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 **P**rof.
Pietro Santo Leopoldo Falletta

CANDIDATO

Camilla Bistolfi
MATR. 620722

CORRELATORE

PROF. Michele Sorice

ANNO ACCADEMICO 2013/2014

Indice

Il termine cyberbullismo è stato coniato nel 2005 dall'insegnante canadese Bill Belsey, per identificare l'uso delle nuove tecnologie finalizzato a supportare un atto o una serie di comportamenti prepotenti ed ostili, perpetrati da bambini e ragazzi nei confronti dei loro coetanei attraverso non soltanto gli SMS/MMS e le telefonate, ma anche e soprattutto grazie all'utilizzo della rete. Quest'ultima, infatti, offre un'ampia varietà di strumenti che possono essere utilizzati dal cyberbullo per perseguitare la sua vittima. In particolare, estremamente diffusa è la creazione di appositi siti web, blog o forum nonché la pubblicazione di materiali offensivi e diffamanti sulle pagine dei social network (sondaggi, post, immagini, video ecc…). A questo tipo di azioni spesso si accompagnano le minacce e le umiliazioni via chat o via e-mail, che rendono l'abuso ancor più pervasivo, articolandolo sia nella sfera privata (*one-to-one*) che in quella pubblica (*one-to-many*).

Grazie alle proprietà della rete, suddetti comportamenti virtuali sono accessibili a chiunque in qualsiasi momento e possono essere messi in atto anonimamente, diffondendosi sino al punto di diventare atteggiamenti collettivi. Le conseguenze di ciò, esplodono violentemente nella vita reale, causando l'isolamento della vittima e, a volte, persino il suo suicidio, giacché non esiste luogo in cui essa possa rifugiarsi per sfuggire alle persecuzioni.
Queste caratteristiche hanno reso il bullismo elettronico identificabile come un tipo di *hate speech*, poiché l'intento è esattamente quello di mettere in ridicolo, screditare e offendere la vittima, cercando di convincere chi legge ad odiarla ed insultarla a sua volta. Spesso, poi, le molestie non si limitano ad affermazioni ingiuriose relative alla persona e al suo aspetto, ma vengono perpetrate dando origine a una diffamazione discriminatoria che verte sulle qualità del soggetto (età, sesso, razza, religione, orientamento sessuale, handicap).
Per questo, è necessario comprendere quale sia il corretto bilanciamento tra libertà di manifestazione del pensiero e gli altri diritti della personalità, quali l'onore, la reputazione e l'identità personale.
Il cyberbullismo, però, 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*, un processo continuo di molestie, caratterizzato dalla persecuzione via web che procura nella vittima stati di ansia o di paura (comprendente le minacce e il furto di identità). Questa descrizione spiega perché, in molti casi, laddove non vi è una legge contro il bullismo elettronico, si cerca di estendere le previsioni sullo stalking al fenomeno in analisi.
Oltre alla messaggistica istantanea, all'uso di forum, blog e social network, il cyberbullo può avere come obiettivo quello di impossessarsi della chiave di accesso della sua vittima o quello di creare un falso profilo per impersonarla e contattare altre persone a suo nome.
Tutte queste tipologie di abusi rispecchiano la complessità del fenomeno, che chiama in causa sia i crimini informatici (*identity fraud*, furto di password, *hacking*) che gli illeciti più tradizionali (diffamazione, discriminazione, minacce, molestie, persecuzioni) unitamente al fatto che i messaggi offensivi spesso hanno lo scopo di diffondere in rete foto scattate senza il permesso del soggetto, immortalato nudo o svestito (cd. *sexting)*, il che, coinvolgendo dei minori, si identifica nella pedopornografia.
La varietà di configurazioni del cyberbullismo va, poi, a sommarsi alla possibilità, offerta dalla rete, di restare anonimi o di creare falsi account, rendendo difficile rintracciare coloro da cui hanno origine le prepotenze.

