Police actions with regard to cyberbullying: The Belgian case

Heidi Vandebosch, Luc Beirens, Wim D’Haese, Denis Wegge and Sara Pabian

1 University of Antwerp, 2 Federal Computer Crime Unit and 3 Local Police Leuven

Research shows that cyberbullying is a common phenomenon amongst youngsters, with potentially severe negative effects. Besides students, parents, schools, and Internet Service Providers, the police have been identified as an important actor in approaches against cyberbullying. Departing from the situation in Belgium, this article describes how the police can: help to prevent cyberbullying, by informing students, parents, and schools about the issue; play a role in the detection of cyberbullying, for instance, by creating online reporting systems (apart from the offline channels) and finally, assist in handling existing cyberbullying cases, by identifying perpetrators and helping victims.

Acciones policiales relacionadas con cyberbullying: el caso belga. La investigación existente muestra que el cyberbullying es un fenómeno común entre los jóvenes y que tiene potencialmente efectos negativos. Además de los estudiantes, los padres, las escuelas y los proveedores de servicios de Internet, la policía ha sido identificada como un importante actor en la prevención del cyberbullying. A partir del caso de Bélgica, este trabajo describe cómo la policía puede ayudar a prevenir el cyberbullying, informando a estudiantes, padres y escuelas sobre este asunto; jugando un papel en la detección del cyberbullying, por ejemplo, creando un sistema en línea de información (además de los canales presenciales) y ayudar en el afrontamiento de los casos de cyberbullying y, finalmente, identificando a los perpetradores y ayudando a las víctimas.

In an academic context, cyberbullying is usually defined as “bullying” (intentional, repetitive, harmful behavior in a relationship characterized by a power imbalance) through electronic devices (e.g., computers, mobile phones…) (Patchin & Hinduja, 2006; Smith et al., 2008). Research shows that cyberbullying is a common problem amongst young people, which has a considerable negative impact on the physical and mental health of victims (Anderson & Hunter, 2012; Heirman & Walrave, 2012; Tokunaga, 2010), and is related to other “delinquent” behavior at the side of the offender (Ybarra & Mitchell, 2004; Ybarra, Espelage, & Mitchell, 2007; Patchin & Hinduja, 2010; Wachs, Wolf, & Pan, 2012). Contrary to (most forms of) traditional bullying, cyberbullying can take place: 24/7, from outside schools, anonymously, and with a (potentially) worldwide (internet) audience (Dooley, Pyzalski, & Cross, 2009). Given these differences, the typical “whole school approach” for addressing traditional bullying in educational contexts (Samara & Smith, 2008), is considered insufficient for dealing with the newest form of bullying (del Rey, Elipe, & Ortega, 2012). Not only should the “content” of the interventions be modified to be able to address cyberbullying adequately (for instance, dealing with cyberbullying might require teaching children special internet literacy skills), but also the number and types of actors involved (Kowalski, Limber, & Agatston, 2008; Zinga, 2010). For instance, besides students, parents, and teachers, also Internet Service Providers and the police have been identified as (potentially) important actors in the fight against cyberbullying (Paul, Smith, & Blumberg, 2012; Palmer & Raskauskas, 2010; Shariff, 2008). In this article we will focus on the role of the latter.

The role of the police with regard to cyberbullying can be threefold. Firstly, the police can help to prevent cyberbullying, by informing students, parents and schools about the issue (Palladino, Nocentini, & Menesini, 2012). Secondly, the police can play a role in the detection of cyberbullying, for instance, by creating online reporting systems (apart from the offline channels). Thirdly, the police can play a role in handling existing cyberbullying cases, by identifying perpetrators and helping victims.

In this article we will depart from a case-study (i.e. the situation in Belgium) to describe and evaluate the (possible) role of the police in cyberbullying incidences (and especially those cases involving under aged victims and perpetrators). On the basis of these insights, we will also provide policy recommendations. As will become clear throughout the text, many of our conclusions will probably also hold for other countries confronted with cyberbullying.

