BACKGROUND PAPER

Cyberbullying: an overview

Introduction

Cyberbullying has been getting more and more attention from the media, decision makers, industry players, and society as a whole over the last decade.

The most tragic consequences of cyberbullying driving teens to commit suicide have caught the media and the public eye's attention. Parents are worried about their children being bullied via their mobile phones, teachers are often lost when it comes to their role and responsibility regarding cyberbullying acts happening outside of the school premises and fear that cyberbullying may disrupt the school's positive learning environment and cause early school leaving, children and teens can feel powerless when faced with cyberbullying and often react counterproductively.

With the rise in the use of mobile technologies with permanent access to the internet, coupled with a sense of anonymity and lack of accountability, cyberbullying has been affecting a substantial number of people including children, teens and even teachers.

Although scare mongering will not help address the issue, it is clear that there are vast arrays of measures that can be taken at each level (national and international law, school rules and policies, teacher training, training of young people, children's and parent's awareness raising and empowerment campaigns…)

Definition

Cyberbullying has many different "official" definitions.

According to the EU Commission, *"Cyberbullying is repeated verbal or psychological harassment carried out by an individual or group against others. It can take many forms: mockery, insults, threats, rumours, gossip, "happy slapping", disagreeable comments or slander. Interactive online services (e-mail, chat rooms, instant messaging) and mobile phones have given bullies new opportunities and ways in which they can abuse their victims."*[1]

[1] http://ec.europa.eu/information_society/activities/sip/projects/centres/practices/info_campaign/index_en.htm

In the United States, The National Crime Prevention Council defines cyber-bullying as *"the process of using the Internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person."*[2]

Although definitions differ, there are a series of descriptors for bullying in general that can be identified:

- Firstly, the concept that the **perpetrator intends to hurt the target intentionally,** whether emotionally or physically**.**

- Second, there is an **imbalance of power** between the perpetrator and the victim. This is easily identifiable for traditional bullying but is harder to define when it comes to the online world. The fact that the bully remains often anonymous and the power that the bully has when it comes to reaching nearly instantaneously a wide audience with embarrassing or hurtful material can be a proof of this imbalance of power.

- Third, there is always an element of **repetition or continued threat of further aggression.** Cyberbullying and/or bullying are not one-off comments or threats, that could be rather defined as "flaming"[3], "trolling"[4] or simply one-off aggression[5]. One has to be careful however, since in the online world, a "one-off" aggression from multiple users or from a single user but massively shared by other users becomes effectively cyberbullying.

Finally, it is worth mentioning that **differentiating cyberbullying from sexual harassment, cyberstalking and other behaviours is very difficult**. Cyberbullying can be carried out in the form of sexual harassment, for instance by commenting the body, appearance or sex/gender, forwarding intimate pictures (sexual content, naked body/body parts) or videos, spreading sexual rumours etc. All of these actions can be understood as both cyberbullying and sexual harassment, but the distinction is less important than to recognise that the **ultimate effect** can be very much the same (see the section below on the consequences of cyberbullying) and therefore the resulting steps to be taken by the victim remain mostly the same.

Research, statistics and facts

What is the extent of cyberbullying?

The figures vary greatly according to the different studies, the countries covered, the age of the sample and the definitions, questions and methodology used by each of the studies.

The Cyberbullying Research Center in the US (lead by Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.) estimate the number of affected youth to be **between 10% to over 40%.** When narrowing the definition to "repeated" acts online intending to hurt someone, the figure they found was **20%** among the randomly selected **11 to 18-year-olds**.

The EU Kids Online 2011 report found that **6 % of 9 to 16-year-olds** report having been bullied online across Europe[6].

[2] http://definitions.uslegal.com/c/cyber-bullying/
[3] http://en.wikipedia.org/wiki/Flaming_%28Internet%29
[4] Many terms such as "trolling" or "flaming" are in their infancy and can take various meanings according to the different cultural setting. Trolling is akin to cyberbullying in some instances.
[5] Des Butler, Sally Kift & Marilyn Campbell , "Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance?", *eLaw Journal: Murdoch University Electronic Journal of Law*, Vol 16, No 1 (2009), p. 85-86.
[6] Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K., "EU Kids Online final report", September 2011, p. 24. http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf

In the UK, BeatBullying found that **28% of 11 to 16-year-olds** have been cyberbullied[7] and in Belgium, Childfocus launched vast awareness raising campaigns around cyberbullying after their figures showed that about **33% of children** were exposed to cyberbullying[8].

