Maria Eduarda Gonçalves and Inês Andrade Jesus*

Security and Personal Data Protection in the European Union: Challenging Trends from a Human Rights' Perspective

Abstract

The protection of personal data was first addressed in the European Community by Directive 95/46/CE. This Directive sought to reconcile personal data protection with the free movement of information in the Internal Market. The processing of personal data in the areas of security policy and police and judicial cooperation was excluded from the Directive's scope of application. However, in recent times, furthered by the "war on terror", security policies have been reinforced in the European Union (EU), a key feature of these policies being the increased collection, use and exchange of information about individuals. Major electronic databases were set up. Additional measures such as the Data Retention Directive and agreements with the USA on Passenger Name Records (PNR) have also raised concerns about their bearing on fundamental rights and liberties. Remarkably though, the legal framework for the protection of personal data in the field of security is still recognisably unsatisfactory. This gap is currently in the process of being filled by way of legislative initiatives of the European Commission, submitted in January 2012.

---

* The authors are members of the Centre for Socioeconomic and Territorial Studies (DINAMIA'CET) ISCTE – Lisbon University Institute; mebg@iscte.pt, ioajs@iscte.pt. This article has been prepared as part of a research project, "Protecting privacy and personal data in a post-Charter Europe" (2011/2013), funded by the Foundation for Science and Technology, Portugal. This project is being carried out under a partnership between DINÂMIA'CET and the Faculty of Law of the New University of Lisbon (CEDIS – Research Centre for Law and Society).

Nevertheless the question remains, how the balancing between security and the right to personal data protection is being construed by the EU. This issue was rendered more acute following the upgrading of personal data protection to the status of a fundamental right by the EU Charter of Fundamental Rights. In this paper, we will seek to address this topic based on a critical consideration of the evolution and current state of legal protection of personal data in the EU.

Keywords: Security, Data Protection, European Union, Fundamental Rights, Balancing Rights

A Introduction

In recent times the world has witnessed dramatic changes in the ways data about individuals and individuals' life are accessed, processed and exchanged. Personal data are a major asset of the information economy. The amount and variety of personal information in public administrations' electronic databases are also escalating, including for law enforcement purposes. Despite the growing penchant of individuals to public exposure in social media, perhaps denoting a new perception of privacy, people are increasingly aware of the risks associated with massive collection, storage and exchange of personal data. Potential threats range from identity theft to discrimination, unwanted marketing to feelings of fear and distrust in institutions. Hence the legal protection of personal data became a key issue in the networked economy and society, ultimately a condition for human security in the contemporary world.

In this context, different interests and values conflict and clash, particularly those of public and private organisations in the more efficient handling of their services and activities by the means of data computerisation and exchange, as unrestricted as possible; and those of individuals toward the safeguard of their personal data and, ultimately, their privacy and

intimacy. In the EU this tension was first addressed by Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).[1]

This Directive was adopted under the Internal Market provisions of European law. The processing of personal data in the areas of the common foreign and security policy and police and judicial cooperation, as well as public security, defense, state security and criminal law has been explicitly excluded from the Data Protection Directive's scope of application.[2]

Thereinafter, under the Area of Freedom, Security and Justice launched by the Treaty of Amsterdam in 1997, and of so-called "war on terror", EU security policies were progressively tightened; a central feature of these policies being the increased collection, use and exchange of information. Major databases containing data on individuals were set up, raising concerns about their bearing on fundamental rights. Remarkably though, the potential conflict between the requirements of EU internal and external security policies, on the one hand, and the protection of personal data, on the other hand, still lacks a legal basis equivalent to Directive 95/46/EC. This gap is currently in the process of being filled by way of legislative initiatives of the European Commission (Commission), submitted in January 2012.

Nevertheless the question remains, how the balancing between security and the right to personal data protection is being construed by the EU. This issue was

---

1 European Parliament and the Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

2 European Parliament and the Council, Directive 95/46/EC, Article 3.

rendered more acute following the upgrading of personal data protection to the status of a fundamental human right in the EU Charter of Fundamental Rights. In this paper, we will seek to address this topic based on a critical consideration of the evolution and current state of legal protection of personal data in the EU.

