

Ethics and human rights in the information society.

Round table 4: Security and governance

The Protection of Rights and Freedoms in the Information Society: Personal Data Protection and Privacy Point of View

Joaquín BAYO DELGADO, Deputy EDPS

Introduction

The present contribution aims at briefly presenting (1) the European legal tools on the protection of privacy and personal data and their relevance in the context of the information society; (2) the role of the European Data Protection Supervisor; and (3) some specific issues that may serve as reference or example in the context analyzed by Round Table 4.

1) European legal tools on the protection of privacy and personal data and their relevance in the context of the information society

The European approach to the protection of privacy and personal data has its origins in Article 8 of the ECHR¹ and in Council of Europe Convention n. 108². Those instruments are technologically neutral, therefore, their principles are fully applicable to the information society.

At European Communities level, Directive 95/45/EC³ has the object of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and allow the free flow of personal data between the member States. This piece of legislation sets the basis for protecting the *data subject*⁴ through the recognition of certain rights to him/her, as

¹ European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 . Right to respect for private and family life. *"1 Everyone has the right to respect for his private and family life, his home and his correspondence. 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"*.

² Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

³ 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, Official Journal L 281 , 23/11/1995 P. 0031 - 0050.

⁴ Article 2 of Directive 95/46/EC: *"(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; (...)"*.

well as the creation of obligations to be respected by the *data controller*⁵ (respect of the data quality principle, respect of the criteria for making data processing legitimate, the obligation to provide information to the data subject, the right of access, etc.)

One of the obligations imposed to the data controller is the implementation of "(...) *appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected*"⁶.

This obligation is also stated by Directive 2002/58/EC⁷ (Directive on privacy and electronic communications): "1. *The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. (...). 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved*".

Another characteristic of the European approach is the existence of independent Data Protection Authorities (DPAs). Their main characteristics are the following: they have investigative powers, powers of intervention, powers to engage in legal proceedings, they shall hear claims lodged by any person concerning the protection of his/her rights and freedoms in regard to the processing of personal data, etc.

This legal framework provides for important protective tools. They have proven to be effective, with the limits of geographical application, considering that the on-line world is not "strictly" linked to geography.

2) The role of the European Data Protection Supervisor (EDPS)

The EDPS is a DPA which acts at EU level. The tasks of the EDPS can be classified into three main roles:

⁵ Article 2 of Directive 95/46/EC: "(...); (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; (...)".

⁶ Article 17.1 of Directive 95/46/EC.

⁷ 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), Official Journal L 201 , 31/07/2002 P. 0037 - 0047.

- Supervision:

The supervisory task is to ensure that the EU institutions and bodies process personal data of EU staff and others lawfully. The EDPS oversees Regulation (EC) 45/2001⁸ on data protection, which is based on two main principles (which are in line with Directive 95/46/EC):

1. The data controller needs to respect a number of obligations. For instance, personal data can only be processed for a specific and legitimate reason which must be stated when the data are collected.
2. The data subject enjoys a number of enforceable rights (e.g.: the right to be informed about the processing and the right to correct data).

Every institution or body should have an internal Data Protection Officer. The DPO keeps a register of processing operations and notifies systems with specific risks to the EDPS. The EDPS prior checks whether or not those systems comply with data protection requirements. The EDPS also deals with complaints and conducts inquiries.

- Consultation:

The EDPS advises the European Commission, the European Parliament and the Council on proposals for new legislation and a wide range of other issues with data protection impact. In essence, the consultative task is to analyse how policies affect the privacy rights of the citizens. This assessment helps to enable proper political discussions on how new legislation can be effective with due respect and adequate safeguards for citizens' freedoms. The advice makes it possible for the legislators in Europe to adopt better legislation that is in line with European values.

- Cooperation:

The EDPS cooperates with other data protection authorities in order to promote consistent data protection throughout Europe. Data protection laws are built on common principles. Moreover, for an increasing number of European databases, supervision is shared between different data protection authorities (such as the Eurodac database). The central platform for cooperation with national supervisory authorities is the Article 29 Working Party.

3) Some specific issues

The EDPS has dealt with certain specific issues in the context of its different roles which are examples of the relevance of the protection of rights and freedoms in the information society.

- Respect of the data quality principle in the digital environment

⁸ 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, Official Journal L 008 , 12/01/2001 P. 0001 - 0022.