In the US, "the 2008–2009 School Crime Supplement (National Center for Education Statistics and Bureau of Justice Statistics) indicates that **6%** of students in **grades 6–12** experienced cyberbullying.

The 2011 Youth Risk Behavior Surveillance Survey finds that **16%** of high school students (**grades 9-12**) were electronically bullied in the past year."[9]

It is impossible to determine and decide upon a definite number of cyberbullying victims, however, some points can be drawn from the studies above.

Firstly, all studies agree that **cyberbullying increases with age.** This means that studies that restrict the age group to younger children would get lower results.

Secondly, in the studies with the highest cyberbullying figures, the **definition of what constituted cyberbullying was broader**, especially when it came to repeated cyberbullying acts or one-off acts. That is why several studies identify inside their main cyberbullying figures, the portion of victims who suffered from **"persistent and intentional" cyberbullying** (from the Beatbullying study, **1 in 13 children**, from the Childfocus study, **1 in 10 children, 3%** from the EU Kids Online study)

Thirdly, the figures vary greatly according to factors such as:

- **technological development and take up by children** (the prevalence of children using mobile phone devices or having access to the internet – since in some EU countries, access to internet or a mobile phone is much lower than in others, it is not surprising that such countries show lower figures for cyberbullying);
- **socio-economic status and educational achievement** (many studies point out that children from poorer families are more at risk);
- **digital literacy;**
- **Gender, sexual orientation, disability, minority status…;**

In conclusion, although we cannot settle for a definite number of cyberbullying victims, even using the most conservative figures, that of the EU Kids Online study, 6% of children across the EU is a very high and significant number, especially when considering the consequences of cyberbullying or bullying, as we will see later. Unsurprisingly, the EU Kids Online report also underlines that cyberbullying is what bothers kids most.

What can some of the consequences be?

For the **victim,** studies point to many serious consequences:

- **negative emotional responses** such as fear, anger, sadness, frustration, powerlessness, lower self-esteem and confidence, depression;
- **behavioural responses** such as isolating oneself, lack of concentration, lower school results, missing school, being pressured into delinquency, revenge and retaliation against the cyberbully or someone else,
- **extreme responses** such as self-harm, attempts of suicide or suicide[10].

[7] Beatbullying, "Virtual Violence II, Progress and Challenges in the Fight against Cyberbullying", 2012, p.6, http://www.beatbullying.org/pdfs/Virtual-Violence-II.pdf
[8] http://fdf.be/spip.php?article4292
[9] http://www.stopbullying.gov/cyberbullying/what-is-it/index.html
[10] Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., "Emotional and psychological consequences", p.1-2. http://www.cyberbullying.us/cyberbullying_emotional_consequences.pdf ; BeatBullying, op. cit. p. 7.

Who are potential victims and perpetrators of cyberbullying?

As regards **victims,** most studies on cyberbullying point to **groups more exposed than others**. For instance, LGBTs are much more exposed to bullying and cyberbullying than others.

Some of the most groups most exposed to the risk of being cyberbullied are[11]:

- LGBTs;
- Children and teens with a disability;
- Children from a migrant background or minority ethnic groups (black, asian, mixed…);
- Girls (where boys tend to do more bullying face-to-face, girls tend to be more exposed to bullying online – a common source of cyberbullying borders on sexual harassment – either with strangers or even with ex-boyfriends taking a "revenge" on a relationship that turned sour. This is more commonly called "sexting".);
- Children and teens with special learning needs;
- Children from lower socio-economic groups and/or whose parents are less educated;
- Children in families where parents do not use the internet.