Several school surveys conducted in Belgium (see for instance: Vandebosch & Van Cleemput, 2009; Walrave & Heirman, 2009) indicate that cyberbullying is a common phenomenon. When young people are asked directly whether they have been involved in “cyberbullying” (during the last three months or in general) these studies show prevalence rates for victimization of, respectively, 11.1% and 34.2% and prevalence rates for perpetration of, respectively, 18% and 21.2%. When asked about their experience with various potentially damaging internet and mobile activities (which are often considered as forms of cyberbullying), the percentages are even higher. For instance, in the study of Vandebosch...
and Van Cleemput (2009) conducted in 2005 amongst 10-18 year olds, the most common forms of potentially offensive Internet and mobile phone activities were: insults or threats via Internet or mobile phone (33.7 % victim, 23.7 % perpetrator), deception via Internet or mobile phone (27.3% victim, 30.8 % perpetrator), spreading gossip or rumours via Internet or mobile phone (18.9 % victim, 12.9% perpetrator) and breaking into someone’s mail or IM account and changing their password (15.9% victim, 14.6% perpetrator).

As in many other countries, there is no specific criminal law with regard to “cyberbullying” in Belgium (for an overview of the legal situation with regard to cyberbullying in the U.S. see: Stefkovich, Crawford, & Murphy, 2010; in Canada, see: Shariff, 2008; in Australia see: Campbell, Butler, & Kift, 2008). Nevertheless, some forms of cyberbullying behavior, might be qualified as a “criminal offense” and thus be the subject of criminal punishment. The existing criminal law, for instance, mentions offenses such as “stalking” (Art. 422bis), “causing damage using electronic communications” (Article 145, § 3bis of the law of 13 juni 2005 with regard to electronic communication), “hacking” (article 550bis), “informatica fraud” (Art. 210bis) ; “defamation and slander” (Art. 448, first paragraph) and “public indecency” (Article 383, first paragraph) (Walrave, Demoulin, Heirman, & Van der Perre, 2009).

As is evident from studies (e.g., Ševciková & Šmahel, 2009), many cyberbullying perpetrators are minors (and the other way around: many youngsters are cyber bullies). Because of their young age, these youngsters are restrained from full responsibility for their acts. In Belgium, like in most European countries, the age of criminal responsibility is set at eighteen. Until that age youngsters are not committing “crimes” (unless in exceptional circumstances), but “acts that are regularly defined as crimes” (Nuytens, Christiaens, & Eliaerts, 2005). In these cases judges may impose measures on the juvenile to promote safety, protection and education. More concretely, the court can refer the child to social services, administer personal council, impose educational tasks or suggest the perpetrator to report his commitment to apologize or to compensate for the loss (Walrave et al., 2009: 97).

Since the police reform of 2001, the Belgian police consists of an integrated police service on two levels: the federal police and the local police. Both levels work autonomously and under supervision of different authorities, but are linked through reciprocal support (Lippens & Van Calster, 2002).

The federal police conduct specialized law enforcement and investigation missions that cover more than one region in Belgium (Lippens & Van Calster, 2002). With regard to cyberbullying, it is important to mention the existence of a Federal Computer Crime Unit (FCCU), which works in close relationship with 25 Regional Computer Crime Units (RCCU) (Beirens, 2010b). The main tasks of the Computer Crime Units are combating “serious” ICT crimes (such as internet fraud, hacking, espionage and sabotage), doing forensic research on ICT used for other crimes (i.e. investigating the computer of a murder victim) and providing support for internet investigations (i.e. the identification and localization of people). The FCCU also manages an internet hotline: www.ecops.be, where internet users can report internet crimes. These reports are evaluated, (if necessary) dispatched to other police departments or handled by the FCCU itself.

The local police level counts 196 police zones (consisting of one or several adjacent municipalities). The Local Police perform the “basic police function”. Concretely, this means that each zone has to carry out at least six basic missions: district policing, reception, intervention, aid to victims, local investigation and public order. When exercising their tasks, the local police are regularly confronted with young perpetrators and victims. Some, but not all, of the local police departments have therefore created a specialized youth department. In line with the philosophy of Community Policing, schools are also considered an important partner for the local police in preventing and dealing with juvenile crime.

