EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies

(2009/C 2/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

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 [1],

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 [2], and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 4 March 2008 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

Consultation of the EDPS

1. The Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies (hereinafter 'the proposal') was sent by the Commission to the EDPS for consultation on 4 March 2008, in accordance with Article 28(2) of Regulation (EC) No 45/2001. This consultation should be explicitly mentioned in the preamble of the decision.

The proposal in its context

2. The new multiannual programme (hereinafter 'the programme') is presented in the continuity of the Safer Internet (1999-2004) and the Safer Internet Plus programmes (2005-2008).

3. Four orientations are defined:

   — reducing illegal content and tackling harmful conduct online,

   — promoting a safer online environment,

   — ensuring public awareness,

   — establishing a knowledge database.

4. The programme is presented as consistent and complementary to relevant Community policies, programmes and actions. Considering the number of existing regulatory measures in the field of the protection of children in the context of new technologies, this programme concentrates on action rather than regulation. Focus is put on the efficiency and effectiveness of initiatives to be taken, and adaptation to the evolution of new technologies. In this perspective, it foresees enhanced exchanges of information and best practices.

5. As a framework instrument, the programme does not go into the details of the actions to be taken, but allows for calls for proposals and calls for tenders in line with the four orientations defined.

Focus of the opinion

6. The general orientations of the programme address the protection of children using the Internet and other communication technologies without putting emphasis on the privacy aspects of the issue [3]. While being totally supportive of the objective of the proposal, the EDPS will in this opinion highlight these privacy aspects.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.

[3] Some references to privacy can be found in the Impact Assessment (3.2. Specific risks: disclosure of personal information; 3.3. Target groups; 5.2. Analysis of the impact of the policy options) but they are not significantly developed.

7. The EDPS considers as essential that the initiatives planned be consistent with the existing legal framework as cited in the proposal ([1]), and in particular Directive 2000/31/EC on e-commerce, Directive 2002/58/EC on e-privacy, and Directive 95/46/EC on data protection ([2]).

8. The protection of personal data should be taken into account with regard to different aspects and different actors involved in the programme: the protection of personal data of children is of course the main issue, but not the only one: personal data related to persons and contents under scrutiny for the purpose of protecting children should also be taken into consideration.

9. These issues will be developed as follows in this opinion:

— Chapter II will develop the link between data protection and the safety of children, highlighting the fact that the protection of children's data is an indispensable step towards more safety and prevention of abuse,

— in Chapter III, the opinion will stress the fact that processing of personal data is also inherent to the reporting, filtering or blocking of suspicious contents or persons on the Internet:

— in a first point, the question of the reporting of suspected persons or facts will be analysed in a data protection perspective,

— the second point will focus on the role of technical tools,

— the responsibility of the industry, in relation with their control on users' data and on content data will be the subject of the last point.

II. **PROTECTION OF PERSONAL DATA AND SAFETY OF CHILDREN**

10. The EDPS fully supports the objective of the programme and the orientations defined in order to enhance the protection of children online. In particular, reducing illegal or harmful content and raising awareness of children and other actors involved are decisive measures which should be further developed.

11. The EDPS wishes to recall that an appropriate protection of the personal information of the child is an essential preliminary step to ensure safety while being online. This interconnection between privacy and security of children is explicit in the recent Declaration of the Committee of Ministers 'on protecting the dignity, security and privacy of children using the Internet' ([3]). The declaration recalls the right of children to dignity, special protection and care as is necessary for their well being, 'to protection against all forms of discrimination or arbitrary or unlawful interference with their privacy and to unlawful attacks on their honour and reputation'.

12. As examples of risks associated with the protection of the privacy of children, the declaration cites the traceability of children's activities that may expose them to criminal activities, such as solicitation for sexual purposes or other illegal activities. Profiling and retention of personal data regarding children's activities are also presented as leading to a potential risk of misuse, e.g. for commercial purposes, or for searches by educational establishments or prospective employers. The declaration therefore calls for removal or deletion in a reasonably short period of time of content and traces left by children online, and for the development and promotion of information to children, especially on the competent use of tools providing access to information, the development of critical analysis of content and the appropriation of adequate communication skills.