In general, we can conclude that cyberbullying cannot be taken out of context and should not be viewed in isolation from offline bullying. It happens in a certain societal context with specific enduring problems such as discrimination against minorities, people with a disability, a specific sexual orientation etc. and in general, hits the most **vulnerable children and teens** or children from **vulnerable families.** There is a case for general policies aiming at shifting the social context and environment in which cyberbullying takes place. Such policies include the fight against with discrimination or for equality between men and women, as well as other broad reaching measures such as social policies and employment policies tackling social exclusion and poverty,…

As regards **perpetrators,** studies point to a variety of reasons[12]:

- Seeking revenge is the most common reason why perpetrators engage in cyberbullying and many cyberbullies were themselves victims of bullying and/or cyberbullying at some point;
- Some perpetrators cyberbullied others as a "joke";
- It is "easier" to engage in bullying online and the fear of getting caught is lower than for bullying;
- Some perpetrators engaged in cyberbullying because they felt "angry" about something.
- Interestingly, while one of the most vulnerable groups of victims exposed to cyberbullying are LGBTs, this same group was most likely to engage in cyberbullying as well;
- Finally, most bullies (80%) knew who their victims were.

Where does cyberbullying take place?

The short answer to this question is where children and teens are most…

Technology and the internet change at a very fast pace. A decade ago, social networks were virtually unheard of, and most cyberbullying happened in **chat rooms or even via email.** Nowadays, more and more bullying happens via **social networks** and **video sharing platforms.** Instant messaging and texting remain "popular" means of cyberbullying while other trends like "intimidating phone calls or hoax phone calls" have become much less prevalent[13].

[11] Beatbullying, op. cit. p. 21-23 ; Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., "Victimization of adolescent girls", http://www.cyberbullying.us/cyberbullying_girls_victimization.pdf ; Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., "Electronic Dating Violence: A brief guide for educators and parents", http://www.cyberbullying.us/electronic_dating_violence_fact_sheet.pdf; Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., " Bullying, Cyberbullying and sexual orientation", http://www.cyberbullying.us/cyberbullying_sexual_orientation_fact_sheet.pdf .

[12] Ibid.

[13] Ibid; Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., "Identification, Prevention and Response", http://www.cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf

Cyberbullying also happens in the **online gaming** environment and in currently popular interactive sites such as **Formspring** and **ChatRoulette.**

What's so different about cyberbullying?

The main differences between bullying and cyberbullying are the following[14]:

- Cyberbullying can happen **24/7 at any time, any day and especially any place** (at the victim's home for instance, removing any feeling of safety and security even in his own house).
- The **potential audience** for humiliating or hurtful images, texts, videos… **is huge** and the **dissemination is virtually instantaneous**.
- **Deleting the hurtful material can be difficult** if not impossible.
- The cyberbully has the feeling that he can remain **anonymous** and it can be very hard to **clearly identify** him/her without reasonable doubt. Sometimes, the cyberbully doesn't even know the victim and vice versa!
- Cyberbullying can be **harsher** due to the fact that the bully cannot see the immediate reaction of the victim and experience empathy, guilt or be convinced that he/she has taken it too far. The victim can also suffer greatly by no knowing exactly how many people including classmates have seen a hurtful material and what their reaction was.

Prevention and intervention

There are many actors that can be potentially involved in helping a victim of cyberbullying or identyfing a perpetrator and each one can play an important part in preventing or tackling cyberbullying as quickly as possible.

Awareness raising campaigns

Whether carried out by public bodies, private companies or civil society organisations, awareness raising among parents, children, teachers, schools or indeed the general public, **awareness raising campaigns** are key to prevent cyberbullying or intervene effectively to put an end to it. At the same time, research has shown that their **effectiveness is questionable**[15].
There remain a high percentage of victims who tell no one about cyberbullying or delete incriminated messages, images, videos, despite the fact that campaigns about cyberbullying strongly advise to seek help and save and document proof of the cyberbullying.

In essence, awareness campaigns by all actors remain necessary but their focus needs to be reconsidered. Education has to play an increasing role as well in tackling and preventing bullying and cyberbullying.

What can victims do?