Police as actors against cyberbullying: the Belgian case

As this short overview indicates, handling cyberbullying related crimes, is not strictly limited to one police level. Although citizens might use the internet hotline of the FCCU to report cyberbullying related incidents, only in very few instances (i.e. in case of hacking), it is really their task (and that of the RCCUs) to deal with them. The local police are considered the first contact point for most cyber bullying incidents. However, they do not always have the right knowledge to handle these cases (and therefore have to ask for the assistance of the FCCU and RCCUs). This rather complicated structure, can create confusion amongst citizens (e.g. youngsters, parents…) who would like to report cyberbullying incidents, but also amongst the police units themselves.

Below we will describe the main tasks the police can perform with regard to cyber bullying. These include: 1) prevention (on the basis of knowledge of the phenomenon), 2) detection and reception of complaints, 3) stopping the crime, identifying the perpetrator and helping the victim (e.g. by removing the harmful content). Again, it will be clear that both police levels are involved. Preventive actions are being organized by the Computer Crime Units (FCCU, RCCU) and (some) local polices. These actions are often in cooperation with other partners such as schools, Internet Service Providers (Associations) (like ISPA Belgium), and the e-safety sector (e.g. Child Focus). The most important target groups are: youngsters, parents and schools.

The Computer Crime Units have extensive knowledge on cyber crime (in general), which they can draw upon in their prevention activities (Beirens, 2010a). The FCCU organizes approximately fifty information sessions about e-safety and cyber crimes (including cyberbullying) a year, usually in close collaboration with other partners (e.g. schools). The “police” input often consists of giving concrete examples, suggestions on how to behave safely, and tips on what to do and whom to contact in case of victimization. Other preventive actions of the FCCU and the RCCUs include: special brochures, comic books, and (twice a week) one-minute e-safety advices on a radio station for the general audience (Beirens, 2010b). The FCCU also helped to create a special handbook on “Legislative Procedures of Computer and Network Misuses in EU countries”, to inform and support the local police.

On the local level, there seems to be variety in the (preventive) attention that the police pay to the phenomenon of cyberbullying. In some police zones (like the police zone Leuven), the local police organized a survey study to establish a picture of off- and online bullying amongst youngsters (D’Haese, 2010). Another example of an initiative by the local police is the “adoption” of school classes by police inspectors (of the police departments of Antwerp and Leuven). These inspectors try to sensitize their class concerning juvenile delinquency (and cyberbullying in particular) and to build...
trust in their relationship with students (D’Haese, 2010). There are also some (limited) initiatives from police officers to be present on the Internet and on social network sites. For example, the student inspector of the local police of Leuven (a university town) has a personal facebook page where students can ask questions (Beirens, 2010b). It should be noted that the examples of cyberbullying prevention activities from the local police mentioned above, come from relatively large police departments in cities with a “young” population, which are probably not representative for other local police departments.

Besides preventive actions, the police are also involved in detecting instances of cyberbullying. Crucial for this detection are user notifications. The FCCU is often informed about cyberbullying by bystanders or victims using the online reporting system, eCops. On this online platform users can report crimes (but not officially file complaints), committed on or through the internet. The reported incidents are very diverse. They range from harassment and stalking to fraud and child pornography. Figure 1 provides an overview of the different criminal specifications which apply to reported incidents related to the two most popular social networking sites in Belgium: Netlog (which is especially popular amongst youngsters) and Facebook (which reaches a more general audience). Some of these behaviors may constitute a form of (what academics define as) “cyberbullying” (i.e. intentional, repetitive, harmful actions through electronic devices, in a relationship characterized by a power imbalance). However, given the lack of information on the context in which these acts take place, it is not possible to extract pure “cyberbullying” incidents from police files. Moreover, the incidents that are being reported to eCops are probably not representative for all the abuses that people witness on the internet (people might only report the serious cases). The statistics resulting from (scientific) studies focusing on (and clearly describing) cyberbullying might therefore give a more accurate picture of the prevalence of the problem (although they also often rely on self-reports).