We will start by reviewing and comparing major trends in data protection regimes in the EU, particularly in the Internal Market and in the Area of Freedom, Security and Justice. We will then discuss the EU institutions' tendency to present stronger security measures, including reinforced information systems, on the one hand, and civil liberties and rights, on the other hand, as mutually reinforcing; and in this way undermining the truly detrimental impact on human rights of the increasing use of personal data for security purposes.

Bearing in mind that the right to the protection of personal data has been raised recently to the status of a fundamental right in the EU, we will inquire whether this development appears to matter, in the end, for duly protecting individuals.

Considering the contents of the latest proposals of the Commission for reforming the EU data protection regimes, we conclude that the adoption of the fundamental right to personal data protection has not been by itself sufficient to assure a data protection regime that resists a great deal of criticism.

B From the Internal Market to the Area of Freedom, Security and Justice: Trends in Data Protection Regimes in the EU

Data protection regimes, like the Data Protection Directive, generally rely on certain basic principles to be observed by the data controllers and processors. In particular these

are: purpose limitation – personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes; consent of the data subject to personal data relating to him being processed; data minimization – processing of personal data must be restricted to the minimum amount necessary; proportionality – personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected; and control – supervision of processing must be ensured by member states' authorities. Also, the data subjects are assigned a set of procedural rights, enabling them to consent, to have access, and to know what information about them is registered in databases, to rectify the data, and to object to data processing in certain situations. Moreover, the Data Protection Directive prohibits transfer of personal data to third countries unless the latter provide an adequate level of data protection as determined by the Commission, or unless one of the enumerated exceptions applies. In this way, the Data Protection Directive sought to reconcile personal data protection, regarded as a minimum level of protection throughout the European Community, with the free movement of information in the interest of the internal market economy.

Actually, the Data Protection Directive represents a change in the balancing of the rights of the individual vis-à-vis the interests of data controllers and processors if compared with its predecessor, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of 1981 (Convention 108). Indeed, the Data Protection Directive contains a catalogue of exceptions, not found in Convention 108, to the data protection principles. That is in particular the principle of consent of the individual for their personal data to be collected and processed,

admitting implicit consent in defined circumstances (Article 7). Still, the Data Protection Directive has been commonly regarded as a balanced, adequate framework, duly followed by effective supervising work by data protection authorities across Europe. Paul De Hert and Vagelis Papakonstantinou maintain, "*in practice, the Directive has by now become the international data protection metric against which data protection adequacy is measured*"[3].

This Directive 95/46/EC was adopted under the Internal Market provisions of the Treaty. The processing of personal data in the areas of the common foreign and security policy and police and judicial cooperation, as well as public security, defense, state security and criminal law has been explicitly excluded from the Data Protection Directive's scope of application, at a time when these areas remained under member states' jurisdiction.[4] However, from the nineties onwards, the launching of the EU Area of Freedom, Security and Justice and the subsequent reinforcement of EU policies against crime and terror that followed the terrorist attacks of New York 2001, Madrid 2004, and London 2005, entailed growing investment in information systems as well as in police cooperation and border control. As a result, new computerized databases containing personal data were set up, namely Eurodac and VIS, demanding an appropriate legal framework. Eurodac, a database for

---

3 De Hert, Paul and Vagelis Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals*, Computer Law & Security Review (Volume 28), 2012, pp. 130-142, at p. 131. See also Hijmans, Hielke and Alfonso Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, Common Market Law Review (Volume 46), 2009, pp. 1485-1525, at p. 1489.

4 European Parliament and the Council, Directive 95/46/EC, Article 3.

comparing fingerprints of asylum seekers, and VIS, the Visa Information System, were established in 2000 and 2008, and entered into operation in 2003 and 2011, respectively. These systems complemented SIS, the Schengen Information System, established in 1990, and into force since 1995. But, despite widespread concerns with the potentially adverse effects of these developments on fundamental rights, Council Framework Decision 2008/977/JHA[5] has been and remains today the unique broad legal basis for the protection of personal data in the framework of police and judicial cooperation in criminal matters, and one that has been generally acknowledged as unsatisfactory both formally and substantially.