Si pone, in tal senso, l'annosa questione della privacy, che investe nello specifico il ruolo degli Internet Service Providers nel comunicare i dati personali degli utenti, al fine di renderli rintracciabili per risolvere i casi di bullismo elettronico. E, ancora, sempre a proposito dei prestatori di servizi, bisogna stabilire quando e come essi siano chiamati ad agire, dalla legge e dalle loro *policies*, per porre fine agli illeciti di tal genere, pur mantenendo l'assenza di responsabilità per i contenuti immessi sulla rete dagli utenti.
L'aspetto interessante del fenomeno, dunque, risiede nella sua capacità di richiamare i temi più importanti e complessi che sono sorti con l'uso (e abuso) della rete, quali quello dell'estendibilità dei reati tradizionali al mondo del web e della possibilità di adottare legislazioni *ad hoc*, quello dell'educazione digitale di adulti e ragazzi, ma anche quello della responsabilità degli ISPs e del loro obbligo di collaborare con le autorità nel rispetto delle norme sulla privacy.
Ciò che si intende dimostrare con questo lavoro è proprio la necessità di un intervento per prevenire e contrastare il fenomeno, che sia coordinato su più fronti. Innanzitutto, attraverso l'adozione di norme giuridiche, che favoriscano la regolazione del fenomeno e la tutela delle vittime a livello statale e sovrannazionale. In secondo luogo, a partire da queste disposizioni, è indispensabile che gli Internet Service Providers adottino dei codici di autoregolamentazione che gli consentano di gestire le situazioni a rischio, mantenendo comunque l'originaria libertà di manifestazione del pensiero sul web, senza dimenticare che essi posseggono una responsabilità sociale di impresa. Quest'ultima va intesa come implementazione delle unità che si occupano della risposta alle segnalazioni e come aumento dei meccanismi di *report* e di supporto a disposizione degli utenti. In terzo luogo, non si può prescindere da un intervento che coinvolga la famiglia, alla quale spetta il compito di supportare i più giovani nell'approccio alle nuove tecnologie, assieme alla scuola, che deve svolgere un'attività di prevenzione e sostegno. Ciò chiama in causa, ancora una volta, il ruolo dello stato e degli enti sovrannazionali, cui spetta l'onere di fornire agli insegnanti gli strumenti necessari e le competenze adatte ad arginare il fenomeno.
Dunque, la necessità di un *frame* normativo solido, di una forte attività statale di promozione scolastica ed extrascolastica, ma soprattutto l'esigenza di un comportamento responsabile da parte degli ISPs, evidenzia il fatto che il cyberbullismo è una questione che riguarda tutti i settori della società, il cui ruolo è stato analizzato nel corso di questo lavoro.

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 quanto riguarda gli Stati Uniti le disposizioni costituzionali vengono messe a dura 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. A livello federale, infatti, non esistono leggi specifiche contro il bullismo elettronico, nonostante nel 2009 fosse stato presentato un disegno di legge (Megan Meier Cyberbullying Prevention Act) con lo scopo di modificare il titolo 18 dello United States Code ed inserire apposite previsioni contro i reati di bullismo elettronico perpetrati sia all'esterno che all'interno della scuola, indirizzati o commessi sia da ragazzi che da adulti.
Tuttavia, in assenza di leggi che puniscono il crimine di cyberbullismo, le vittime possono solo ricorrere ai reati ad esso assimilabili come le molestie e le minacce, l'*offensive speech*, il *false statements of fact* o il *cyberstalking*.

Per questo, a livello federale, si tende a fare riferimento a tre statuti come base della protezione contro il bullismo elettronico: il Titolo IX degli *Education Amendments* del 1972; il titolo VI del *Civil Rights Act* del 1964; l'*Americans with Disabilities Act* (ADA).
Unitamente a ciò, nel caso in cui vi sia qualsiasi minaccia di nuocere ad una persona potrà essere applicato l'*Interstate Communications Act*, che però non copre quei casi in cui il danno sia meramente psicologico o immateriale. Anche il *Computer Fraud and Abuse Act*, che rende un crimine l'uso non autorizzato del computer, può essere applicato solo ad un segmento ristretto di forme di bullismo elettronico (ad es. furto di identità o di password).
A livello federale, dunque, rimangono piuttosto insoddisfacenti le previsioni a tutela delle vittime di cyberbullismo, così come nella maggior parte degli stati non vi sono previsioni penali relative al fenomeno. Infatti, secondo il recente resoconto del *Cyberbullying Research Center*[1], solo sette stati hanno delle norme specifiche per il fenomeno e lo considerano un crimine: l'Arkansas (*Cyberbullying crime law* del 2011); la Louisiana (sezione "*Families in Need of Services"* del *Children's Code*[2]); il Missouri (*Senate Bills nos. 818&795*); il Nevada (§392,915 del *Revised Statue* del 2013); il North Carolina (*amends 14-458,1* del *Senate Bill 707*); il Tennessee (*Senate Bill 113*); lo stato di Washinghton (*Bullying Act* del 2007 e *Cyberstalking Law*[3]).

Anche all'interno dell'Europa non vi è ancora, dal punto di vista sovrannazionale, un intervento normativo concreto, nonostante sia l'Unione Europea che il Consiglio d'Europa tutelino l'infanzia e l'adolescenza, pur garantendo la libera espressione (art. 11 della Carta dei Diritti Fondamentali dell'UE e art. 10 della Convenzione Europea dei Diritti dell'Uomo del Consiglio d'Europa).
Consapevoli del fatto che suddetta libertà possa degenerare nella comunicazione/ricezione di contenuti offensivi e violenti sul web, non adatti ai minori, questi due organismi hanno intrapreso numerose iniziative.
Durante il *Safer Internet Day*[4] del 2009 (10 febbraio), ad esempio, la Commissione Europea ha lanciato la campagna contro il cyberbullismo con la partecipazione di tutti gli stati membri e anche di Islanda e Norvegia. Inoltre, nell'ambito del *Daphne III Funding Programme*, dal 1 febbraio 2013 ha preso vita il progetto *Delete cyberbullying*[5], attivo fino a giugno 2014, con l'obiettivo di collaborare insieme a partner internazionali per sviluppare un approccio comune alla prevenzione dei rischi e alla stesura di linee guida per insegnanti, genitori, bambini e altre parti interessate (providers, legislatori, autorità garanti ecc…).
Anche il programma *European Strategy for a Better Internet for Children* del 2012, promosso dalla Commissione nell'ambito dell'Agenda Digitale Europea, ha lo scopo di fornire ai bambini le competenze digitali di cui hanno bisogno per godere del web in modo sicuro attraverso l'insegnamento in tutte le scuole dell'UE.
Inoltre, nel novembre del 2012, gli Stati Uniti e l'Unione Europea, entrambi sprovvisti di una legislazione specifica, si sono uniti nella lotta al fenomeno, attraverso la *EU and US Joint*