From what research tells us, in many cases, **victims can make some bad decisions when cyberbullied.**
According to the figures from Jane Riese's presentation at the New Jersey Bullying Prevention Summit in 2012, reactions from cyberbullying victims were the following[16]:

- Did nothing (36%)
- Asked person to stop (35%)
- Cyberbullied back (29%)
- Made fun of the bully to others (17%)

[14] http://www.stopbullying.gov/cyberbullying/what-is-it/index.html ; http://www.ncpc.org/topics/cyberbullying/what-is-cyberbullying ;
[15] Beatbullying, op. cit., p. 35.
16 Jane Riese, MSW, LSW, Clemson University, "NJ Bullying Prevention Summit", 17 April 2012, http://fea.njpsa.org/documents/CyberbullyingNJSummit.pdf

- Blocked the bully (17%)
- Saved the evidence (17%)
- Told on them (13%)
    - In 30% of the cases, victims told their friends
    - In 15%, victims told their parents
    - In 13%, their siblings
    - In 4% and adult in school
    - In 2% their teacher

The figures from the BeatBullying 2011 study show similar trends[17]:
- 27% of victims ignored the message
- 23% told a friend or peer
- 22% blocked the bully
- 21% deleted the message
- 20% saved the message for evidence
- 20% told a parent or adult
- 13% bullied back
- 10% told a teacher or school staff
- 7% reported the problem to the network provider

The most common tips for victims of cyberbullying are the following:

- **Do not respond** to cyberbullying messages and **do not forward** them, and especially, **do not cyberbully back**;
- **Save the evidence** of the cyberbullying (print screen, save on hard drive, record the dates and times of the cyberbullying actions,…);
- **Block the bully**;
- **Report the incident to the administrator of the website** (social networking sites and video sharing sites should have a way to report cyberbullying);
- **Talk to an adult you can trust** (your parents, your school teacher, or any other adult) or **a trusted friend;**

The role of parents

Studies show that when parents maintain an **open and candid communication** with their children about the use of the internet and **explicitly condemn bullying behaviours**, their children are less likely to engage in bullying and are in a better position to deal with bullying[18].

There are many guidelines available online for parents and the most common recommendations on the **preventive** side are the following:

- Parents need **to be involved and take interest in what their children do online**. This means asking regular questions and discuss the activities of their children. This can be complemented by monitor their activities with parental control tools in a transparent manner.
- Parents should **talk about cyberbullying with their children** and make two points clear: that they are there to help their children should they have any trouble with a cyberbully (reassure them that you will not simply confiscate their devices and access to the web) and that cyberbullying behaviour is not acceptable and will have consequences should they engage in such activities. One way to encourage children to open up on the topic of cyberbullying is to ask them whether they know of someone that has been cyberbullied or to show them a cartoon, advertisement, movie… that talks about cyberbullying and then discuss with them the general idea of cyberbullying.
- **Establish clear age-appropriate rules** about the use of technology and the internet, letting children know what is permitted and what is not.

[17] Beatbullying, op. cit., p. 35-36.; http://www.healthychildren.org/english/family-life/media/pages/Cyberbullying.aspx
[18] Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., "The Influence of Parents, Educators, and Peers", http://cyberbullying.us/Social_Influences_on_Cyberbullying.pdf

On the **early intervention** side, the recommendations are the following:

- Parents need to be on the look-out for **signs** in order to **identify as soon as possible and address cyberbullying**[19]**.** If their child:
  - seems to unexpectedly stop using the computer or mobile phone;
  - is nervous or worried when receiving a text message, email…;
  - looks upset, angry, sad or depressed after using a mobile phone or a computer;
  - doesn't want to go to school;
  - is unwilling to discuss his use of the computer or mobile phone;
  - withdraws him or herself from social contacts (close friends and family members).

  These are signs that he or she may be a **victim of cyberbullying.**

- In a similar way, if a child shows signs such as:
  - suddenly turning off screens or closing programmes when a parent passes by;
  - being very upset when his access to computers or his mobile phone is restricted;
  - an unwillinness to discuss his use of the computer or mobile phone;
  - using multiple accounts for email, social networking or any other platform;
  - suddenly displaying strange behaviour, very different than usual.