Additional notifications reach eCops via Child Focus and Netlog, two organizations (cfr. supra) with which the police cooperate. Instances of child pornography that are reported on Child Focus’ website, for example, are passed to the FCCU. Netlog, a social network site, features a “report abuse” button on member pages and can also automatically forward a standardized complaint to eCops, if necessary (Beirens, 2010b).

It is evident that cyberbullying detection is primarily based on user initiated actions. The federal police receives reports through eCops (directly or by collaborating organizations) from bystanders or victims. To officially file a complaint (which requires a signed declaration and is necessary for some types of crimes) cyberbullying victims are recommended to contact their local police department. When people contact the (local) police to file a complaint about cyberbullying, law enforcement officers first have to evaluate whether (and how) the reported behavior can be qualified as an offense. As noted earlier, not all instances of cyberbullying may be considered “criminal” acts. Beirens (2010b) gives the example of publishing other people’s pictures online without permission.

![Figure 1. eCops-messages concerning Netlog and Facebook per penal qualification - 2010](source: Federal police, Federal Computer Crime Unit, eCops database)
This behavior is subject to civil liability, because it constitutes an infringement on portrait rights. Law enforcement, however, is not competent in this matter, as civil cases are only dealt with in court. In other instances, different criminal provisions (cfr. supra) might be used to label the same “cyberbullying” behavior.

Apart from “qualification” problems, cyber crimes in general (and cyberbullying in particular) also give rise to procedural questions, such as: who is territorially qualified to intervene (e.g. when two Belgians are bullying each other on the American SNS Facebook)? To avoid deadlocks, the public prosecutor currently assumes to be qualified to handle all incidents that have illegal effects in Belgium.

Stopping cyberbullying, identifying the bullies and helping the victims

When dealing with cases of cyberbullying, the local police (potentially with the assistance of the Regional Computer Crime Units or, in very serious cases, the FCCU), will firstly try to identify the perpetrator(s), since - as is also indicated by academic research on cyberbullying (see for instance: Kowalski & Limber, 2007), many of them try to disguise who they are (e.g. by creating a false profile).

In trying to identify the offenders, the police can sometimes rely on evidence on the side of the victims (e.g. records of the abuse: dates, times and virtual places, the content of the message(s), user names, e-mail addresses…). In many instances, however, (young) victims of cyberbullying are too shocked at the time of the incident to react in an appropriate way. Instead of saving the evidence, they, for instance, often delete the threatening messages they got. In that case the police might investigate the computer or mobile phone of the victim to find traces e.g. in the log files of chat applications, in mails, in configuration files, and so on.

Starting from these traces (i.e. IP addresses, nick names…) the police then usually have to cooperate with (different types of) Internet Services Providers. A major distinction is that between Access Providers (who provide a link from the customer to the internet, or a mobile or fixed telephony network) and Content Providers (e.g. Social Network Sites, photo sharing sites, messaging systems, and so on). The data held and the legal situation applying, differ for each type. The Access Providers are described as “operators” by the Belgian Electronic Communication Law of 13 June 2005 (BS 20 juni 2005). This law prescribes that these operators have to have a (continuously available) coordination cell “justice” and sets the time limits within which they have to give an answer to questions (court order/warrant) from legislatively designated authorities. The primary legal imperative for these ISPs (as infrastructural suppliers) is customer data protection and privacy (cfr. the EU directive 58/2002, which installs a general principle of wiping or rendering anonymous all information concerning e-communications, except when needed for billing or marketing, or when needed for national security and investigation (as provided by national law)). The EU directive 24/2006 on data retention (which tries to harmonize the exceptions of art. 15 in the EU directive 58/2002), formulates obligations with regard to the retention of certain types of (connection) data (date/time, source/
destination, location of device) for some types of communication (telephony, internet access, internet telephony, e-mail), for a period between 6 and 24 months. Content Providers (like, for instance, SNS) are not legally obliged to retain data with regard to the activities of their end users. For these services, the police do not know what type of data they keep and for how long.