[1] S. Hinduja, J. W. Patchin, *State cyberbullying laws*, febbraio 2014 in cyberbullying.us.
[2] *House Bill 1259, Act No. 989*, in www.legis.la.gov.
[3] Revised Code of Washinghton §9.61.260, Cyberstalking.
[4] Parte del Safer Internet Programme (IP/08/1899) della Commissione Europea.
[5] deletecyberbullying.eu.

Declaration to Make the Internet Safer for Kids con l'obiettivo di lottare insieme contro gli abusi online.
Per quanto riguarda il Consiglio d'Europa, nell'aprile 2011, il Comitato dei ministri ha adottato la *Declaration on Internet Governance Principles*[6], per dare corretta applicazione alla Convenzione Europea dei Diritti dell'Uomo da parte di ciascuno stato membro anche nella realtà online, con particolare riguardo alla tutela dei bambini nella società dell'informazione, sia per quanto riguarda lo sviluppo dell'alfabetizzazione digitale che per la loro protezione contro i contenuti dannosi.
Da questo approccio è nata la campagna (2012-2014), gestita dallo *Youth Department of the Council of Europe*, "*No hate speech movement*" che mira a definire le linee guida per le *policies* da adottare nei singoli stati affinché si combatta il razzismo e la discriminazione online, ma anche l'incitamento all'odio sul web, in tutte le sue forme, compreso il cyberbullismo.
Quindi, similmente agli 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.
Insomma, come già evidenziato per USA e UE, anche per il Consiglio d'Europa la dimensione del web richiede un'azione multilivello, intrapresa sia dalle istituzioni che dai cittadini, con l'obiettivo di fornire alle vittime una maggiore protezione legale e un più forte sistema di prevenzione.

Nel contrasto al fenomeno del cyberbullismo, gli Internet Service Providers ricoprono un ruolo fondamentale, dal momento che essi offrono agli utenti gli spazi in cui hanno luogo gli abusi.
A questo proposito, l'Unione Europea, con la direttiva 2000/31/CE sul commercio elettronico, ha escluso la possibilità di attribuire agli ISPs un obbligo generale di sorveglianza o di ricerca attiva degli illeciti nella prestazione dei servizi di *mere conduit*, *catching* e *hosting*, fermo restando il loro obbligo di collaborare con le autorità competenti affinché si ponga fine ad una violazione o la si impedisca. Inoltre, pur nel rispetto delle norme sulla privacy, i prestatori di servizi della società dell'informazione devono informare «senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o 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»[7].
Negli Stati Uniti, invece, la *Section 230* del *Communications Decency Act* (CDA) garantisce ai providers, in ogni caso, l'immunità dalla responsabilità nel paragrafo c, intitolato "*Protection for "Good Samaritan" blocking and screening of offensive material*". In esso si stabilisce che l'ISP non è responsabile per i contenuti immessi dagli utenti né 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.

In Italia, l'8 gennaio 2014, è stata approvata la prima bozza del Codice di Autoregolamentazione per la prevenzione e il contrasto del cyberbullismo, redatta dal Ministero dello Sviluppo

[6] 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.
[7] Art. 15, Direttiva 2000/31/CE.

Economico, 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 (Confindustria digitale, Assoprovider, Google, Microsoft…). L'obiettivo è sia quello di contrastare il fenomeno attraverso l'autoregolazione, che quello 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»[8].
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.
A livello ministeriale, oltre alla Direttiva del MIUR n. 16 del 2007, sul ruolo della scuola nella prevenzione del bullismo tradizionale ed elettronico, che deve essere articolata in specifici programmi di informazione ed educazione, vi è anche la Direttiva Ministeriale n. 104 del 2007, riferita ai casi di violazione della privacy ed abuso dell'immagine altrui all'interno degli istituti.
Posto che nell'ordinamento italiano non è presente una norma relativa al cyberbullismo, al fenomeno, vengono applicate le previsioni relative a fattispecie già esistenti nel codice penale, fermo restando 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 gli 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.
Comunque, con riferimento alla protezione della privacy, il cyberbullo può essere punito ai sensi dell'art. 615-bis c.p. sull'appropriazione indebita di audio o video con l'aggravante per «chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini» in questione.
Vi sono, poi, i casi di ingiuria previsti dall'art. 594 c.p., che stabilisce la possibilità di punire chiunque «offende l'onore o il decoro di una persona presente», con un'aggravante nei casi in cui «l'offesa sia commessa in presenza di più persone». Spesso, inoltre, la vittima si appella 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» e prevede un'aggravante della pena se l'offesa viene arrecata con un «mezzo di pubblicità».
In ognuno di questi casi l'art. 120 c.p. stabilisce 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».
Altri due reati estendibili al fenomeno in esame sono quelli previsti dall'art. 610 c.p. (violenza privata), dall'art. 612 c.p. (minacce e minacce gravi), dall'art. 528 c.p. (pubblicazioni oscene) oppure dagli artt. 600bis, ter e quater del codice penale, relativi alla pedopornografia ed applicabili ai casi di *sexting*. Ancora, se 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 oppure dall'art. 615quinquies nel caso in cui utilizzi programmi «diretti a danneggiare o interrompere un sistema informatico».

