EUROPEAN DATA PROTECTION SUPERVISOR

Executive Summary of the Opinion of the European Data Protection Supervisor on the dissemination and use of intrusive surveillance technologies

(The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2016/C 79/04)

The EDPS addresses in this Opinion the data protection and privacy issues raised by the dissemination and use of intrusive surveillance technologies. The use of these tools implies by default the processing of personal data and a possible intrusion of privacy: the main goal of intrusive surveillance tools is to remotely infiltrate IT systems (usually over the internet) in order to covertly monitor the activities of those IT systems and over time, send data back to the user of the surveillance tools.

While such tools can be instruments for legitimate (and regulated) use by law enforcement bodies or intelligence agencies, they can be also used as 'Trojan horses' to circumvent security measures in electronic communications and data processing.

The tension between the positive use of ICT tools and the negative impact that the misuse of technology can have on human rights, and especially on the protection of personal data and privacy, has to be addressed by national and EU policies, and by all actors involved in the ICT sector (developers, service providers, sellers, brokers, distributors, and users).

In this Opinion, the EDPS proposes to address the threat constituted by the use of intrusive surveillance technologies with the following actions:

— an assessment of the existing EU standards for ICTs should be performed, with the purpose to increase the protection of human rights, especially in case of exportation of surveillance or interception technology and related services,

— the use and dissemination (including inside the EU) of surveillance and interception tools, and related services, should be subject to appropriate regulation, taking into account the potential risk for the violation of fundamental rights, in particular the rights of privacy and data protection,

— consistent and more effective policies should be developed by the Council of the EU, the European Parliament, the European Commission and the EEAS regarding the export of intrusive surveillance tools in the context of dual-use technologies, at EU and international level,

— up-to-date policies should regulate '0-day' exploits and vulnerabilities in order to avoid their use for fundamental rights violations,

— EU policies on cybersecurity should take into account the dissemination of interception and surveillance technologies and address specifically this issue within the appropriate legislation,

— investments in security on the internet and initiatives to embed privacy by design in new technological solutions should be fostered,

— a consistent approach should be put into place to grant international protection to whistle-blowers who contribute to revealing violations of human rights through the use of interception and surveillance technologies.

Done at Brussels, 15 December 2015.

Giovanni BUTTARELLI

European Data Protection Supervisor