The information exchange between the ISPs and the police may thus help the latter to gather “evidence” and to detect the “criminal”. This cooperation is also necessary to mitigate the problem (i.e. to remove certain (illegal) contents). Both in Europe and the US the states have imposed the power of “content self regulation” on these private actors (Ahlert, Marsden, & Yung, 2004; Lievens, Dumortier, & Ryan, 2006): “Under Notice and Takedown (NTD) regimes Internet Service Providers have the duty to remove illegal and harmful content from the internet once they are made aware that their servers host it” (Ahlert et al., 2004). These notifications may not only come from the police. Many Content Providers (for example, SNS like Facebook) also provide possibilities to their users to (directly) report abuses to them. Furthermore they often actively screen the (public) contents themselves (by using human or automatic monitoring). On the basis of these reports and detections, they can remove certain content (which represents “illegal” content or breaches the T&C of use), or take other measures such as excluding the offender from further using their services (based on the same T&C of use) (Walrave et al., 2009; Durrant, 2010).

Discussion

Cyberbullying is a common phenomenon (especially) amongst youngsters, in Belgium (Vandebosch & Van Cleemput, 2009; Walrave & Heirman, 2009: 10) but also in other countries (Aoyama & Talbert, 2010; Livingstone et al., 2011). It refers to behaviors such as: insulting or threatening someone online or by mobile phone, organizing a defamatory polling website, posting embarrassing pictures or video clips, creating fake profiles on SNS, spreading gossip and false rumors, and so on. Research shows that cyberbullying may have severe negative consequences for the victim. Factors that are said to possibly increase the impact of cyberbullying (compared to traditional bullying) are its 24/7 character and (potentially) world wide audience. Although there is a considerable overlap between “traditional bullying” and “cyberbullying”, suggesting that what happens offline (for instance, in a school context) is extended online, the typical “whole school”-based approaches (involving students, parents and teachers) are often deemed insufficient to deal with this problem. Both ISPs and the police have been identified as other relevant actors in the battle against cyberbullying. In this article, we especially focused on the past and current actions of the (Belgian) police with regard to cyberbullying amongst youngsters, and the specific problems they encounter(ed).

This overview, however, may also raise a more fundamental question, namely: should the police actually be involved in cyberbullying amongst youngsters? There are a range of arguments that would plea in favor of not involving the police. Like traditional bullying, cyberbullying, is often regarded as a form of (peer) aggression that is quite “normal” in certain developmental phases (childhood/adolescence) (Tyler, 1998). In these phases children and adolescents learn social skills and moral norms by trial and error. Instead of looking at cyberbullying from a legal perspective, which implies that the acts and the perpetrators are being “criminalized”, a more social-therapeutic perspective could be more appropriate. This philosophy is, for instance, also present in the “no blame” approach against (traditional) bullying from Robinson and Maines (1997). Transferred to the context of cyberbullying, this means that the different parties involved (youngsters, parents, schools), should try to prevent and solve cyberbullying in a constructive way.

Another argument against the involvement of the police in cyberbullying amongst youngsters, is the fact that not all forms of cyberbullying (as identified in the academic literature or experienced by youngsters) really constitute a criminal offense. Students that are massively being defriended on SNS, for example, are (theoretically speaking) the victim of social exclusion (a form of cyberbullying). But defriending someone is clearly not a crime. Other types of cyberbullying behaviors (such as those involving the publication of other people’s pictures without their permission) are only subject to civil law (and thus not relevant for the police). Moreover, the distinction between what constitutes bullying behavior, a joke, or an argument is often blurred, especially in an online context (with less interactional cues) (Kowalski et al., 2008). From a police perspective, many of the complaints on cyberbullying (as for instance reported on e-Cops) are in fact complaints on online “quarrels” (Beirens, 2010b). These “quarrels” should be solved by the actors involved themselves, instead of taking up the scarce police capacity (which could better be devoted to “serious” offenses). Internet Services Providers (who are increasingly aware of their role in the fight against possible abuses of their services) provide their users with several empowering (technological) tools. On many Social Network Sites, for instance, users can adjust their privacy settings (to minimalize the risk of being victimized) and report abuses (which may lead to the removal of illegal or harmful content or fake profiles and the exclusion of the offender from further use of the services).