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

In Gran Bretagna spicca senz'altro, all'interno del *Department for Children, Schools and Families*, la creazione della *Cyberbullying Taskforce*, la quale, a seguito del *Byron Review Action Plan* del 2008, ha il compito di studiare e monitorare il fenomeno per proporre dei rimedi attraverso raccomandazioni dirette al governo, alle forze di polizia e alle scuole.
A livello legislativo, invece, per proteggere le vittime del fenomeno, si distingue tra comunicazioni che possono costituire minacce credibili di violenza alla persona o di danni materiali e quelle comunicazioni che invece colpiscono specificamente un individuo o un gruppo e che possono configurarsi come molestie o stalking, entrambe tutelate dal *Protection from harassment Act* del 1997. Tuttavia, anche le comunicazioni che non rientrano in nessuna delle due categorie sopracitate, ma che sono grossolanamente offensive, indecenti, oscene o false, possono essere tutelate se avvengano su un social media, come nel caso del cyberbullismo.
In quest'ultimo caso, infatti, la tutela è offerta dalla *Section 1* del *Malicious Communications Act* (se la comunicazione elettronica ha l'intento di causare disagio o ansia nel destinatario, attraverso contenuti indecenti o offensivi, oltreché falsi o trasmessi con identità nascosta) o dalla *Section 127* del *Communications Act* che si applica anche all'invio di messaggi di carattere "intimidatorio" attraverso una rete pubblica di telecomunicazioni, cioè alle minacce credibili. A queste ultime, poi, si può applicare anche la sezione n.16 dell'*Offences Against the Person Act*, qualora si dichiari di voler uccidere una persona, parallelamente all'uso dell'art. 4 del *Protection From Harassment Act*, se le intimidazioni consistono in una condotta continuativa.
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*, 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 nel caso britannico, dunque, manca del tutto la previsione di illeciti relativi al cyberbullismo, per questo nel marzo 2014 il *Criminal Justice and Courts Bill Committee* si è riunito per discutere un possibile emendamento al *Criminal Justice and Courts Act*, in modo da introdurre una condanna fino a due anni di carcere per i colpevoli di bullismo elettronico e di "*text-message abuse*".

In Nuova Zelanda, come nel Regno Unito, è stata creata la *National Cyber Bullying Taskforce*, che ha il compito di comprendere come 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. Similmente ad Europa e Stati Uniti, dunque, anche in questo caso non si cercano solo rimedi giuridici, bensì l'obiettivo è quello di mantenere un approccio *multi-stakeholder*s al fenomeno che, comunque, gode di tutele pre-esistenti quali: il *Defamation Act* del 1992, la *Section 15* del *Crimes Amendment Act* del 2003[9], la *Section 5* del *Crimes Amendment Act* del 2011[10], la *Part 9A* della *Crimes Law* (*personal privacy* e «*intimate visual recording*), il *Summary Offences Act* alla *Section 2* (intimidazione consapevole), l'*Harassment Act* (molestia ripetuta in almeno due occasioni diverse e nell'arco di tempo di 12 mesi o più).
Comunque, nel maggio 2013, è stato proposto l'*Harmful Digital Communications Bill*, che vorrebbe l'introduzione di un'*Agency* incaricata di investigare sui casi di cyberbullismo e di

[9] *Accessing computer system for dishonest purpose.*
[10] Accessing *computer system without authorization.*

risolverli innanzitutto con la mediazione, per poi passare alla *District Court* nel caso la controversia non venga risolta.

