbullying.org

www.endcyberbullying.org

www.europarl.europa.eu

www.eu-un.europa.eu

www.facebook.com

www.fbi.gov

www.foxnews.com

www.garanteprivacy.it

www.getcybersafe.gc.ca

www.giovaniemedia.ch

www.gop.gov

www.gov.uk

www.gu.se

www.helpconsumatori.it

www.helpguide.org

www.huffingtonpost.com

www.ifos-formazione.com

www.ilfattoquotidiano.it

www.ilmattino.it

www.independent.co.uk

www.informagiovani-italia.com

www.justice.gc.ca

www.kidsandmedia.co.uk

www.lastampa.it

www.lawcom.govt.nz

www.lba.k12.nf.ca

www.leg.state.nv.us

www.leginfo.ca.gov

www.legis.la.gov

www.legislation.govt.nz

www.lemonde.fr

www.mcafee.com

www.medialaws.eu

www.medialiteracy.org

www.mespa.net

www.minedu.govt.nz

www.mirror.co.uk

www.mlaw.gov.sg

www.ncpc.org

www.netsafe.org.nz

www.nj.com

www.nohatespeechmovement.org

www.nspcc.org.uk

www.nzherald.co.nz

www.oco.ie

www.osservatoriopedofilia.gov.it

www.overcomebullying.org

www.pewinternet.org

www.poliziadistato.it

www.provincia.rimini.it

www.qp.alberta.ca

www.rai.it

www.risky-re.it

www.safenetwork.org.uk

www.savethechildren.it

www.sec-ed.co.uk

www.senate.mo.gov

www.smontailbullo.it

www.socialspacescuo.be

www.stateofmind.it

www.staysafeonline.org

www.stopbullying.gov

www.stopbullyingworld.org

www.st-richards.org.uk

www.stuff.co.nz

www.sviluppoeconomico.gov.it

www.teachtoday.eu

www.telecompaper.com

www.telegraph.co.uk

www.theglobeandmail.com

www.theguardian.com

www.thejournal.ie

www.thinkuknow.co.uk

www.tolerance.org

www.unar.it

www.unicef.it

www.upi.com

www.usconstitution.net

www.violencepreventionworks.org

www.wiredsafety.org

www.wisekids.org.uk

www2.gnb.ca

Filmografia e Videografia

Cyberbully, regia di Charles Binamé, 2011

Disconnect, regia di Henry Alex Rubin, 2103

Block bullying online! Keep the Internet fun! Keep control!, European Commission, in www.youtube.com

My story: Struggling, bullying, suicide, self harm, TheSomebodytoknow, in www.youtube.com

End Cyberbullying 2014 | ETCB Organization, End to Cyber Bullying, in www.youtube.com

Cyberbullying: there is a way out!, DeleteCyberbullying, in www.youtube.com

Think Time: How Does Cyberbullying Affect You?, My Secure Cyberspace, in www.youtube.com

Connettilatesta!, video tutorial del Garante per la privacy, in www.garanteprivacy.it

Carolina, vittima del cyberbullismo, Lucignolo, in www.video.mediaset.it