



EUROPEAN DATA
PROTECTION SUPERVISOR

Cyber-Harassment Closing Conference

Teacher Union strategies on Cyber-Harassment

Bratislava, 7 June 2010

Data protection legislation in Europe, preventing cyber-harassment by protecting personal data and privacy

Giovanni Buttarelli, Assistant European Data Protection Supervisor

Speaking points

1. I have been asked to speak about data protection legislation in Europe in the context of cyber-harassment in schools. In particular, you wanted to hear about the extent to which data protection legislation could prevent or be used as a tool to deter cyber-harassment, for example, of teachers and students alike.
2. To address this issue, first, I would like to say a few words about harassment and how it has been aggravated by information and communication technologies.
3. Second, I would like to talk about why data protection applies and the responsibility of individuals engaged in publishing other people's information on the Internet, including the responsibility of the platforms. In this context, the principle of privacy by design or privacy by default is very important.
4. Third, I would like to walk you through the main principles of European data protection legislation. In particular, I want to illustrate how data protection principles may be violated in some cases of cyber

harassment. I will talk about the role of individuals when they upload information on the Internet harassing other individuals.

5. Fourth, I want to refer to the role of the Data Protection Authorities, which are independent authorities that are responsible, among others, for enforcing the European and national data protection laws. People who have suffered cyber bullying should consider complaints before such authorities.
6. Let us start with the first point, setting up the scene.
7. Harassment understood as unwanted or unwelcome behavior which may range from unpleasant remarks to physical violence has existed for a long time. When information and communication technologies are used to harass individuals, we talk about cyber-harassment.

As some speakers have confirmed this morning, cyber-harassment is increasing by the day. We hear constantly how children, teenagers are humiliated or harassed by their peers using blogs, social networks, instant messaging etc. Very often rumors or gossip are posted in social networks to instigate others to dislike and gang up on the targeted individuals. In some cases, individuals engaged in cyber harassment pose as the identity of a victim for the purpose of publishing material in their name that defames or ridicules them. Cyber-bullying may have terrible consequences, including intimidation, emotional damage and even suicide. Teachers are not spared from cyber harassment either. Pictures posted in social networks to radicalize them, comments about their looks or social life posted in blogs, are only examples. You may all be aware of the web site 'RateMyTeacher' which features reviews of teachers. Difficulties are also to be mentioned in having this information deleted: once something it is on Youtube or on another site, one loses control and it is very difficult to have it deleted or rectified. Dissemination and loss of control are major problems with cyber-harassment.

The use of ICT and its evolution into cyber-harassment offer three new dimensions which need to be underlined and addressed in order to grasp properly the new potential damages and to identify possible countermeasures:

- the individual who conducts this harassment benefits from an almost absolute anonymity provided by on-line platforms which do not require strong identification or even a simple registration. A safe or "immune" position is therefore offered. On the other hand traceability means processing of personal data, and the providers of

platforms like social network will have to comply with the corresponding data protection rules. A delicate balance will have to be found between the need to protect online users from harassment and the need to avoid blocking social discussions, which generates online advertisement revenue, as much as possible.

- the Information Society also provides an unbelievably large scale diffusion for the communication of the harassment and offers the possibility to involve a large number of people. Pictures can be instantaneously broadcast the general public reaching an almost unlimited number of individuals. This digital world offers to its users the possibility to widely publish "information" and this capability is immediately available - free of charge. The providers of such platforms are however in a position to technically limit these communication abilities and enforce some obligations on their users or at least raise their awareness on the risk of such tools and their responsibility from a data protection point of view.

- It is important to highlight the persistent memory of the internet regarding the information used for the harassment. This information might stay for ever on the web and will be extremely difficult to erase completely. This point presents a great challenge for the respect of the right to be forgotten or for the enforcement of an appropriate and proportionate data retention policy. Here again the providers of such platforms are in a position to play a determinant role and their role could be driven by the respect of data protection rules which can, if properly implemented, mitigate the side effects produced by these three factors.