In Canada, a livello federale, esistono due approcci al fenomeno. Il primo è relativo alle molestie, disciplinate dalla *Section 264* del *Criminal Code*, 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 famiglia. 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. Il secondo approccio, invece, riguarda la diffamazione, protetta dalla *Section 301*, che per la pubblicazione di calunnie può riferirsi al bullismo elettronico nel caso in cui, ad esempio, internet venga utilizzato per ridicolizzare la vittima attraverso affermazioni o pubblicazione di immagini.
Inoltre, sempre all'interno del *Criminal Code*, 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 la *Section 403* si riferisce all'*Identity fraud*.
In ambito scolastico, ai sensi del *Constitution Act* (*Legislation respecting Education*) 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 l'atto avvenga fuori dall'istituto e via web.
Comunque, nel novembre del 2013, il Parlamento ha iniziato le discussioni sul *Bill C-13*, intitolato proprio "*The Protecting Canadians from Online Crime Act*" che 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. Si introdurrebbe così la possibilità di avere accesso ai dati e di conservarli, per acquisire prove elettroniche che consentano una maggiore tutela delle vittime, soprattutto laddove il colpevole si nasconde dietro l'anonimato. Inoltre, 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, 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. In aggiunta a ciò, la proposta di legge andrebbe a vietare la distribuzione non consensuale delle immagini intime per fronteggiare il cd. *sexting*.
A livello nazionale, invece, tra tutti gli stati canadesi soltanto la Nuova Scozia ha una legge specifica contro il bullismo elettronico. Si tratta del *Cyber-Safety Act*, approvato nell'agosto 2013, che 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. Inoltre, 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.
Un'altra novità del *Cyber-Safety Act* è la creazione della *CyberScan Unit*, composta da cinque investigatori che hanno il compito di rispondere a tutte le denunce di bullismo elettronico. Chiunque 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 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[11].
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.
Similmente, nella Repubblica di Singapore, Il *Factsheet on the protection from Harassment Act 2014* applica esplicitamente alla rete gli stessi standard di ciò che costituisce reato nel mondo reale e consente alla vittima di richiedere ai tribunali di applicare *protection order* contro il molestatore, affinché ad esso sia imposto di desistere dal perpetrare l'abuso, sia che si tratti di *sexual-harassment*, di cyberbullismo o di stalking, anche commessi al di fuori di Singapore.
Dal punto di vista penale, il colpevole degli illeciti previsti verrà multato fino a S$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.

In questo contesto, i social network costituiscono sia uno strumento di relazione che una minaccia diretta per i giovani che ne fanno uso, dal momento che, come si è visto, non vi sono norme a livello sovrannazionale né statale - salvo eccezioni - che tutelino i giovani rispetto al cyberbullismo. Per questa ragione è essenziale comprendere quali siano gli strumenti messi a

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

disposizione dalle piattaforme di social networking per prevenire, arginare e reprimere il fenomeno.
L'Unione Europea, in proposito, 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. Nonostante ciò, però, ciascun social ha la sua *policy*, che può o meno rispondere in modo soddisfacente alle richieste degli stati di tutelare i giovani dalle minacce della rete, tra cui spicca il bullismo elettronico. Di questo fenomeno, inoltre, ne esistono ben due tipologie sulle piattaforme social. La prima si verifica quando viene pubblicato un video che testimonia l'atto di bullismo tradizionale, mentre la seconda riguarda la diffamazione, che si può realizzare attraverso la chat privata o con la pubblicazione di 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/pagine che prendono di mira un ragazzo anche senza che lui ne sia a conoscenza.
Comunque sia perpetrata, l'attività diffamatoria si serve di affermazioni scritte, sondaggi, foto e 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 quest'ultima riguarda le piattaforme espressamente dedicate all'upload di video (es. YouTube), in cui, se il video è pubblico, milioni di utenti possono avervi tramite ricerca per parole chiave. Sulle piattaforme di social networking, invece, essi sono situati all'interno di un profilo e non sono immediatamente reperibili.
Detto questo, è chiaro quanto siano importanti le *policies* dei social network, poiché esse si pongono a fondamento dell'eventuale intervento della piattaforma per arginare gli abusi, prima ancora di adire le autorità competenti.

Facebook nei suoi "Standard della comunità", facenti parte delle Condizioni d'uso, si riferisce al bullismo elettronico, stabilendo che non vengono tollerati «atti di bullismo o molestie»[12] cui verranno posti dei limiti «in caso di segnalazione di comportamenti offensivi nei confronti di singoli individui»[13]. Inoltre, il social non consente i contenuti che incitano all'odio (*hate speech*) né la discriminazione «in base a razza, etnia, nazionalità, religione, sesso, orientamento sessuale, disabilità o malattia»[14].
Nel "Centro per la sicurezza", si prevede una collaborazione con le autorità nel rispetto della direttiva europea 2000/31/CE, finalizzata a rilasciare le informazioni richieste, soprattutto nei casi "di emergenza" (danno imminente a un bambino o al rischio di morte o serio danno fisico a qualsiasi persona). Per questo, rispetto alla possibilità di rilasciare dati dei cittadini europei, Facebook ha aderito al programma *Safe Harbor*[15], nato in seguito all'emanazione della direttiva della Commissione europea sulla protezione dei dati personali[16] per garantire che le aziende operanti nell'Unione Europea inviino dati personali a paesi non appartenenti allo Spazio economico europeo, solo se essi sono disposti a fornirgli adeguati livelli di protezione.

[12] www.facebook.com/communitystandards.
[13] Ibid.
[14] Ibid.
[15] export.gov/safeharbor.
[16] Direttiva 95/46/CE.

