The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters*

Rosanna Belfiore

Contents

Abstract The present paper provides a general overview of Framework Decision 2008/977/JHA on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters, adopted much time after 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—which applies only to activities falling within the scope of the former Community law and does not cover processing operations concerning the activities of the State in areas of criminal law. In line with the original three-pillar construction of the EU, such a frame results in a clear-cut distinction between the protection against data processed for commercial reasons

*This paper was submitted for publication by September 2011. In January 2012 the European Commission has put forward two legislative proposals: a Regulation setting out a general EU framework for data protection and a Directive on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. For obvious reasons, the paper does not take into account these proposals.

R. Belfiore (✉)
Department "Seminario giuridico", University of Catania, Via Gallo No. 24, Catania, Italy
e-mail: rbelfiore@lex.unict.it

S. Ruggeri (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, DOI 10.1007/978-3-642-32012-5_24,

under the former first pillar on the one hand, and the protection against data processed for crime prevention and investigation purposes under the former third pillar on the other. In the light of the entry into force of the Lisbon Treaty, which has removed the pillar structure, the present paper examines the most recent developments towards the adoption of a single legal instrument on personal data protection in the EU, aimed at replacing both the Framework Decision and the Directive.

Abbreviations

CIS	Customs Information System
EDPS	European Data Protection Supervisor
EU FRCh	Charter of Fundamental Rights of the European Union
SIS	Schengen Information System
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union

1 Introduction

As is well known, the main objective of the initial European Community integration project was limited to the creation of an area of free movement of persons, goods, services and capital. Following the foundation of the European Union and the expansion of the scope of the integration project, including the criminal law sector, the idea of free movement has been applied, *mutatis mutandis*, to information,[1] data and judicial decisions within the framework of police and judicial cooperation. The idea of free movement of information in criminal matters is therefore envisaged to favour cooperation between the competent national public authorities for the prevention, investigation and prosecution of criminal offences, leaving individuals mostly unable to escape swifter and faster legal assistance in cross-border cases.

The present paper is focused on the means of protection that have been provided to individuals by Framework Decision 2008/977/JHA[2] against the exchange of personal data processed under the framework of police and judicial cooperation in criminal matters. In the light of Article 7 EU FRCh concerning the right to privacy and Article 8 EU FRCh concerning the right to protection of personal data,[3] and on account of the implementation of the principle of

[1] On the increasing importance of information sharing at EU level, see: Gialuz (2009), 16 ff.

[2] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30 December 2008, p. 60.

[3] On the difference between privacy and data protection, see: Gutwirth and De Hert (2008), pp. 278–293, and Mitsilegas (2009), pp. 276–277.

availability in the area of police and judicial cooperation in criminal matters strongly promoted since the Hague Programme,[4] a measure aiming at the protection of individuals during data exchange for crime prevention purposes was much needed. Indeed, 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[5] does not apply to the processing of personal data in the course of an activity falling outside the scope of the former Community law, nor to processing operations concerning public security, defence, State security or the activities of the State in areas of criminal law [Art. 3(2)].[6]

Thus, in line with the original three-pillar construction of the EU, the result is a clear-cut distinction between protection against data processed for commercial reasons under the former first pillar on the one hand, and the protection against data processed for crime prevention and investigation purposes under the former third pillar on the other. However, after the adoption of the Lisbon Treaty, which has removed the pillar structure, and because of the shortcomings of Framework Decision 2008/977/JHA, the European legislator has planned to adopt a single legal instrument on personal data protection in the EU aimed at replacing both the Directive and the Framework Decision. The present paper briefly examines the most recent developments of such a plan, i.e. the Communication from the Commission of 2010 and the Opinion delivered by the European Data Protection Supervisor in 2011.

2 Framework Decision 2008/977/JHA: Scope of Application

The main objective of Framework Decision 2008/977/JHA, as expressly affirmed under Art. 1, is to ensure a high level of protection of fundamental rights and freedoms of natural persons, in particular the right to privacy, while guaranteeing a high level of public safety. In this respect, processing of personal data in the framework of police and judicial cooperation in criminal matters is emblematic of the conflict between private and public interests in the criminal law sector.

Protection as envisaged by this Framework Decision is limited in scope: it is provided only when personal data are transmitted or made available between Member States, or between Member States and authorities or information systems established under the former EU and EC Treaties [Art. 1(2)]. In principle, this

[4] The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, OJ C 53, 3 March 2005, p. 1. On the principle of availability, see: Ciampi (2009), pp. 34 ff.

[5] OJ L 281, 23 November 1995, p. 31.

[6] After Article 286 EC Treaty concerning data protection was introduced by the Treaty of Amsterdam, Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies (this processing being left outside by the scope of application of Directive 95/46) has been adopted. Directive 95/46 has been further complemented by Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31 July 2002, p. 37).

means that Member States are bound by the standard set forth in the Framework Decision only when they process data among themselves, not at the domestic level. In practice, however, this standard of data protection should be ensured at the national level as well: Member States are not precluded from providing higher standards of protection for personal data collected or processed at the national level, i.e. the Framework Decision is a floor, which should not allow lower standards [Article 1(5)].[7] But there is the danger of a double standard depending on the level, national or transnational, where exchange of data takes place. The possibility of a double standard is evident also under Article 12, which provides that, where, under the law of the transmitting Member State, specific processing restrictions apply in specific circumstances to data exchanges between competent authorities within that Member State (i.e. at national level), the transmitting authority must inform the recipient of such restrictions, who in turn must ensure that these processing restrictions are met.