  These are signs that he or she may be a **perpetrator of cyberbullying.**

Once a parent is aware that their child has been cyberbullied, some of the steps that parents should take include[20]:

- To **make sure that their child feels safe and secure and convey unconditional support**;
- To **save all evidence** of the cyberbullying (emails, texts, instant messaging conversations, images, intimate pictures, videos…);
- if your child know who is behind the cyberbullying, and only with your child's permission, you might consider **contacting the parents of the perpetrator** to discuss the issue;
- If not done already by your child, **report the cyberbullying to the online service providers;**
- **Get in touch with the school**, the head teacher and other relevant school staff and be prepared that the school may not want to get involved;
- **Contact law enforcement authorities** in case the situation seems to place your child in danger and if you have enough material as proof that the law has been broken (for instance in case of serious threats, unwillingness for either the perpetrators' parents or the school to cooperate)
- Should their child be a **perpetrator,** parents need to discuss at length the extremely hurtful and damaging effects that cyberbullying can have on others. Parents should especially focus on education and dialogue to help their child to change his/her behaviour. However, parents might also have to apply firm consequences to cyberbullying others such as installing thorough parental control software (monitoring, filterning and blocking tools), limiting or removing technology privileges and follow up regularly to see if the "lessons" have been learned and internalised.

The role of schools, teachers and school staff

With regards to **prevention**, schools can[21]:

- include in their teaching curriculum, or outside the curriculum utilising external organisations, courses on the responsible use of the internet;

- update their school policy and rules to make sure that cyberbullying is clearly forbidden and that specific measures proportionate to the seriousness of the cyberbullying are taken (from

[19] Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., "Identification, Prevention and Response", http://www.cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf
[20] http://www.healthychildren.org/english/family-life/media/pages/Cyberbullying.aspx ; http://www.stopbullying.gov/cyberbullying/how-to-report/index.html
[21] Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., *op. cit.*

detention, contacting parents to expulsion of a student) The school rules should include a mention that the staff is competent to act in the case of cyberbullying even if it happens outside of the school premises, so long as it disrupts the learning environment in school, and the school policy should clearly outline how the school responds to incidents.

- Foster a positive school climate which can comprise of many things: keeping the school premises clean and safe, organise many extra-curricular activities in school, promote a culture of respect and positive behaviour in school, encourage participation of students and open dialog with teachers… A "positive school climate" has been identified in many different studies as a way to boost consistent attendance, higher student achievement and other desirable educational outcomes but it also can have a preventive effect on peer conflict which can lead to bullying or cyberbullying.

- Provide training to teachers and school staff on all things digital including cyberbullying;

- Designate a teacher responsible for anti-bullying policies and activities;

- Organise peer-mentoring sessions where students engage in activities promoting a responsible behaviour online and demoting cyberbullying as such.

With regards to **intervention**, schools can:

- Identify and make use of school staff that can liaise with law enforcement and investigate incidents according to their seriousness. Once the perpetrator has been identified, the school must develop a response proportionate to the harm done.
- Work with parents of both the victim and the perpetrator in order to organise counselling sessions or take disciplinary action in cooperation with parents.
- Where cyberbullying has been taken to dangerous stages (in case of serious threats, if the victim does not feel safe coming to school, if the cyberbullying persists even after traditional disciplinary measures), a formal response by the school may be warranted. Actions such as detention, suspension, changes of placement or even expulsion may be needed.

The role of peers and bystanders

Both peers and bystanders can really make a difference with regards to cyberbullying. Peers can be trained to be **mentors** and help raise awareness about cyberbullying and empower potential victims. Mentoring usually involves using older students to change the way younger students think about certain situations and actions such as cyberbullying. Coming from their own peers and age group, the message can be more powerful and meaningful to young people. Therefore, peers can essentially help spread the messages about how to prevent cyberbullying and how to respond to it (see above)[22].

Bystanders can be peers but also any other person who witness cyberbullying may while it happens (a perpetrator(s) sending or posting something or a victim receiving something).

Although bystanders are usually passive and are not willing to get involved for fear of bringing cyberbullying (or bullying) on to them, their role is crucial in the early detection and intervention to cyberbullying. What they can do is akin to what was seen above:

- take note/save what they have witnessed as evidence to prove the cyberbullying;
- step up for the victim and make it clear that they do not approve of the cyberbullie's behaviour;
- talk to a trusted adult about what they have witnessed;
- never encourage or indirectly contribute to the cyberbullying (forwarding a message, "liking" inappropriate or hurtful jokes…)

[22] http://www.cybermentors.org.uk/ ; http://cyberbullying.us/blog/peer-mentoring-as-a-strategy-to-address-cyberbullying.html

The legal framework and the role of law enforcement

Before addressing the role of law enforcement, it is essential to briefly sketch the existing legal background related to cyberbullying, i.e what the state of the law is in various countries when it comes to tackling cyberbullying.