13. The EDPS supports these findings. In particular, he considers as essential to raise the awareness of the child as to the risks linked with a spontaneous communication of personal details such as real name, age or place of residence.

14. Point 3 of the measures ([4]) proposed by the multiannual programme is specifically dedicated to 'Ensuring public awareness', through actions directed to children, parents, carers and educators, as to opportunities and risks related to the use of online technologies and 'means of staying safe online'. Among the means indicated in the proposal, the dissemination of appropriate information and the provision of contact points where parents and children can receive answers to questions about how to stay safe online, are two useful tools that should integrate explicitly this dimension of the protection of the child's personal data.

15. The EDPS wishes to stress that data protection authorities are relevant interlocutors in this context. They should be mentioned as such in the proposal, especially where it foresees the promotion of cooperation and sharing of information, experience and good practice at national and European level ([5]).

([1]) Explanatory Memorandum, 2.1. The legislative context; Summary of the Impact Assessment, 1.2. State of play: legislation.

([2]) — Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1),
— Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37),
— 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).

([3]) Declaration adopted by the Council of Ministers on 20 February 2008 at the 1018th meeting of the Ministers' Deputies, available at: wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Ver=0001

([4]) Annex 1, Actions, point 3.

([5]) Annex 1, Actions, point 1.

16. Several initiatives can be mentioned as an illustration of recent actions taken in this perspective in Member States or Members of the EEA. The Swedish DPA is conducting a yearly survey on young peoples' attitudes towards internet and surveillance, just like the DPA of the United Kingdom ([1]) which conducted a survey directed to 2 000 children between 14 and 21 years old. In January 2007, together with the Ministry of Education, the Norwegian DPA has launched an education campaign directed at schools ([2]). In Portugal, a protocol has been signed between the DPA and the Ministry of Education, to promote a data protection culture on the Internet and especially on social networks ([3]). Following this project, Portuguese social networks have integrated an interface and a mascot dedicated to children between 10 and 15 years old.

17. These examples illustrate the active and decisive role played by data protection actors when it comes to the protection of children online, and the need to include them explicitly as interlocutors in the multiannual programme.

III. PROTECTION OF PERSONAL DATA AND RIGHTS OF OTHER STAKEHOLDERS

I. *Reporting and exchange of information*

18. The first point of the proposal ('Reducing illegal content and tackling harmful conduct online' ([4])) includes as one of its main actions the provision of contact points for reporting online illegal content and harmful conduct. It is not questionable that to be fought efficiently, illegal content or harmful conduct must be brought to the attention of the competent authorities. Contact points have actually already been established in relation with the protection of children but also, e.g. for the fight against spam ([5]).

19. The EDPS notes nevertheless that the notion of harmful content remains unclear: no indication is given on who is responsible for defining what harmful content is, and according to what criteria. This is all the more worrying considering the implications of a possible reporting of such content.

20. In addition, as already mentioned above, in the framework of a programme like the present one not only personal data of children are at stake, but also personal data of all persons who are connected in some way with the information circulating on the network. It can be, for instance, the person suspected of misbehaviour and reported as suspect, but also the person reporting a suspicious conduct or content, or the victim of the abuse. While this information is necessary to an efficient reporting system, the EDPS considers it important to recall that it should always be processed in accordance with data protection principles.

21. Some data at stake might even need specific protection, if they can be considered as sensitive data in the sense of Article 8 of Directive 95/46/EC. This can be the case for data related to authors of infringements as well as victims of abuse, especially when it comes to child pornography. It must be noted that at national level, some systems of reporting have required modification of the data protection legislation in order to enable the processing of judicial data of suspected offenders or victims ([6]). The EDPS insists on the fact that any reporting system to be put in place takes into account the existing data protection framework. The demonstration of a public interest, as well as guarantees related to the supervision of the system, in principle by law enforcement authorities, are decisive elements to comply with this framework.