First of all, Council Framework Decision 2008/977/JHA only applies to personal data processed in the framework of European police and judicial cooperation, leaving apart data processing at the member states level. Besides, despite the Decision's accent on the need to "*fully respecting fundamental rights of individuals*" (Preamble paragraph 5), data protection is limited by a substantial amount of exceptions to the data protection principles and rights. An example concerns the purpose limitation principle. According to Article 11 Council Framework Decision 2008/977/JHA, personal data may be processed for other purposes than those for which they were transmitted or made available for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; for the prevention of an immediate and serious threat to public security; or any other purpose, with the prior consent of the transmitting member state *or* the consent of the data subject. An

[5] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27 November 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:EN:PDF.

additional exception is admitted to the principle of data subjects' consent, in the name of the efficiency of law enforcement's cooperation *"where the nature of a threat to the public security of a member state or a third state is so immediate as to render it impossible to obtain prior consent in good time*". In this case, "*the competent authority should be able to transfer the relevant personal data to the third state concerned without such prior consent*" (Preamble paragraph 25). Though the principles of lawfulness, proportionality and purpose are explicitly affirmed (Article 3, N° 1), "*further processing* for another purpose*shall be permitted in so far as: (a) it is not incompatible with the purposes for which the data were collected; (b) the competent authorities are authorized to process such data for such other purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose*" (Article 3, N° 2).[6] Moreover, "*appropriate time limits" shall be established for erasure and review of the need for the storage of the data*" (Article 5).

A considerable margin of discretion is therefore left to the competent authorities to define the scope of the exceptions to the data protection principles and the obligations of the data controllers, as well as the meaning of what are "appropriate" time limits of storage.

At the end of the day, the main principle guiding the exchange of personal data among police and judicial authorities is "the principle of availability of information" meaning that authorities responsible for internal security in one member state or Europol officials who need information to perform their duties should obtain it from another member state if it is accessible there.[7]

---

6 Emphasis added.

7 European Commission, Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in

Remarkably, the Commission itself acknowledged the shortcomings of this regime:

"*The processing of data by police and judicial authorities in criminal matters is currently principally covered by Framework Decision 2008/977/JHA, which pre-dates the entry into force of the Lisbon Treaty. The Commission has no powers to enforce its rules, as it is a Framework Decision, and this has contributed to uneven implementation. In addition, the scope of the Framework Decision is limited to cross-border processing*."[8]

Likewise, in its 2010 Communication "A comprehensive approach on personal data protection in the European Union", the Commission conceded, Framework Decision 2008/977/JHA contains too wide an exception on the purpose limitation principle.[9] The Commission further admitted that this and other weaknesses may directly affect the possibilities for individuals to exercise their data protection rights, e. g. to know what personal data are processed and exchanged

---

the area of JHA, COM (2005), 597 final, 24 November 2005, at p. 3, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF.

8 European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*, COM (2012) 9 final, 25 January 2012, at p. 9. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF.

9 European Commission, Communication on *A comprehensive approach to the protection of personal data in the European Union*, COM (2010) 609 final. 2010. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

about them, by whom and for what purpose, and on how to exercise their rights.[10]

Such a recognizably insufficient scenario from the standpoint of the safeguard of personal data used for security purposes is made more serious in view of other legislative measures taken by the EU in recent years prompting even larger apprehension with EU "securitarian trends", particularly:

a. The adoption, under pressure from USA's authorities following 9/11, of Council Regulation (EC) Nº 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member states, amended in 2009.[11] The "biometric passport" has raised concern for its bearing on people's intimate features as well as autonomy since with biometrics the human body is being modeled and digitalized and turned into an instrument under control.

b. The successive PNR agreements with the USA obliging European air travel companies to transmit to Homeland Security authorities in the US several data about individuals travelling to this country.[12]

---

10 European Commission, COM (2010) 609 final, at p. 14.

11 European Parliament and the Council, Regulation (EC) Nº 444/2009, amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member states, 28 May 2009. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF.

12 Council of the European Union (EU), Council Decision 2007/551/CFSP/JHA on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of

This agreement is in the process of being revoked and replaced by another just approved by the Civil Liberties Committee of the European Parliament (March 2012). Back in December 2011, the European Data Protection Supervisor (EDPS) considered that: "*Any legitimate agreement providing for the massive transfer of passengers' personal data to third countries must fulfil strict conditions. Unfortunately, many concerns expressed by the EDPS and the member states' data protection authorities have not been met*."

c. Directive 2006/24/EC (Data Retention Directive) imposing strengthened obligations on telecommunications operators to collect and store data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.[13]

Directive 2006/24/EC aimed to harmonize rules on data retention across member states in order to ensure the availability of traffic data for anti-terrorism purposes, in case of investigation, detection and prosecution of this crime. Operators are obliged to retain a wide range of data

Homeland Security (DHS) (2007 PNR Agreement), 23 July 2007. Available online at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00160017.pdf.

