LIBE Hearing on combating sexual abuse, sexual exploitation of children and child pornography

Tuesday 28 September 2010

Giovanni Buttarelli

SPEAKING POINTS

Preliminary remarks.

The EDPS appreciates this initiative aimed at strengthening preventive and repressive measures against sexual abuse and sexual exploitation.

This phenomenon does not seem to diminish over time. It is directed against children who are increasingly vulnerable on-line and have a right to special protection and care as is necessary for their wellbeing.

We welcome the establishment of minimum rules concerning the definition of criminal offences and sanctions at Union level, the introduction of new investigation tools, as well as any other robust social response to address new forms of abuse and exploitation using information technologies within the internal and external policies of the EU: the child's best interests must be a primary consideration.

I am not dealing now on either the possible criminalisation of new or lightly punished serious forms of abuse facilitated by the use of Internet and IT technologies (with particular regard to the publication and the

dissemination of child abuse material), or on the recognition of special investigative techniques.

Similarly, the EDPS contribution today does not focus on the validity of evidence, the prohibition from certain activities, the exchange of information to ensure implementation throughout the EU, new rules on jurisdiction, legal remedies or assistance to victims.

Our contribution today will only focus on provisions more directly relevant for the protection of personal data, with particular regard to the blocking of access by Internet users.

Sexual abuse and sexual exploitation of children constitute a serious violation of fundamental rights. However, there are other rights to consider. This is why we appreciate the intention of the Commission to conduct an in-depth evaluation to ensure that any new legislative measures will be fully compatible, with no grey areas with all other fundamental rights including the freedom of expression and information and the protection of personal data (see recital n. 15 of the proposal).

The questions raised by EDPS do not target the fight against child abuse as such, but they address more generally all initiatives which have an impact on the role of the private sector in a law enforcement context.

With regard to the restriction of access to child pornography on the internet, the EDPS does not question the need to put in place a better framework providing for adequate measures to reduce the circulation of child abuse material, making it more difficult for offenders to upload such content onto the publicly available web through increased cooperation with third countries and international organizations.

However, some of the measures envisaged in the proposal, such as the removal and the blocking of websites and the setting-up of hotlines, have a serious impact on the fundamental rights to privacy and data protection of the different individuals involved.

The data protection issues 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.

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

With regard to the 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) the EDPS could support actions taken by police or judicial authorities in a well defined legal framework, with full respect of the ECHR jurisprudence and of the constitutional traditions common to the member States, with particular regard to the freedom of communication and the jurisdictional guarantees provided by constitutional charters.

The EDPS has strong doubts about the legal certainty of any blocking operated by private parties, also given the possible monitoring of the Internet which could lead to such blocking.

Indeed, blocking may imply different monitoring activities, including scanning the Internet, identifying unlawful or suspect websites and blocking access to end users, but also monitoring on-line behaviour of end-users who are trying to access or download such content.

The proposal of the Commission does not entrust ISPs with monitoring activities but with blocking. However, if ISPs are told to block websites it is difficult to see how they would do this without at least some monitoring of users. And this is something new compared to the Council of Europe Convention 201/2007.

The tools to be used are different: for instance, DNS blocking, IP addresses blocking or ´deep packet inspections´ on a trial basis. They imply different degrees of invasiveness and sometimes getting knowledge of the content of telecommunications while they are transferred, but all give rise to similar questions as to the role of Internet Service Providers with regard to the processing of content information.

These surveillance activities have consequences in terms of data protection, since the 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 parties (*e.g.* ISPs or copyright holders), in areas that are in principle under the competence of law enforcement authorities.

Three major concerns:

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.

It would be important to better verify whether blocking sites will be in future an efficient measure or a useless and costly measure that can be easily by-passed. But, what are the criteria for blocking? A code of conduct or voluntary guidelines would not bring enough legal certainty in this respect.

Risks linked with possible blacklisting of individuals and their possibilities of redress before an independent authority.

The EDPS has already stated on 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*".

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. The reference of Article 21 of the proposal to "*adequate safeguards"* is a first base for further analysis.

So we do not say there can be no control, just that it must be <u>strictly framed</u>.

We appreciate that the European Parliament has adopted in another context (intellectual property rights) a written declaration supporting the same view:

"*The European Parliament;*
(...) Takes the view that internet service providers should not bear liability for the data they transmit or host through their services to an extent that would necessitate prior surveillance or filtering of such data; (...)"

The setting-up of a network of hotlines.

A network of hotlines is mentioned in recital 13 of the proposal - not in the text itself: this network is not developed in the proposal as such but is mentioned in a previous document, the Safer Internet Programme, on which the EDPS has already issued an opinion.

The EDPS commented on the conditions under 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.

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, and also information on the person reporting suspicious content or the victim of the abuse. The rights of all these individuals should be taken into account in compliance with the existing data protection framework.

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.

We also plead for guarantees related to the supervision of the system, in principle by law enforcement authorities, transparency and independent redress possibilities.

In conclusion, there is:

- a need to ensure legal certainty with regard to all parties involved, including Internet Service Providers and individuals using the network, with a clear legal and judicial framework;

- a need for an obligation on Member States to ensure harmonised, clear and detailed procedures when combating illegal content, under the supervision of independent public authorities.