The need to respect the data quality principle in the digital environment has been underlined by the EDPS in the context of a Prior Checking case⁹, where it can be read: "[t]his principle is also of relevance in the processing involved in forensic examinations of computers. Regarding seizures in physical premises, the OLAF Manual expresses in point 3.4.4.1 : '[a]ddress books or diaries that are found on the premises may be considered to be used for professional purposes and may be seized if relevant to the goal of the inspection, unless it is clearly indicated that they are used only for private purposes. Wallets, handbags, and obviously private papers should not be seized.' These precautions should also be taken regarding the access to the contents of a computer belonging to a Community institution or body since it may also contain files used by the data subject for private purposes (for instance in the folder 'My documents', or e-mails marked as 'private'), or files not relevant or excessive for the purposes of the investigation. The EDPS welcomes the existence of particular authorization mechanisms to allow the conduction of such computer forensic examinations. Moreover, the EDPS recommends in this regard that whenever the access to files that are apparently of a private nature appears to be necessary for the investigation, this access be conducted respecting adequate guarantees, and considering any potential risk of inadmissibility of the evidence in a possible future criminal case that could arise if the fundamental rights to privacy and personal data protection are not respected in the collection of evidence (see point 2.2.10 below). Furthermore, the EDPS recommends the adoption of a formal Protocol of 'Standard Operating Procedures' for the conduction of computer forensics investigations by OLAF, which will also contribute to the safeguard of the data quality principle (see point 2.2.10 below)".

- The purpose limitation principle and the use of traffic data

The EDPS has issued an Opinion on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC¹⁰ (the data retention Directive). The EDPS has taken into account that, notwithstanding the importance of the proposal for law enforcement, it may not result in people being deprived of their fundamental right to have their privacy protected. The EDPS envisaged a balanced approach, in which the necessity and the proportionality of the interference with data protection play a central role. Therefore, several recommendations have been made in order to foster the protection of personal data (e.g. limitation of data retention periods, limitation of number of data to be stored, limitation of the purpose of processing to "certain serious criminal offences", etc).

⁹ Opinion on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations, Brussels, 23 June 2006 (Case 2005-418), available at:

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2006/06-06-23_OLAF_internal_investigations_EN.pdf

¹⁰ EDPS' Opinion is available at:

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_EN.pdf

Indeed, respect of the purpose limitation principle is at the core of case C-275/06 (*Promusicae v Telefónica de España*) being handled by the European Court of Justice (ECJ). On 18 July 2007 Advocate General Kokott submitted her Opinion.¹¹ The case was brought before a Spanish Court by Promusicae, a music and audiovisual association, after telecoms and internet provider Telefónica refused to hand over names and addresses linked to computers that were used in alleged copyright infringement. Promusicae wants to pursue civil actions against the users, but Telefónica insists they are only obliged to turn over this information as part of criminal investigations, for public security or national defence. The referring national judge has submitted a preliminary question to the ECJ on whether excluding disclosure of this information in civil litigation is compatible with European law generally.

The Advocate General concluded that refusing access to information on internet users in civil cases involving intellectual property rights violations is compatible with European law, specifically considering the ePrivacy Directive 2002/58/EC. This opinion follows similar arguments to those previously expounded by the Article 29 Working Party, such as the 2005 paper on data protection issues related to intellectual property rights¹².

The Advocate General's Opinion is well developed advice to the ECJ about the limits on the purposes and uses to which internet traffic data can be put, with an understanding of the notion and application of the proportionality principle when conflicting rights are involved.

4) Concluding remarks

The protection of privacy and personal data in the context of the information society can only be guaranteed through the adoption of sufficient legal safeguards. Security measures are a key factor in order to achieve sufficient protection. Nevertheless, security measures may be void without clear rights and obligations recognised and imposed respectively to the different actors.

Reaching a high level of protection must be a goal in the global arena to ensure a sustainable information society. Data Protection Authorities have an important role to play in guaranteeing the correct implementation of the legal framework. This role is to be exercised both *ex-ante* (through the use of preventive mechanisms, such as prior-checking controls, inspections, etc.), and *ex-post* (for instance, through the application of sanctions when the failure to comply with the obligations imposed has been proved).

The involvement of the different stakeholders of the policy dialogue is an important factor for success. The draft Code of Ethics is a relevant step in awareness raising. However, it has to be borne in mind that fundamental rights have to be protected

¹¹ Advocate General Kokott's Opinion is available at: <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&Submit=Rechercher&alldocs=alldocs&docj=docj&docop=docop&docor=docor&docjo=docjo&numaff=C-275/06&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100>

¹² http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf

through enforceable and binding instruments. Therefore, it is expected that work continue to be done in order to reach consensus for achieving such aim.