13 European Parliament and the Council, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15 March 2006. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

between 6 and 24 months from the date of communication, and provide to the competent national authorities without undue delay, if requested, incoming and outgoing phone numbers fixed and mobile, the duration of phone calls, IP address, log-in and log-off times and e-mail activity details. In fact, the Directive is an illustration of a wider trend, also manifested in the PNR agreements, to preventively store personal data of all costumers. Unsurprisingly, to the question: "*What should we expect from the future?*" Stefano Rodotà answered "*there are reasons for pessimism*". And, the author adds, "*The fundamental right to data protection is continuously eroded or downright overridden by alleging the prevailing interests of security and market logic*."[14].

Personal data are more and more recorded, exchanged and retrieved at a European scale involving police and security systems as well as private entities such as telecommunications operators and aircraft companies. Not only is there more information available about individuals, but new techniques are also being developed to use data and information in increasingly sophisticated ways. Searching techniques such as data mining allowing information to be collected amid huge amounts of data, and methods for assessing risk of specific individuals based on profiling associated with stereotypes like race and religion are increasingly being employed.[15]

---

[14] Rodotà, Stefano, *Data Protection As Fundamental Right*, in: Gutwirth, Serge, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection*, Springer, The Netherlands, 2009, at p. 77 and p. 80.

[15] Hijmans and Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, at p. 1491.

C Balancing Security and the Rights to Data Protection and to Privacy

One might notice that, notwithstanding the wide recognition of the strains imposed by EU security policies upon data protection principles and rights, EU institutions' discourse has often taken a conciliatory stance. It appears to presume that stronger security measures, including reinforced information systems, on the one hand, and civil liberties and rights, on the other hand, can be easily well-adjusted.[16] This view has been underlined in several EU policy documents: instead of a "zero sum game", the official description points to a "win-win" situation.[17] The argument has been built around the idea that security measures can be instrumental in guaranteeing privacy (e. g. when employed to control access through fingerprint or other recognition technique), countering the idea of "more security, less privacy".[18]

Decision No. 1982/2006/EC of 18 December 2006 approving the 7th Framework Programme on Research

---

16 Goold, Ben and Liora Lazarus, *Introduction: Security And Human Rights*, in: Goold, Ben and Liora Lazarus (eds.), *Security And Human Rights*, Hart Publishing, Oxford, 2007, pp. 1-24. See also Liberatore, Angela, *Balancing Security And Democracy, And The Role Of Expertise: Biometrics Politics In The European Union*, European Journal on Criminal Policy and Research (Volume13, Issue 1-2), 2007, pp. 109-137, at p. 114.

17 Robinson, Neil, Hans Graux, Maarten Botterman and Lorenzo Valeri, *Review Of The European Data Protection Directive*, Rand Europe, Brussels, 2009, at p. 16. Available online at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf.

18 Hornung, Gerrit, *The European Regulation On Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework And Technical Safeguards*, SCRIPT-ed (Volume 4, Issue 3), 2007, pp. 246-262, at p. 249. Available online at: http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.pdf.

and Development follows this line of reasoning, too. It states that "*security in Europe is a precondition of prosperity and freedom*."[19] Referring to information technology systems generally, the Commission also acknowledged that "[they] *can serve to protect and amplify the fundamental rights of the individual*".[20] In this way, European institutions ultimately defend the role they play in security as one of promoting human rights. These understandings are reminiscent of the theoretical approaches that do not consider rights and policies to be exclusive of one another, the former concerning the individual and the latter society, but see them as living in harmony.[21]

The conciliatory rhetoric also pervades the Commission proposals, presented on the 25 January 2012, aiming "*to build a modern, strong, consistent and comprehensive data protection framework for the European Union*".[22] In the Commission's own terms, this

19 European Parliament and of the Council, Decision No 1982/2006/EC concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013), 18 December 2006. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:412:0001:0041:EN:PDF.

20 European Commission, COM (2010) 609 final, at p. 2.

21 Dworkin, Ronald, *Sovereign Virtue, The Theory and Practice of Equality*, Harvard University Press, Cambridge, 2002, at p. 23; Raz, Joseph, *Rights and Politics*, in: Tasioulas, John (ed.), *Law, Values And Social Practices*, Aldershot, Dartmouth, 1997, at p. 89.

22 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, 25 January 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF; European Commission, Proposal for a Directive of

reform will first of all "*benefit individuals by strengthening their data protection rights*".[23] But, the Commission also purports to "*simplify the regulatory environment*" for businesses "*by drastically cutting red tape and doing away with formalities such as general notification requirements*".[24] Additionally, growing trust among law enforcement authorities is also sought "*to facilitate exchanges of data between them and cooperation in the fight against serious crime* […] *while ensuring a high level of protection for individuals*".[25]

Yet, beyond this pacifying discourse, what one really witnesses is, in our opinion, a determined move by the EU to foster the use of personal data for the sake of security with clear detrimental effects on the effectiveness of personal data protection principles and rights. As a matter of fact, the Commission has consistently shown its determination to improve the "*effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*".[26] "*Security in the EU*", the Commission underscored, "*depends on effective mechanisms for exchanging information between national authorities and other European players*."[27] Apprehensive

the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, 25 January 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

23 European Commission, COM (2012) 11 final, at p. 8.

24 European Commission, COM (2012) 11 final, at p. 12.

25 European Commission, COM (2012) 11 final, at p. 8.

26 European Commission, COM (2005) 597 final.

27 European Commission, Communication to the European Parliament and the Council, *An area of freedom, security and justice serving the citizen*, COM (2009) 262 final, 10 June 2009, at p. 15.

with the "under-exploitation of existing systems", the Commission has vigorously promoted extensive access by police and security services to information systems, for instance, by asylum and immigration authorities to VIS and SIS: "*In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for SIS II immigration and Eurodac data*."[28]

A parallel trend can be noticed for continually broader categories of personal data to be included in these databases. From SIS I to SIS II (planned to start in 2013) digital prints and photographs, as well as biometrical data will be added to the system. Legal instruments facilitating the access to and exchange of information became a priority for the EU legislature.[29]

Concerns in respect of these developments have been voiced within the EU itself. Referring to the Commission proposal for a new legislation on requesting comparisons with Eurodac data by member states' law enforcement authorities and EUROPOL,[30] the EDPS did

---

28 European Commission, Proposal for a Council Decision on requesting comparisons with EURODAC data by member states' law enforcement authorities and Europol for law enforcement purposes, COM (2009) 344 final, 10 Setember 2009.

29 Hijmans and Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, at p. 1487.

30 European Data Protection Supervisor (EDPS), Opinion on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) (establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the member states by a third-country national or a stateless person), and on the proposal for a Council Decision on

not conceal its uneasiness. Eurodac database was set up to identify asylum-seekers rather than to allow police to search for criminals. The Commission put forward this proposal following a request from member states, led by Germany, to allow their law enforcement authorities and Europol access to the Eurodac database to help investigations into terrorism and other serious crimes. For the EDPS, the proposal not only fits in the general trend to grant law enforcement authorities access to several large-scale information and identification systems. It also constitutes a further step in a tendency towards giving law enforcement authorities access to data of individuals who in principle are not suspected of committing any crime.[31] Moreover, it concerns data that have been collected for purposes that are not related to the combat of crime. Rather, the EDPS stressed, to be valid, the necessity of the intrusion must be supported by clear and undeniable elements, and the proportionality of the processing must be demonstrated:

"*The systematic storage of the fingerprints of asylum seekers who have not been related to any crime in the same database with other fingerprints collected by law enforcement authorities — of asylum seekers and/or other persons suspected of crime or convicted — raises in itself serious concerns as to the purpose limitation principle and the legitimacy of data processing*."[32]

This is all the more required, the EDPS added, in case of an extensive intrusion in the rights of individuals

requesting comparisons with Eurodac data by member states' law enforcement authorities and Europol for law enforcement purposes (2010/C 92/01), 10 April 2010.

31 EDPS, Opinion 2010/C 92/01, at p. 4.

32 EDPS, Opinion 2010/C 92/01, at p. 5.

constituting a vulnerable group in need of protection, as foreseen in the proposal.

Remarkably, the EDPS points to the inconsistency between growing personal data gathering, use and transfer, and a political rhetoric where emphasis on human rights appears on the rise:

"*The Commission explicitly deals with the compliance with fundamental rights, inter alia with Article 8 of the EU CFR. It explains that, … in order to ensure that the processing of personal data for law enforcement purposes does not contravene the fundamental right to the protection of personal data, in particular the necessity and the proportionality, the proposal sets out strict conditions.(…) The EDPS is not convinced by this statement of the Commission*."[33]

In the same vein, Rodotà alerted that Directive 2006/24/EC, rather than an exception to general rules, may turn out to be "*an anticipation of the future, the first stage for a deep change of the basic data protection principles*." The logic of reuse and interconnection or multifunctionality, prevails.[34] More than that, these developments occur with "*no real debate or analysis of the necessity or proportionality of measures taken for fighting terrorism and no real evaluation of the balancing vis-à-vis fundamental rights*".[35] It comes, therefore, as no surprise that scholars have baptized the society we live in as a "surveillance society", one that poses new threats for data

33 EDPS, Opinion 2010/C 92/01, at p. 6.

34 Rodotà, Stefano, *La Conservación De Los Datos De Tráfico En Las Comunicaciones Electrónicas*, Revista de Internet, Derecho y Política (Volume 3), 2006, pp. 53-60, at pp. 53-55.

35 Rodotà, *La Conservación De Los Datos De Tráfico En Las Comunicaciones Electrónicas*, at p. 57.

protection and privacy.[36]

Against this backdrop, the question returns whether Article 8 of the EU Charter of Fundamental Rights, elevating the protection of personal data to the status of a fundamental human right, is resulting in a rebalancing of data protection principles and rights vis-à-vis the requirements of security.

D The Fundamental Right to Personal Data Protection: Does it Really Matter for Protecting Data in the Domain of Security?

As indicated, a latest breakthrough in this domain has been the granting of a constitutional standing to personal data protection by Article 8 of the EU Charter of Fundamental Rights, now an integral part of the EU law. Article 8 states that "*Everyone has the right to the protection of personal data concerning him or her*" and that "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*".

The entry into force of the Lisbon Treaty marks a new era for data protection, the EDPS predicted. Article 16 of the Treaty on the Functioning of the EU not only contains an individual right of the data subject, but also provides a direct legal basis for a strong EU-wide data protection law. Furthermore, the abolition of the pillar structure obliges the European Parliament and the Council to provide for data protection in all areas of EU law, allowing for a comprehensive legal framework for data

36 Hijmans and Scirocco, *Shortcomings In EU Data Protection In The Third And The Second Pillars. Can The Lisbon Treaty Be Expected To Help?*, at p. 1487.

protection applicable to the private sector, the public sector in the member states and the EU institutions and bodies.[37]

In the light of such optimistic expectations, one might expect that the European Treaties and the Charter could bring about a reshaping of EU data protection regimes. But is the upgrading of the right to data protection to a constitutional status having any perceivable effect on a rebalancing of the values and interests at stake?

In its recent proposals for a regulation and for a directive in this field[38] the Commission summons Article 8 of the Charter insistently, although signaling that the right to the protection of personal data is not an absolute right, but "*must be considered in relation to its function in society*".[39] Both proposals rely on the balancing discourse referred to above whereby protecting the fundamental rights and freedoms of natural persons and, in particular, their personal data, should not be regarded as incompatible with the growing use of these data either for economic or administrative purposes or for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[40]

The proposed regulation, designed to replace the 1995 Data Protection Directive, is guided by concern for

---

37 EDPS, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, 14 January 2011, at p. 6. See also Blas, Diana Alonso, *First Pillar And Third Pillar: Need For A Common Approach On Data Protection?*, in: Gutwirth, Serge, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, The Netherlands, 2009.

38 European Commission, COM (2005) 597 final.

39 European Commission, COM (2012) 10 final, at p. 6.

40 European Commission, COM (2012) 10 final, at p.2.

more harmonization of the data protection regime across member states and by the will to reinforce the mechanisms for institutional supervision and control.[41] This objective should be accomplished through the establishment of privacy officers in enterprises with more than 250 workers, the obligation to notify data breaches in no more than 24 hours, higher penalties for infringement, and the replacement of the Article 29 Data Protection Working Party, the independent EU Advisory Body on Data Protection and Privacy according to the Data Protection Directive, by a European Data Protection Board. The proposal also adds two novel rights to the existing ones, namely: a right to be forgotten and a right to data portability. The right to be forgotten has been approached as "*nothing more than a way to give (back) to individuals control over their personal data and make the consent regime more effective*"[42]. In these ways, a real reinforcement of data protection principles as well as of data subjects' rights may be achieved. Accordingly, De Hert and Papakonstantinou assent that "[t]*he replacement of the Regulation is an important and far-reaching development; once finalized, the new instrument is expected to affect the way Europeans work and live together*",[43] a "*definite cause for celebration for human rights*."[44]

The same authors, however, admit that the proposal endorses the move toward allowing the processing of personal information for purposes unforeseeable at the

41 European Commission, COM (2012) 11 final.

42 Ausloos, Jeff, *The 'Right To Be Forgotten' – Worth Remembering?,* Computer Law and Security Review (Volume 28), 2012, at p. 143.

43 De Hert and Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals*, at p. 131.

44 Id., at p. 142.

time of data collection, to which evidently no consent has been given by the individuals concerned, thus undermining the principle of purpose specification. Furthermore, the "compatibility" criterion in the draft regulation is of little assistance, because in practice data controllers will be those deciding what is "compatible" or not, leaving it up to individuals the difficult task of taking action to challenge such decisions.[45]

Reservations are much stronger, however, with respect to the proposed Directive on the Protection of Individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

First of all, the choice of a separate instrument to regulate the processing of personal data in the police and judicial sectors has not been uncontroversial. The Commission indeed had two law-making options at hand while amending the EU Data Protection Framework: either to replace both the Directive and the Framework Decision with a single instrument or to amend each one of these. By choosing the second approach, the Commission gave rise to several criticisms. The EDPS argued that police and justice should be included in a single general EU legal instrument, preferably a regulation. A single instrument would give more guarantees to citizens, render the task of police authorities easier, as well as enabling data protection authorities the same extensive and harmonized powers vis-à-vis police and judicial authorities as they have regarding other data controllers.[46] "*In the area of data protection a Regulation is all the more justified, since*

45 Id., at p. 135.

46 EDPS, *A comprehensive approach on personal data protection in the European Union*, at pp. 11-26.

Article 16 TFEU has upgraded the right to the protection of personal data to the Treaty level and envisages – or even mandates – a uniform level of protection of individual throughout the EU."[47] A fundamental right to personal data protection should be meant as to protect citizens under all circumstances, the EDPS underlined. Moreover, the distinction between general and commercial data protection, on the one hand, and security-related personal data processing, on the other, is elusive. This is because datasets are increasingly created by private data controllers for their own purposes and may be accessed at some future point by law enforcement agencies. "*By insisting on two separate instruments for each type of processing, the Commission risks to prolong ambiguity in the field each time law enforcement agencies and the private sector interact*."[48]

With that option, the Commission eventually contradicted the comprehensive approach of its Communication, which paved the way for this reform. The Commission itself had stressed the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies, including law enforcement and crime prevention as well as in international relations.[49]

---

47 EDPS, *A comprehensive approach on personal data protection in the European Union*, at p. 9.

48 De Hert and Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals*, at p. 132.

49 European Commission, Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme, 20 April 2010, COM (2010) 171 final, p. 3. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF.

The projected Directive employs a rather permissive language in many of its provisions, directing member states to apply data protection principles in "*as far as possible*" or to provide that "*all reasonable steps*" are taken by controllers to comply with data subjects' rights (see, for instance, Articles 5, 6 and 10). While some of the recommendations advanced by the EDPS, for instance, for distinguishing between various categories of data subjects (criminal suspects, victims, witnesses etc.) have been incorporated in the draft directive, others have not been envisaged, including for specific conditions and safeguards to be foreseen for the processing of data of non-suspects or for specific safeguards to be devised in relation to the (increasingly relevant) processing of biometric in the field of law enforcement.

Of course, defending the data subject's fundamental right to data protection does not imply that data protection should always prevail over other important interests in a democratic society. Yet, it should have consequences for the nature and scope of the protection that must be given, so as to ensure that data protection requirements are always adequately taken into account, making it feasible for individuals to exercise their rights in practice, with limitations to the exercise of the right taken as exceptional, duly justified and never affecting the essential elements of the right.