In ogni caso, in linea con la *Section 230* del *Communications Decency Act* statunitense, il social network si chiama fuori da qualsiasi coinvolgimento nelle responsabilità, 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. A ciò si aggiunge la recente piattaforma di prevenzione contro il bullismo[17], del maggio 2014, che si affianca alla tutela offerta dai meccanismi di segnalazione e dalla cd. "segnalazione sociale" (per i contenuti ritenuti inadeguato che però non violano le Condizioni d'uso). Si tratta di una piattaforma fatta di «strumenti, suggerimenti e programmi per aiutare le persone a difendere se stesse e gli altri»[18], che si articola in quattro diverse sezioni, destinate rispettivamente al bullo e alla vittima, ai suoi amici, ai genitori di entrambe le parti e agli insegnanti. In tutti i casi, Facebook ha suddiviso la parte informativa da quella relativa all'azione, in cui descrive quali strumenti/opzioni siano fruibili direttamente dal social network e quali, invece, siano le *best paractices* da intraprendere al di fuori della rete. Si tratta di consigli che vanno da "come affrontare il discorso" a "quando contattare le autorità", con una particolare attenzione - nella sezione che riguarda gli insegnanti - alle tecniche di prevenzione oltreché di repressione, il che dimostra la necessità dell'intervento coordinato su più livelli che si è auspicato nel corso di questo lavoro.
Tuttavia, il lavoro educativo di Facebook non può considerarsi sufficiente finché non sarà implementato in modo da garantire un intervento tempestivo dei team già definiti che rispondono alle segnalazioni.

Nei casi di cyberbullismo, Twitter «consiglia in genere di bloccare l'utente in questione e di porre fine alla comunicazione», fornendo strumenti simili a quelli di Facebook poiché, qualora ciò non bastasse, Twitter offre un suo meccanismo di segnalazione per le violazioni delle "Regole di Twitter"[19] (impersonificazione, divulgazione di informazioni private, minacce di violenza specifiche e dirette, dar vita ad illeciti o a prenderne parte, pornografia e abuso mirato). Tuttavia, come sull'altro social network, 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». A questo proposito, mentre Facebook ha stabilito come impostazione di default la condivisione solo con gli "amici", i *tweet* vengono condivisi pubblicamente all'atto di registrazione, perciò - a meno che non vengano settate le impostazioni necessarie a mantenerli protetti - il minore corre il rischio di essere bersagliato, soprattutto considerando che i *followers* non si basano sulla con sensualità come le "amicizie" di Facebook.
Comunque, anche Twitter ha aderito al progetto *Safe Harbor* e per questo 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[…]»[20] poiché è possibile che un comportamento o alcune affermazioni costituiscano una «violazione della legge locale»[21]. In questo caso, «se Twitter viene contattato direttamente dalle forze dell'ordine, [può] lavorare con

[17] www.facebook.com/safety/bullying.
[18] Ibid.
[19] *Le Regole di Twitter*, in support.twitter.com/articles.
[20] twitter.com/privacy.
[21] support.twitter.com.

loro e fornire assistenza per la loro indagine, nonché indicazioni sulle possibili opzioni»[22]. A tal proposito, dal luglio 2012, Twitter ha dato vita al Transparency Report, nel quale, ogni sei mesi, pubblica i dati relativi alle richieste governative (suddivise per paese) che la piattaforma riceve affinché essa fornisca informazioni sugli utenti o riguardanti il blocco dell'accesso ai *tweet* che risponde ad un criterio di censura geografica selettiva.

Ask.fm è una piattaforma lettone che consente di porre interrogativi in forma anonima a chiunque, sia che si possegga un profilo, sia che non si abbia un account. L'unica differenza se ci si registra consiste nel poter rispondere 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 se si conosce il *nickname* dell'utente. Inoltre, come su Twitter, si possono avere dei *followers*, ma anch'essi restano anonimi pur avendo un profilo registrato.
La possibilità di rimanere ignoti ha dato luogo a moltissimi illeciti perpetrati grazie all'uso di Ask.fm, la cui politica è quella di dare seguito a tutte le segnalazioni di violazione dei termini di utilizzo, «soprattutto quelle riguardanti azioni che potrebbero aver sconvolto, angosciato o impaurito l'utente. Quindi, qualora l'utente pubblichi qualcosa che [la piattaforma ritiene] inappropriato o inaccettabile, [questi contenuti potranno essere rimossi] dal sito» e/o, «dove possibile»[23], verrà bloccato l'accesso del colpevole alla piattaforma»[24]. Dunque, nonostante nella sezione riguardante le "Politiche di abuso"[25], vengano elencate le «principali azioni che non sono permesse all'utente», collocando al primo posto il bullismo, non è chiaro quali siano le azioni intraprese dal social network nel caso in cui a compiere l'illecito sia un utente non registrato.
Nel caso in cui l'utente abbia un account, invece, è possibile bloccarlo, così come è possibile segnalare le domande unitamente al meccanismo di filtro automatico grazie al quale lo staff viene avvisato sulla presenza di «parole e frasi maleducate/offensive che non sono ammesse su Ask.fm»[26] e, in questo modo, può rimuoverle.
Comunque, oltre alla discutibile efficacia delle *policies* rispetto alla possibilità di anonimato e di assenza di registrazione, un'altra difficoltà risiede nel fatto che il team di moderatori è composto solo da una cinquantina di persone che devono vigilare su milioni di utenti in oltre 150 lingue[27].
Insomma, per quanto riguarda la piattaforma lettone, essa non si prende la responsabilità sociale che gli spetta in quanto azienda che lavora per offrire dei servizi agli utenti e ciò comporta l'assenza di un intervento che ponga effettivamente fine alle prepotenze dei cyberbulli.
In conclusione, se si volesse riflettere sugli approcci dei diversi social network, è chiaro che la tutela assoluta contro il cyberbullismo non è possibile, ma ciò 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* che dovrebbero implementare le *policies* - come nel caso della piattaforma contro il bullismo di Facebook - e la capacità di effettuare interventi successivi.

[22] Ibid.
[23] ask.fm/about/policy/terms-of-service.
[24] Ibid.
[25] ask.fm/about/policy/abuse-policy.
[26] Ibid.
[27] Laure Belot, *Ask.fm affole les ados en quête de cyber-frissons*, Le Monde, 3/6/2013.

YouTube è la piattaforma di *videosharing* più diffusa al mondo, soprattutto perché la condivisione su altri social network e la fruizione personale rimangono svincolate dal possesso di un account registrato, utile soltanto per l'*upload*.
In questo contesto, è nata una nuova tipologia di cyberbullismo, che consiste nella ripresa di atti di bullismo tradizionale poi caricati su YouTube, così da mandare in onda il fatto, agendo da cassa di risonanza rispetto all'umiliazione subita dalla vittima.
La piattaforma si assume la licenza gratuita di riprodurre i contenuti, dei quali, quindi, dispone sia la presenza che la rimozione, ma non effettua un controllo preventivo, bensì interviene «nel momento in cui dovesse venire a conoscenza di qualsiasi potenziale violazione»[28] dei termini di servizio. In tal caso, «si riserva il diritto (ma non ha l'obbligo) di decidere se i Contenuti si conformino con i requisiti previsti nei Termini e potrà rimuovere tali contenuti e/o inibire l'accesso di un utente al caricamento dei contenuti che siano in violazione dei Termini in qualsiasi momento, senza preavviso ed a sua esclusiva discrezione»[29].
Suddette disposizioni si applicano poiché «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»[30].
Il bullismo, in particolare, viene assimilato alla violazione della privacy, poiché la piattaforma lo interpreta come "attacco dannoso" che si sostanzia in: «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»[31].
In tal caso, è possibile segnalare il video compilando il "reclamo per la violazione della privacy"[32] e «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»[33]. Se a seguito dell'arco di tempo previsto «la causa della potenziale violazione della privacy è ancora presente sul sito […] il reclamo verrà esaminato dal team di YouTube»[34].
La segnalazione può essere presentata solo dall'interessato attraverso il proprio account oppure, qualora si tratti di «una persona vulnerabile»[35], potrà intervenire anche il genitore, ferma restando la possibilità per chiunque di farsi rappresentare da un legale.
Dal momento che la piattaforma manda in onda l'atto di bullismo tradizionale, ci si è domandati se essa abbia un ruolo per concorso nel reato di diffamazione, trovando risposta nel celebre caso Google-Vividown.
La Corte di Cassazione, infatti, confermando quanto stabilito nel giudizio di secondo grado, con la sentenza 5107/2013 ha sottolineato, ai sensi del D. Lgs. 70/2003, l'assenza di qualunque obbligo di sorveglianza da parte del provider ed ha affermato che il titolare del trattamento dei dati personali è colui che ha potere decisionale su finalità e modalità di suddetto trattamento,

[28] www.youtube.com/t/terms.
[29] Ibid.
[30] www.youtube.com/t/community_guidelines.
[31] support.google.com/youtube/answer/2802268.
[32] support.google.com/youtube/answer/142797.
[33] www.youtube.com/t/privacy_guidelines.
[34] Ibid.
[35] Ibid.

perciò non è una figura assimilabile a Google Italia, ma piuttosto all'utente che ha immesso il video in rete. In ultimo, viene precisato che non vi è il dolo specifico previsto dall'art. 167 del 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.
Questo caso ha dimostrato che è giusto pretendere dagli ISPs la massima collaborazione nella tutela dei minori - rimozione del video, temporanea sospensione dell'account -, ma che i prestatori di servizi devono poter applicare le loro *policies* in un contesto di maggiore educazione e responsabilizzazione dei giovani, che solo le istituzioni (legislatore e scuola) possono garantire. In questo modo, sia l'ordinamento statale che le condizioni d'uso dei social network, assieme agli strumenti educativi, andrebbero ad agire sul livello preventivo e su quello successivo, diminuendo i reati ma mantenendo il più possibile invariata la libertà di espressione sul web, poiché l'intervento su più livelli è l'unico possibile.