At present, countries around the world have a very different way to deal with cyberbullying in the law. Starting with the **United States,** the main strategy seems to be oriented towards **schools.** Many States in the US have passed legislation which calls on school districts to mandatorily introduce in their school rules and policies an article on electronic harassment and identify prohibited behaviour as well as consequences for such behaviour.

These "school rules" have been more or less detailed and often criticized as ambiguous or impeding on the right to free speech.

On the federal level, the primary law regarding internet safety is the CIPA (Child Internet Protection Act – 2000). It obliges schools and libraries to have an internet safety policy for their computers. This includes for instance the use of filters that block harmful content[23].

Rulings of several court cases shed some light as to how cyberbullying cases can be handled, how perpetrators can be prosecuted and punished by the law. The first case to consider is the *Tinker v. Des Moines Independent Community School District (1969)* ruling in which the school suspended three students for wearing black armbands to protect the Vietnam War. The students protested as this violated their right to Free Speech under the First Amendment.

Two elements in this court case are relevant to cyberbullying cases today:
- first, the behaviour happened inside the school premises;
- second, the behaviour was passive and non-threatening.

In essence, a school cannot prohibit the expression of an opinion unless there is a **substantial interference with school discipline or the rights of others.** But this ruling also limited the scope of the law to the **school premises** thus creating a potential problem in addressing cyberbullying that occurred **outside** of the school premises**.**

A second court case, *J.S. v. Bethlehem Area School District (2000),* tackled this very question. J.S was expelled from school after he created a website that threatened specific school staff.
In the ruling, the court underlined that schools **do have the authority** to discipline students even when a behaviour or action happened outside the school premises but only if the school could demonstrate that such activity had a **disruptive and negative impact on the school and its learning environment**.

In essence, schools need to prove that the activities of a cyberbully have had a negative impact on their school environment, which is not an easy task. Also, the legitimacy of a school's decision when faced with a cyberbullying situation depends greatly on the quality of its policy and rules.

Sameer Hinduja and Justin W. Patchin identified six main elements of what could be an effective school policy:

- "Specific definitions for harassment, intimidation, and bullying (including the electronic variants) Graduated consequences and remedial actions
- Procedures for reporting
- Procedures for investigating
- Specific language that if a student's off-school speech or behavior results in "substantial disruption of the learning environment," the student can be disciplined

[23] http://www.fcc.gov/guides/childrens-internet-protection-act

- Procedures for preventing cyberbullying (workshops, staff training, curriculum enhancements)"[24]

In **Europe**, the situation is extremely diverse. On the one hand, there are **European laws** that apply to all countries (in theory) and provide some protection against cyberbullying, on the other hand, there are a variety of specific **national laws and government policies and strategies** that deal directly or indirectly with cyberbullying.

At the EU level, a variety of standards have been established to clarify legal issues relating to the protection of minors online. An extensive list can be found on the Commission's website here: http://ec.europa.eu/information_society/activities/sip/policy/legislation/index_en.htm

More specifically, we can mention the **Data Protection Directive** (95/46/EC) that applies to all Member states. Data protection plays a role because "whenever personal data of individuals is collected by electronic means; for example, in Internet forums, in social networks, by using instant messaging or email communication, [t]he legislation sets forth various principles that must be respected by those […] who publich information about third parties."[25]

What this means is that whenever a cyberbully discloses personal information about a victim, the provisions of the EU Data protection directive are fully applicable, since sharing such information requires the consent of the individual beforehand. The responsibility lies therefore in the hands of the cyberbully who, by processing and disclosing personal data, becomes a "data controller" and as such, has serious legal responsibilities associated to this role. The 2003 ruling of the ECJ (European Court of Justice) on the Lindqvist case confirms this interpretation.

Victims can, on the basis of this law, launch a complaint about the violation of their data protection rights to the supervisory data protection authorities or in a court.

As regards **EU Member states**, there is, to our knowledge, **no dedicated law** that explicitly makes cyberbullying illegal. Most Member states have general laws on **harassment, stalking, defamation, violence** etc[26].