8. The second point refers to the responsibility under applicable EU data protection laws.
9. Harassment potentially constitutes insult or defamation and may be pursued as such. In addition, such behavior is a criminal offense. In this context and against the background described above, a starting question is why data protection legislation plays a role in this context? The answer is simple: data protection legislation applies 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. The legislation sets forth various principles that must be respected by those who process personal data, for example, by those who publish information about third parties.

- *Individuals*

10. When individuals put information about third parties, for example, comments on their appearances or behaviors, independently of whether this constitutes legally cyber-harassment, they disclose personal information of their victims. For example, their real name, their address, school, etc. The principles and obligations embodied in the EU data protection legislation are fully applicable to the disclosure of this information, which under EU legislation qualifies as personal data, for example, in forums or social networks. For example, data protection legislation requires informing and in many cases obtaining the consent of individuals before publishing information that relates to them. Obviously, those engaged in cyber harassment do not inform, much less ask for the consent of their victims to publish their personal data, thus, automatically breaching data protection legislation.
11. A related, very important question to address is who in this context is bound by EU data protection legislation. In other words, who is obliged to comply with the rules of EU data protection legislation and who may be ultimately responsible and subject to sanctions. Who is ultimately responsible ?
12. Teenagers or even adults sometimes do not realize that by publishing information about third parties they are becoming what the EU data protection legislation calls 'data controllers'. These are the individuals or legal entities that are who control and are responsible for the use of personal information that they collect and further process, for example uploading on the Internet. They do not realize that under law being a data controller carries with it serious legal responsibilities.
13. This was confirmed in 2003 by European Court of Justice in the so called Lindqvist case. In particular, the Court upheld that (1) The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC (2) Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.
14. Recently, in its Opinion n. 5/2009 on social networks, the Article 29 Working Party has confirmed that in many cases users are considered to be data controllers, particularly if they give access to data to a number of users that goes beyond self-selected contacts. In this regard, there is a clear need for schools and parents to set up

appropriate measures to teach children about such responsibilities. A second WP 29 Opinion adopted on February 2008 on the protection of children's personal data (General Guidelines and the special case of schools) should be also mentioned today.

15. The above leads me to highlight the need for children's education, as early as possible, about the importance of respecting other people's privacy, information, etc. There is an absolute need to be very proactive and spare no efforts to show children the importance of information, the existence of legal rules in this context and last but not least the 'dangers' associated with publishing personal data, given the large scale diffusion of the Information that is put on the Internet.
16. The responsibility of those entities that provide the platforms, such as social networks could be engaged. You may remember a much commented upon case of a Milan court which held three Google executives criminally responsible for an online video of an autistic teenager being bullied. They were found guilty of violation of Italian data protection legislation by virtue of posting the video made by other teenagers. While I do not want to enter into the merits of this case, it is true that liability for hosting third party content, as in this case, is subject to the liability limitations of the eCommerce Directive and it is less clear how/under which circumstances they could be liable under data protection for third party content (except if they have knowledge of the content and they have not taken it down).
17. In addition to the above, data protection authorities around the EU as well as the Commission have urged social networks and other platforms to implement 'privacy by default' settings. The idea is that users' information should be 'by default' private. This would help to ensure that only for those who are voluntarily interested in sharing their data with other people would the barriers to be taken down. However, we see that today the exact opposite principle tends to apply. For example, Facebook, applies a no-privacy policy by default, meaning that only the most privacy-conscious users protect their profiles. Other users' profiles are accessible to all without their knowledge.
18. The third point of my presentation refers to the specific data data protection rules. It is not possible in the short time of this presentation to give you a thorough description of EU data protection legislation. This would take too much time. However, I think that I can very briefly refer to the main principles, in particular

to whose which should be respected. The basic principles which I will mention are those of necessity and proportionality, purpose limitation, notice and information, the rights of data subjects and data retention. The principles of necessity and proportionality are a cornerstone of data protection: in few words, personal data should only be collected and processed if it is necessary for a determined purpose. About notice and information it should be said that data protection is also about processing personal data "fairly". Fairness generally requires you to be transparent – clear and open with individuals about how their information will be used. Purpose limitation means that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. In addition, personal data shall be processed in accordance with the rights of data. These include a right of access to a copy of the information relating to them, a right to request rectification of inaccurate or incomplete data, a right to object to the processing for legitimate and serious reasons and a right not to be subject to automated individual decisions. Finally, the principle of data retention is that personal data should only be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they were further processed.