II. *The role of technical tools in a privacy perspective*

22. The use of technical tools is promoted as one of the solutions to deal with illegal content and harmful conduct ([7]). Examples of such tools are given in the impact assessment ([8]), including age recognition, face recognition (for victim identification by law enforcement authorities) or filtering technologies. According to the proposal these tools should be better adapted to practical needs and accessible to relevant stakeholders.

23. The EDPS has already taken a clear position ([9]) in favour of the use of new technologies to enhance the protection of the rights of individuals. He considers that the principle of 'privacy by design' should constitute an inherent part of technological development which implies the processing of personal data. The EDPS therefore strongly encourages the development of projects aiming at developing technologies in that sense.

24. It is especially important to develop systems that will reduce as much as possible the exposure of children's personal data providing them a reliable protection and to offer them accordingly the opportunity to use new tools of the Information Society like social networks in a safer way.

([1]) See 'www.ico.gov.uk/youngpeople'.
([2]) See 'www.dubestemmer.no'.
([3]) See 'dadus.cnpd.pt/'.
([4]) Annex 1 of the proposal.
([5]) See e.g. the website put in place by the Belgian authorities for these purposes: www.ecops.be
([6]) See the Belgian Law on Data Protection of 8 December 1992, Article 3(6) related to the processing of data by the Centre for the reporting of missing or sexually abused children.
([7]) Annex 1, Actions, point 1.
([8]) Impact assessment, point 3.1.
([9]) 2006 EDPS annual report part 3.5.1 Technological developments.

25. It should nevertheless be recalled that, depending on the way they are used, technological tools can have a variety of impacts on individuals. If they are used in order to filter or to block information, they can stop the access by children to content that could be potentially damaging, but they can also prevent someone to get access to legitimate information.

26. Even if the major concern here relates to freedom of access to information, there is still a consequence in a privacy perspective. Indeed, filtering, especially in its most recent developments using identity management, can function on the basis of given criteria, including personal data such as the age of the individual connected to the network (to prevent access by adults or children to specified content), the content of the information and traffic data linked with the identity of the author of the information. Depending on the way this personal information will — automatically — be processed, the individuals concerned could face consequences with regard to their right to communicate online.

27. The use of filtering or blocking tools to control the access to networks must therefore be used in a cautious way, taking into account their possible adverse effects and taking full profit of the privacy enhancing opportunities offered by the technology.

28. The EDPS welcomes the precision given in the impact assessment ([1]) according to which none of the proposed options should affect the rights to privacy and freedom of expression. He also shares the view expressed therein that one of the main objectives is user empowerment, i.e. 'empowerment for making better choices and taking appropriate actions' to protect children ([2]).

III. *The responsibility of service providers*

29. The collaboration of all stakeholders is considered in the proposal as a necessary element to enhance the protection of children using communication technologies. Among these stakeholders, the proposal ([3]) foresees the participation and the involvement of the industry especially through self-regulation.

30. Being responsible for the provision of telecommunication and content services, the industry in this sector could have some influence on the reporting, filtering or blocking of information when it is considered as illegal or harmful. The extent to which it can actually be entrusted with such a task, in a legal perspective, could nevertheless lead to discussion.

31. The collaboration of the industry in the perspective of raising the awareness of children and other actors concerned, like parents or educators, is of course welcome. Putting in place alert systems and moderators on websites allowing for the exclusion of inappropriate content, is also an essential aspect of the responsibility of content providers.