Laws dedicated to cyberbullying are however being contemplated by some EU countries like Ireland[27].

Finally, governments develop **action plans** to fight cyberbullying and these include the set up of helplines, awareness raising campaigns, recommendations for schools to include cyberbullying in their school policy and rules (similarly to the US).

In conclusion, **the legal framework regarding cyberbullying can change quickly**. Some states like Canada have tried to introduce new legislation but failed.[28] Other such initiatives are pending or in the works and are likely to become increasingly frequent as the awareness around cyberbullying increases and governments are ever more willing to act and address the issue.

---

[24] Sameer Hinduja, Ph.D., Justin W. Patchin, Ph.D., "A brief review of relevant legal and policy issues", http://www.cyberbullying.us/cyberbullying_legal_issues.pdf

[25] Giovanni Buttarelli, "Data protection legislation in Europe, preventing cyber-harassment by protecting personal data and privacy", 07/06/2010, http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-06-07_Speech_Cyber-harassment_EN.pdf

[26] http://www.fosigrid.org/europe/europe-edition ; http://www.segec.be/Documents/Lgs/Prevention_et_lutte_contre_le_cyberharcelement.pdf ; Eliot Kaough, "Combatting cyberbullying: government, NGO and the Private Sector", http://mops.gov.il/Documents/International_Public_Security_Briefs/cyberbullying%20brief%2001.13.pdf

[27] http://www.thecorknews.ie/articles/motion-legislation-cyber-bullying-8098 ; http://www.dcya.gov.ie/viewdoc.asp?DocID=2570

[28] http://news.nationalpost.com/2012/11/22/conservatives-defeat-ndp-motion-to-craft-national-anti-bullying-strategy/

As regards the role of law enforcement:

- Law enforcement officers - be it school staff responsible for school policy, the police, data protection authorities – have a clear **dissuasive** role to play by communicating with children, parents, and the general public and informing them about the consequences of cyberbullying.
- Law enforcement officers also have the obligation to **keep up to date** on laws and regulation relative or relevant to cyberbullying (be it data protection laws, harassment laws…) In many cases, for instance, school staff are unaware which laws are relevant in case of cyberbullying or even what the school's policy is on the matter and what type of actions they can legitimately undertake!
- Finally, law enforcement agencies need to **cooperate more** between themselves and especially with schools, civil society organisations active in the field of cyberbullying and online service providers.

The role of the industry (especially online service providers)

The way online service providers configure their services, the options and features included, their reviewing, monitoring and censorship mechanisms, all of these can have a substantial impact on the prevention of cyberbullying and/or early intervention (takedown of abusive material, punitive or disciplinary actions such as banishment or account termination for breach of terms of use, gathering evidence for law enforcement…)

More specifically, online service providers are expected to[29]:

- periodically review the design and features of online services in order to identify potential misuses and address them if possible;
- take obvious preventive steps that would help protect users online from cyberbullying such as configuring restrictive privacy settings by default;
- communicate regularly and raise awareness of users on various e-safety topics among which cyberbullying;
- set up clear and simple reporting mechanisms;
- improve their follow up on reports and communicate in a transparent way about the status, a swift response time and actions taken (removal of content; evidence gathering…) relating to a cyberbullying report;
- step up the moderation of user-generated content by combining several mechanisms like skilled physical moderators, smart screening technologies etc.
- easy access to resources, tools and help for victims of cyberbullying, especially by signposting and/or referring users to organisations who can support them like relevant online support services.
- increase cooperation, support and funding of NGOs and other organisations dealing with cyberbullying that is taking place through their services (online help services, hotlines, helplines,…)
- ensure an independent monitoring of the industry's voluntary actions and code of practices and inform the parents and children about the results of such monitoring, identifying best practices and services offering the best protection for children.

At the EU level, many industry players take part in self-regulatory measures, whether they are lead by the Commission or the Industry. For example, the ICT Coalition and the CEO Coalition both regroup industry partners, NGOs, experts, public authorities, and aim at creating a better online environment for children. For the CEO Coalition, signatory companies committed to take positive action throughout 2012 in 5 areas: simple tools for users to report harmful content and contact, age-appropriate privacy settings, wider use of content classification, wider availability and use of parental controls, effective take down of child abuse material.[30]

[29] Beatbullying, op. cit. p. 10.
[30] http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm

The role of governments and policy makers

Governments and policy makers can make a tremendous difference in preventing and intervening in cyberbullying cases by:

- Recognising the seriousness of bullying and cyberbullying;
- Including these issues as priority areas of action;
- Support proven anti-bullying programmes among which those of civil society organisation.

Governments should also periodically **review their legislation** to ensure that law enforcement authorities (police, courts…) can act effectively against cyberbullying. In this regard, it is in the government's remit to **strike the right balance** between protecting individuals' right to privacy and free speech and enabling victims of cyberbullying to press charges against a perpetrator, allowing law enforcement authorities to carry out an investigation and collect elements or proof.

Finally, it is also within the scope of policy makers, both at National and European level, in case self-regulation or co-regulation fails, to r**egulate** online service providers.

Examples of self-regulation include for instance the social networking principles agreed to at European level between the Commission and key industry stakeholders. Should self-regulation fail to deliver, for instance, on making it easy to report abusive content or on providing a timely response to a complaint, policy makers need to consider regulatory measures.

The role of NGOs and civil society organisations

Civil society organisations are extremely diverse and their role is directly linked to their specificity:

- Organisations can work with different **target groups or actors** (children, parents, trainers, teachers, schools, governments and policy makers, women, men, victims, perpetrators…)
- Their **activities** can include:
    - raising awareness:
    - providing training sessions (for young people, professionals and parents);
    - producing resources
    - cooperating with schools, online service providers or law enforcement and acting as an intermediary between these traditional actors;
    - campaigning for change and lobbying governments;
    - directly assisting victims, parents of victims, teachers… seeking information or help (as illustrated by the many helplines and hotlines available across the EU inside and outside of the INSAFE and INHOPE network).

The diversity of civil society organisations is what makes their strength. With the right support (monetary, regulatory…), they can fill in the gaps that other actors have left, like **targeting directly specific vulnerable groups** like LGBTs. Their independent nature, **free from any conflict of interest**, is a strong source of legitimacy.

Provided that their activities have been proven to be effective, civil society organisations need **support** from all stakeholders and especially governments (to ensure their enduring independence) to function fully and effectively.

Conclusion

While some tend to minimize the impact of cyberbullying and it's emergence and spread over the last years, it is worth taking a closer look at this phenomenon and its consequences.

Whether we use the most conservative or most alarming numbers on the prevalence of cyberbullying among youth, it is important to underline that these figures cannot be understood without looking at the broader context. Cyberbullying is closely linked to **bullying.** Many researchers have found that victims of cyberbullying were also bullied in real life. But why should we focus so much attention on cyberbullying?

Simply because while two decades ago victims of bullying could seek **refuge** in a "safe" environment such as the family or a circle of trusted friends, out of physical reach of the perpetrator, with the emergence of cyberbullying, a victim is **never safe** and continues to suffer from threats, hurtful messages, embarrassing and humiliating pictures or videos and so forth.

This is enough to drive a victim to the point of attempting or committing **suicide.**

So while the present times have not seen a surge in "evil bullies", the existing tools at the disposal of bullies have made it much easier and even, some would argue, less risky for bullies to hurt their victims while making it harder for victims to resist and stop the bullying and for bystanders, parents and teachers to quickly identify victims and help them (arguably, it is easier to notice a black eye than a threatening SMS).

It is up to every actor listed above to address this issue seriously as the consequences can be **life threatening**. Whether we are talking about 4% of children victims of cyberbullying or 30%, the number of affected children revolves around the hundreds of thousands and in both cases, this calls for immediate action and concern from all actors and stakeholders.

23.4.2013

Contact
Martin Schmalzried, Policy Officer - Tel: +32 2 500 56 94 - Email: mschmalzried@coface-eu.org

About the project
European Awareness Raising Campaign on Cyberbullying
#DeleteCyberbullying: www.deletecyberbullying.eu

This project is funded by the Daphne III programme. The Daphne III programme aims to contribute to the protection of children, young people and women against all forms of violence and attain a high level of health protection, well-being and social cohesion. More: http://ec.europa.eu/justice/grants/programmes/daphne/index_en.htm