There are, however, also some arguments in favor of the involvement of the police in cyberbullying amongst youngsters. First of all, it is clear that mobile phones, computers, and the internet give a new dimension to bullying. What before was restrained to a rather clear (physical, time) context (i.e. school (time)), with related actors (students, parents, teachers), is now taken into “cyberspace”. While school teachers and principals often take a central role in the prevention, detection and solution of the traditional bullying that happens in schools, their role with regard to cyberbullying is less clear cut. Although cyberbullying is often an extension of “real life” bullying (in school), most online bullying actually takes place from outside school and outside school hours. This may also make it less evident that schools mediate in cases of cyberbullying (between, for instance, the victim and the perpetrator and their respective parents). Hence, the (local) police might fulfill this role. This function of the police also fits with the current “community policing” concept (central in Belgian policing).

The involvement of the police is also necessary in those cases where cyberbullying does represent a serious threat to the mental and/or physical health of the victim, and fast cooperation with the ISPs is needed (to identify the perpetrator and to stop the crime). Some typical “serious” cases in Belgium (handled by the FCCU) were: a 2003 case in which a young woman became the victim of the creation of false profiles on sex sites (by an ex-boyfriend who used intimate pictures of her and also mentioned her contact information, resulting in unwanted phone calls and visits from
strangers) and a case in 2006 in which a 13 year old boy became the victim of cyberbullying in an online game and via mobile phone (the boy announced his suicide online and actually committed suicide).

As indicated in this article, the work of the police in the case of cyber bullying (and cybercrime more in general) is not always easy. The number of policemen specifically dealing with cyber crime (at the FCCU and the RCCUs) is limited, and sharply contrasts with the (rising) number of abuse reports (on e-Cops, Child Focus, SNS...). The local police, who are considered the first contact point for cyber bullying incidents, do not always have the right (ICT) expertise to deal with these cases. The fact that both the federal and the local police can actually be involved in dealing with cases of cyberbullying, may also lead to confusion, both on the side of the police and of the general public. Another problem concerns the legal qualification of cyberbullying. As is clear from this article, cyberbullying may consist of different types of behaviors (to which different qualifications may apply). As a result it is very difficult, if not impossible, to extract correct information on the prevalence of cyberbullying, from the police databases. Apart from these “qualification” problems, cyber

crimes in general (and cyberbullying in particular) also give rise to procedural questions, such as: who is territorially qualified to intervene (e.g. when two Belgians are bullying each other on the American SNS Facebook)?

To conclude, it is evident that to address cyberbullying effectively, an integrated approach is necessary, involving youngsters, parents, schools, the police and ISPs. Parents and schools (and e-safety organizations) can fulfill their educating role by teaching youngsters how to behave safely and appropriately online. They can also closely monitor the online activities of their children and students, and intervene in (less serious) cases of cyberbullying, e.g. by urging the (known) perpetrator to delete the harmful content, or by reporting the abuse (by an unknown) offender to the ISPs. The involvement of the police is necessary in those cases where cyberbullying does represent a serious threat to the mental and/or physical health of the victim, and fast cooperation with (international) ISPs is needed (to identify the perpetrator and to stop the crime). This also requires better international procedures to obtain digital traces from ISPs, retention principles for all ISPs, adequate “notice and takedown” procedures, and more “cyber police” (not only police involved with IT forensics).

References


Psicothema, 24, 621-627.


Lippens, R., & Van Calster, P. (2002). Policing as forestry? Re-imagining the mental and/or physical health of the victim, and fast cooperation with (international) ISPs is needed (to identify the perpetrator and to stop the crime). This also requires better international procedures to obtain digital traces from ISPs, retention principles for all ISPs, adequate “notice and takedown” procedures, and more “cyber police” (not only police involved with IT forensics).