32. As far as *telecommunication* service providers are concerned, the monitoring of telecommunications is however a debatable question, either aimed at the control of content protected by intellectual property rights or other illegal content. The issue raises the question of the intervention of a commercial actor, offering a specific (telecommunication) service, in a sphere where it is in principle not supposed to intervene, that is, the control of the content of the telecommunications. The EDPS recalls that such control should in principle not be done by service providers, and certainly not in a systematic way. When it is necessary in specific circumstances, it should in principle be the task of law enforcement authorities.

33. In its opinion of 18 January 2005, the Article 29 Working Party has recalled in relation with this issue ([4]) that 'no systematic obligation of surveillance and collaboration can be imposed on ISPs, pursuant to Article 15 of Directive 2000/31/EC on electronic commerce. (…) As stated in Article 8 of the Data protection Directive, processing of data related to offences, criminal convictions or security measures can be processed only under strict conditions as implemented by Member States. While any individual obviously has the right to process judicial data in the process of his/her own litigation, the principle does not go as far as permitting in depth investigation, collection and centralisation of personal data by third parties, including in particular, systematic research on a general scale such as the scanning of the Internet (…). Such investigation falls within the competence of judicial authorities'.

34. In an area where freedom of speech, access to information, privacy and other fundamental rights are at stake, this intervention of private actors raises the question of the proportionality of the means used. The European Parliament has recently adopted a resolution stressing the need for a solution in compliance with the fundamental rights of individuals ([5]). In point 23 of its resolution, it states that 'the Internet is a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society; [the Parliament] calls on the Commission and the Member States, to avoid adopting measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access'.

([1]) Impact assessment, point 5.2.
([2]) In that sense, filters would be meant to be initialised by parents, and could be de-activated, so that the adult remains in full control of the filtering effect.
([3]) Recital 8 of the preamble; Annex 1, point 1.4; Summary of the impact assessment, point 3.1.
([4]) Working document of the Article 29 Working Party on data protection issues related to intellectual property rights, WP 104.
([5]) European Parliament resolution of 10 April 2008 on cultural industries in Europe (2007/2153(INI)), point 23.

35. The EDPS considers that a balance has to be found between the legitimate objective to fight against illegal content and the appropriate nature of the means used. He recalls that any action of surveillance of telecommunication networks, where necessary in specific cases, should be the task of law enforcement authorities.

IV. **CONCLUSION**

36. The EDPS supports the proposal for a multiannual programme to protect children using the Internet and other communication technologies. He welcomes the fact that this programme intends to focus on the development of new technologies and on the elaboration of concrete actions to enhance the effectiveness of the protection of children.

37. The EDPS recalls that the protection of personal data is an essential prerequisite to the safety of children online. Misuse of children's personal information must be prevented, using the orientations proposed in the programme, and especially the following:

— ensuring awareness of children and other stakeholders like parents and educators,

— promoting the development of best practice by the industry,

— promoting the development of privacy compliant technological tools,

— favouring the exchange of good practice and practical experience amongst relevant authorities, including data protection authorities.

38. These actions should be developed without overlooking the fact that the protection of children takes place within an environment where the rights of others might be at stake. Any initiative of collecting, blocking or reporting information should only be taken in the respect of the fundamental rights of all individuals involved and in compliance with the data protection legal framework. In particular, the EDPS recalls that the surveillance of telecommunication networks, where necessary in specific circumstances, should be the task of law enforcement authorities.

39. The EDPS notes that this programme constitutes a general framework for further concrete actions. He considers that some observations made in this opinion are a first step and could be developed in a practical way, by reference to the projects still to be put in place, in line with the orientations of the programme. He recommends that data protection authorities be closely involved when it comes to the definition of these practical projects. He also refers to the activities of the Article 29 Working Party on the subject, and in particular to the present work of the Working Party on social networks ([1]).

Done at Brussels, 23 June 2008.

Peter HUSTINX

European Data Protection Supervisor

([1]) See the Working Document 1/2008 of 18 February 2008 on the protection of Children's Personal Data, WP 147, and for a more general view, the work programme 2008-2009 of the Working Party including social networks, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm