Opinion of the European Data Protection Supervisor

on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION

I. INTRODUCTION

1. On 29 March 2010, the Commission adopted a proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA[1] (further: the proposal).

2. The proposal intends to repeal a Framework Decision adopted on 22 December 2003, due to some shortcomings of this previous legislation. The new text would improve the fight against child abuse with regard to the following aspects: criminalisation of serious forms of child abuse in relation for instance to child sex tourism, protection of unaccompanied children; criminal investigation and coordination of prosecution; new criminal offences in the IT environment; protection of victims; prevention of offences.

[1] COM(2010)94 final

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

3. With regard to the objective to prevent offences, one of the tools would be the restriction of access to child pornography on the internet.

4. The EDPS has noted the main purpose of the proposal. His intention is not to question the need to put in place a better framework providing for adequate measures to protect children against abuses. He nevertheless wishes to stress the impact of some of the measures envisaged in the proposal, such as the blocking of websites and the setting-up of hotlines, on the fundamental rights to privacy and data protection of different individuals involved. For this reason, he has decided to submit this brief opinion at his own initiative.

II. ANALYSIS OF THE PROPOSAL

5. The data protection issues relate to two aspects of the proposal, which are not specific to the fight against child abuse but to any initiative aiming at the collaboration of the private sector for law enforcement purposes. These issues have already been analysed by the EDPS in different contexts, especially related to the fight against illegal content on the Internet[2].

6. With regard to the proposal, the two elements of concern are developed in recital 13 and in Article 21. They can be described as follows.

II. 1. The role of service providers with regard to the blocking of websites

7. The proposal foresees two possible alternatives to block access from the Unions' territory to internet pages identified as containing or disseminating child pornography: mechanisms to facilitate blocking by order of competent judicial or police authorities, or voluntary actions by Internet Service Providers to block the internet pages on the basis of codes of conducts or guidelines.

8. The EDPS questions the criteria and conditions leading to a blocking decision: while he could support actions taken by police or judicial authorities in a well defined legal framework, he has strong doubts about the legal certainty of any blocking operated by private parties.

9. He questions first of all the possible monitoring of the internet which could lead to such blocking. Monitoring and blocking may imply different activities, including scanning the internet, identifying unlawful or suspect websites and blocking access to end users, but also monitoring online behaviour of end-users who are trying to access or download such content. The tools used are different and imply different degrees of invasiveness, but give rise to similar questions as to the role of Internet Service Providers with regard to the processing of content information.

[2] The EDPS has issued in particular the following opinions which include remarks relevant in view of the present initiative:
- EDPS Opinion of 23 June 2008 on the Proposal for a Decision establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, OJ 2009, C 2/2
- EDPS Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti Counterfeiting Trade Agreement (ACTA).
See also Article 29 Working Party, Working Document on data protection issues related to intellectual property rights (WP 104), adopted on 18 January 2005.

10. These surveillance activities have consequences in terms of data protection, as personal data of various individuals will be processed, be it information about victims, witnesses, users or content providers. The EDPS has in previous opinions expressed his concerns regarding the monitoring of individuals by private sector actors (*e.g.* ISPs or copyright holders), in areas that are in principle under the competence of law enforcement authorities[3].

- The EDPS underlines that monitoring the network and blocking sites would constitute a purpose unrelated to the commercial purpose of ISPs: this would raise issues with regard to lawful processing and compatible use of personal data under Article 6.1.b and Article 7 of the Data Protection Directive[4].

- The EDPS questions the criteria for blocking and stresses that a code of conduct or voluntary guidelines would not bring enough legal certainty in this respect.

- The EDPS also underlines the risks linked with possible blacklisting of individuals and their possibilities of redress before an independent authority.

11. The EDPS has already stated at several occasions that "*the monitoring of Internet user's behaviour and further collection of their IP addresses amounts to an interference with their rights to respect for their private life and their correspondence (...). This view is in line with the case law of the European Court of Human Rights*[5]". Considering this interference, more appropriate safeguards are needed to ensure that monitoring and/or blocking will only be done in a strictly targeted way and under judicial control, and that misuse of this mechanism is prevented by adequate security measures.

II. 2. The setting-up of a network of hotlines

12. A network of hotlines, as mentioned in recital 13 of the proposal, is foreseen by the Safer Internet Programme on which the EDPS has issued the opinion referred to above. One of the comments of the EDPS relate precisely to the conditions according to which information would be collected, centralised and exchanged: there is a need for a precise description of what should be considered as illegal or harmful content, who is enabled to collect and keep information and under what specific safeguards.

13. This is particularly important considering the consequences of reporting: in addition to the information related to children, personal data of any individual connected in some way with the information circulating on the network could be at stake, including for instance information on a person suspected of misbehaviour, be it an internet user or a content provider, but also information on a person reporting a suspicious content or the victim of the abuse. The rights of all these individuals should not be overlooked when developing reporting procedures: they should be taken into account in compliance with the existing data protection framework.

[3] See both EDPS opinions mentioned above.
[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.
[5] EDPS opinion on ACTA, p. 6.

14. The information collected by these hotlines will also most probably be used for prosecution during the judicial stage of the case. In terms of quality and integrity requirements, additional safeguards should be implemented in order to guarantee that this information considered as digital evidence has been properly collected and preserved and will therefore be admissible before a court.

15. Guarantees related to the supervision of the system, in principle by law enforcement authorities, are decisive elements to comply with. Transparency and independent redress possibilities available to individuals are other essential elements to be integrated in such a scheme.

III. CONCLUSION

16. While the EDPS has no reason to challenge the development of a strong and effective framework to fight against sexual abuse, sexual exploitation of children and child pornography, he insists on the need to ensure legal certainty with regard to all actors involved, including Internet Service Providers and individuals using the network.

17. The mentioning in the proposal of the need to take into account the fundamental rights of end users is welcome but not sufficient: it should be complemented by an obligation for Member States to ensure harmonised, clear and detailed procedures when fighting illegal content, under the supervision of independent public authorities.

Done in Brussels, 10 May 2010

(signed)

Peter HUSTINX
European Data Protection Supervisor