19. The fourth point of my presentation refers to data protection authorities and to their enforcement powers.
20. Under EU data protection legislation, each member state must set up a supervisory authority, an independent body, competent to monitor the data protection level in that member state as well as to start legal proceedings when data protection regulation has been violated.
21. A very important element to highlight is that individuals may lodge complaints about alleged violations to the data protection legislation to the supervisory authority or in a court of law. The authorities are obliged to hear claims concerning the protection of the rights and freedoms of individuals in regard to the processing of personal data and to inform the person concerned of the outcome of the claim.
22. From the point of view of data subjects, in this case of those who are victims of cyber-harassment, the possibility to file a complaint for violation of data protection legislation with the data protection authority is a very relevant course of action. Data Protection Authorities can (if not overloaded) offer more flexible assistance/

access to redress than courts, with less costs. Of course, one of the problems that can be encountered in this context is that sometimes it may be difficult to identify the responsible individual if his/her comments were made anonymously or using a pseudonym, which is often the case. There is a conflict here between the right to be (completely) anonymous which we have always defended, and the right for those being harassed to obtain redress. Another aspect of the problem is that ISPs deny in some case access to names of those responsible for harassment, for the same privacy reasons they use against IP rights holders requests. I think they should give that information also to DPAs because they act in a very different capacity (official authorities) than copyright holders. I suppose part of the solution for that conflict between privacy of the offender and of the victim is also on the judicial side.

23. Finally, connected to this problem there is a question of applicable law, which sometimes arises although cyber-harassment is frequently made on a national basis only. Under the data protection perspective, the criteria of applicability of the law is the establishment of the controller (and the means when the controller is established outside the EU). This means that the nationality and the place of habitual residence of data subjects is irrelevant, as well as the location of the processing.

This induces a broad scope of application, with extraterritorial implications. The Directive 95/46 -and national laws of implementation- indeed apply to the processing of personal data outside the EU (when the controller is established in the EU), and it also applies to controllers established outside the EU (when they use means in the EU).

The purpose of this broad scope of application is primarily to ensure that individuals are not deprived of the protection to which they are entitled under the Directive, and concomitantly, avoid circumvention of the law.

According to this framework, in the area of data protection it is particularly important to distinguish the concept of applicable law, which determines the provisions applicable to a certain matter, from the concept of jurisdiction, which instead refers to the material or geographical scope of the competence of the authorities that may apply and enforce the applicable law.

24. Let me finalize by highlighting some points that I have made during this presentation:

First, clearly, when individuals put information about third parties, for example, comments on their appearances or behaviors, independently of whether this constitutes legally cyber-harassment, they disclose personal information of their victims. This behavior is subject to data protection rules which must be obeyed. Lack of compliance is punishable.

Second, education is key in this context. Schools and other education related initiatives should dedicate efforts to educate children. Such education should aim at showing children the effects of publishing theirs and others people information. They should proactively tell them about their legal implication and overall negative effects that may have in their lives.

Third, those whose data protection rights have been violated should not hesitate to launch complaints also with data protection authorities. They have the powers to investigate and impose sanctions. However, it is a fact that in many cases the investigation will not be straight forward, also due to the difficulties in identifying the authors or in acting in a certain jurisdiction.

In conclusion, in any event data protection is to be considered as an helpful tool not only for prevention and repression but also for education.

Thank you for your attention

Giovanni BUTTARELLI