Il caso di Rebecca Sedwick, di soli dodici anni, suicidatasi a seguito delle persecuzioni subite a causa di due compagne di scuola, ha dimostrato che dall'assenza di regolazione normativa del cyberbullismo può derivare una mancanza di conseguenze. Infatti, anche se le colpevoli all'inizio erano state arrestate, ai sensi del Title 46 dei Florida Statutes, per "*felony aggravated stalking of minor 16 years of age*"[36], le accuse sono cadute per insufficienza di prove, giacché nello stato mancano le leggi che individuano il bullismo elettronico come un illecito.
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. Perciò, mentre in via ufficiosa si può pensare di difendere la vittima di cyberbullismo, in via ufficiale non esiste alcuna disposizione che lo configuri come misfatto dalle conseguenze concrete. Ciò è confermato dal fatto che una pena viene effettivamente comminata solo quando il bullismo elettronico è preceduto da danni fisici e materiali "tradizionali", come nel caso delle minacce e delle violenze perpetrate da Keeley Houghton ai danni di Emily Moore in Inghilterra o quando il fenomeno si lega alla pedopornografia (*sexting*/*revenge porn)* come quello di Carolina Picchio, suicidatasi a Novara, nel gennaio del 2013, a seguito della pubblicazione su Facebook di un video che la ritraeva ubriaca ed abusata da più ragazzi, oggi tutti indagati per violenza sessuale di gruppo. Colui che ha effettuato l'*upload* è stato accusato di diffusione di materiale pedopornografico online e di istigazione al suicidio come conseguenza di altri reati e, allo stesso modo, è stato accusato ed arrestato il persecutore di Amanda Todd, una sedicenne di Vancouver che si è tolta la vita nel 2012 a seguito della diffusione su Facebook delle foto dei suoi seni.
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*…) 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 un disincentivo a ripetere l'abuso.

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

[36] Florida Statutes, Title XLVI – Chapter 784 (Crimes: assault; battery; culpable negligence), par. 048, Stalking; definitions; penalties.

esempio, dello stato di Washinghton, dove una dodicenne di Issaquah, perseguitata da due compagne di classe nell'aprile del 2011, ha visto condannare una delle due cyberbulle ai servizi civili e all'uso supervisionato di internet grazie al fatto che lo stato di Washinghton identifica il cyberbullismo come reato con il *Bullying Act* del 2007.

Anche ad Alamance County, grazie alla legge esistente in North Carolina (*amends 14-458,1* del *Senate Bill 707*), Robert Bishop (insieme ad altri cinque coetanei) è stato punito per essersi preso gioco di Dillion Price su Facebook, postando lo *screenshot* di una conversazione avuta erroneamente con lui ed accusandolo di essere gay. Così, 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 di utilizzare Facebook o altri siti di social networking per un anno.

In entrambi i casi, i giudici hanno stabilito una "*suspended sentence*", cioè una sentenza che, ha sospeso la pena relativa alle accuse, rispettivamente per sei e dodici mesi, affinché i colpevoli potessero essere messi alla prova - con il servizio civile o con l'interdizione dai social network - e dimostrare di aver compreso la lezione.
Si tratta di un risultato estremamente soddisfacente, poiché l'applicazione della norma ha condotto alla rieducazione, così da correggere i comportamenti e reprimere gli abusi. Per chi scrive, questo è ciò che dovrebbe essere fatto in tutti i paesi, poiché è necessario proporzionare i mezzi all'entità del crimine e all'età del cyberbullo, affinché possano attivarsi meccanismi di cooperazione tra la legge, le scuole e le famiglie. Infatti, essere ritenuti responsabili delle proprie azioni da una legge è già una componente fondamentale della repressione e della prevenzione. Tutto ciò che si è sino ad ora auspicato, può essere pensato solo all'interno di un quadro regolamentare il cui obiettivo è quello di individuare le fattispecie che costituiscono reato per garantire conseguenze quali la sospensione scolastica, la cessazione momentanea della disponibilità dei servizi in rete e qualsiasi altro metodo correttivo per giungere sino all'incarcerazione e al risarcimento nei casi più gravi, bilanciando così la libertà di espressione in rete con la tutela dei diritti della persona. A ciò, poi, dovrà aggiungersi la previsione di appositi programmi scolastici che contribuiscano all'alfabetizzazione digitale di adulti e ragazzi.
Se, poi, da una parte si tende a deresponsabilizzare il provider, dall'altra è necessario richiedergli collaborazione poiché, trattandosi di un'azienda, essa deve rispondere a degli standard minimi di qualità 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. Parte di questo compito, poi, risiede nel far fronte all'a-territorialità della rete, da cui derivano intese internazionali - come la Convenzione di Budapest sul Cybercrimine e la Convenzione di Lanzarote sulla pedofilia - ma anche gli accordi presi tra enti sovrannazionali e *providers*, come quello del Safe Harbor.
Dunque, da tutti gli elementi analizzati, emerge la necessità di intervenire su più livelli, per coinvolgere lo stato, l'istruzione, le famiglie e le aziende 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.

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

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 on-line a rischio - Linee guida per genitori*, in www.cyberbullismo.com

N. Pinna, M. E. Saturno, L. Pisano, *Prevenire il cyberbullismo e la navigazione on-line a rischio - Linee guida per docenti*, in www.cyberbullismo.com

N. Pinna, M. E. Saturno, L. Pisano, *Prevenire il cyberbullismo e la navigazione on-line 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