In this light, the proposal for a directive also raises misgivings as to the balance reached. In contrast with the proposal for a regulation, the proposal for a directive contains a specific provision on the limitations of the right of access (Article 13, proposal for a regulation) admitting the adoption by member states of legislative measures restricting, wholly or partly, the data subject's rights. Besides, the principle of transparency in personal data processing, affirmed in the proposal for a regulation, has

been excluded from the proposal for a directive (Article 5, a)).

According to the Charter, any restriction to fundamental freedoms and rights must be necessary and proportional in view of the goals pursued, namely fighting crime and terrorism (Article 52, Charter of Fundamental Rights). The EDPS admitted that limitations to the rights of data subjects may be foreseen, but they have to be necessary, proportionate and not alter the essential elements of the right itself. In addition, specific safeguards needed to be put in place, in order to compensate the data subject by giving him additional protection in an area where the processing of personal data may be more intrusive.[50]

The latest developments concerning the transfer of PNRs to other countries for security purposes have not gone without controversy, too.[51]Article 29 Data Protection Working Party and the EDPS considered these measures non-proportional since a great number of personal data are collected on all passengers regardless of the fact that they are under suspicion; and no statistical or other data were available to demonstrate their necessity.[52] The

---

50 EDPS, *A comprehensive approach on personal data protection in the European Union*, at p. 17.

51 Council of the European Union, Council Decision 2007/551/CFSP/JHA.

52 Article 29 Data Protection Working Party, Opinion 10/2011 on the proposal of a directive of the European Parliament and the Council concerning the use of PNR for the purposes of prevention, detection, investigation and repression of terrorist and criminal acts, 2011. Available online at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf; EDPS, Opinion on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Brussels (2012/C 35/03), 9 December 2011. Available online at: http://eur-

simple argument of necessity and of general acceptance of PNR for combatting terrorism and serious crime, put forward by the Commission, was disallowed as insufficient to demonstrate the necessity of what was being proposed.[53] Other available means should have been explored preferably with less intrusive effects for *bona fide* passengers in order to ensure security in air travelling".[54]

To sum up, we may sceptically infer that the inclusion of the right to personal data protection in the EU Charter of Fundamental Rights has not been by itself sufficient to assure a data protection regime that resists criticism.

E Conclusion

Protection of personal data is one of the major legal issues facing present-day information society. Indeed, in the last decade, the reinforcement of security policies alongside the expansion of information systems and databases containing personal data designed for law enforcement and crime prevention caused mounting concerns from the human rights' standpoint. This concern was accentuated in the EU, by the apparent inadequacy of the existing legal basis in addition to the ostensive lack of proportionality as

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:035:0016:0022:EN:PDF.

53 European Commission, Proposal for a Directive of the European Parliament and the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM (2011) 32 final, 2011. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0032:FIN:EN:PDF.

54 Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of PNR data to third countries, 2010.

regards the quantity and the kind of data processed for security purposes, awakening fears about the emergence of a state-controlled surveillance society. Amazingly, the EU institutional discourse has regularly presented security and human rights as if they were the two sides of the same coin. However, this conciliatory approach appears to be contradicted by the ways in which EU security policies have been impacting upon the protection of personal data regimes, giving rise to rather ambiguous feelings.

The recent adoption of the EU Charter of Fundamental Rights, including a fundamental right to the protection of personal data, opened up reasonable expectations for a rebalancing of the requirements of EU security policies vis-à-vis personal data protection principles and rights, and paved the way for the ongoing reform of EU data protection regimes. However, whereas the 2012 Commission's proposal for a new regulation, submitted under the Internal Market provisions of the EU Treaty, is being regarded by some observers as a "*cause for celebration for human rights*"[55], the proposal for a new directive under the EU Area of Freedom, Security and Justice has been received unenthusiastically. Reservations have been voiced, first of all, concerning the two legal instruments option, a regulation and a directive, thought to hamper an uniform, consistent level of protection of individuals throughout the EU, allowing data protection authorities the same extensive and harmonized powers as regards police and judicial authorities as they have for other data controllers. The degree of flexibility permitted by the language of the proposal for a new directive also caused apprehension.

Eventually, expectations opened up by the adoption of Article 8 of the Charter of Fundamental Rights end up unfulfilled to a considerable extent.

---

55 See note 44 above.

The purpose limitation principle and data minimization policies, both in the public and the private sector, and the rights of the data subject need to be more effectively safeguarded if a sounder equilibrium between the important values at issue, and an effective promotion of the fundamental rights are to be achieved in a more and more complex societal and technological environment.