The Framework Decision does not apply to data exchanged as part of existing obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral or multilateral agreements with third countries (point 38 of the *Consideranda*) and is without prejudice to acts adopted on the basis of the then Title VI TEU that contains *ad hoc* data protection provisions (point 39 of *Consideranda*)—this is the case for data exchanges concerning Europol, Eurojust, the SIS and the CIS, as well as Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.[8]

Finally, protection meets its ultimate limitation where there are essential national security interests and specific intelligence activities in the field of national security [Art. 1(4)].

The scope of application of the Framework Decision is not limited by type of personal data being processed. According to Article 2a, "personal data" mean any *information* relating to an identified or identifiable natural person (defined as the "data subject"). The result of such broad definition is the questionable extension of the Framework Decision to "soft data," i.e. data based on uncertain facts or on assumptions and hearsay.[9]

Also the operations performed upon personal data that fall within the definition of "processing" are broadly defined: they consist of collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, whether or not carried out by automatic means (Art. 2b).

[7] As explained in recital 10, the approximation of Member States' laws should not result in any lessening of the data protection they afford but should instead strive for a high level of protection within the Union.

[8] For some critical remarks, see De Hert and Bellanova (2009), p. 6.

[9] De Hert and Papakonstantinou (2009), p. 408.

3 Obligations upon the Competent Authorities

Protection under Framework Decision 2008/977/JHA is afforded not only to rights and remedies that the data subject can exercise against processing of personal data,[10] but also and primarily in the form of obligations that the competent authorities[11] must comply with in the processing of the data. Indeed, Article 3(1) provides that, according to the purpose specification principle (recalling the principle of speciality[12] traditionally envisaged in measures of legal assistance), personal data may be collected only for specified, explicit and legitimate purposes and may be processed only for the same purpose for which data were collected. Furthermore, according to the principles of legality and proportionality, processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected. Unfortunately, the European legislator failed to strictly limit further processing, where most dangers for illegitimate processing occur. Indeed, further processing is permitted as long as: it is not incompatible with the purpose for which the data were collected; the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and processing is necessary and proportionate to that other purpose [Art. 3(2)].[13] These are all open-ended conditions that create a danger of potentially arbitrary processing.[14]

A specific provision is dedicated to special categories of data, such as those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sexuality, which can be processed only when this is strictly necessary and the national law provides adequate safeguards (Art. 6). Although the purpose of this provision is to guarantee a higher level of protection because of the sensitive nature of the data concerned, protection is actually equivalent, if not lessened, in respect of the standard provided

[10] See below, § 5.

[11] All the data protection rules which apply to the competent authorities are also binding on persons working for a competent authority of a Member State and allowed to have access to and process personal data (Art. 21). These rules shall apply to the members and staff of the national supervisory authorities too (Art. 25, para. 4).

[12] As pointed out by De Busser, "[...] the rule of speciality and purpose limitation both have the objective of restricting the use of data to the intended use." However "purpose limitation is [...] weaker [...] in comparison to speciality." De Busser (2007), p. 49 and p. 55.

[13] The purposes other than those for which data can be further processed are listed under Article 11. They are: (a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which data were transmitted or made available; (b) other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; (c) the prevention of an immediate and serious threat to public security; or (d) any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law. This provision is envisaged so as to have a broad scope. On this point see Hijmans and Scirocco (2009), p. 1494.

[14] For some critical comments on this issue see De Hert and Papakonstantinou (2009), p. 411.

for data in general. Indeed, the necessity criterion is nothing more than the proportionality principle already established for any category of data, and the adequacy principle refers to national laws, thereby deferring to national standards of protection, which may vary considerably.

The competent authorities are also responsible for verification of quality of data before they are transmitted or made available (Art. 8). To this end, they must take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available: in particular, the receiving Member State must be able to assess the degree of accuracy,[15] completeness, up-to-dateness and reliability of data transmitted or made available. If it emerges that data are incorrect or have been unlawfully transmitted, they must be corrected (if inaccurate), erased (when they are no longer required for the purpose for which they were collected or further processed) or blocked (if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject), as provided under Article 4. Time limits for the retention of data are to be set by the transmitting authority, and time limits for the erasure of personal data or for a periodic review of the need for the storage of the data must be established by the receiving authority according to its national law (Arts. 5 and 9).

Another verification duty refers to the lawfulness of the data processing. For such verification, all transmissions are to be logged or documented. This may serve also the purpose of self-monitoring and ensuring proper data integrity and security (Art. 10).

A duty of information is imposed on the recipient and the transmitting Member State. First, the recipient—be it a Member State, a third country, an international body or a private party[16]—must, when requested to do so, inform the competent authority which transmitted or made available the personal data about their processing (Art. 15). Second, both the receiving and the transmitting Member States must ensure that the data subject is informed regarding the collection or processing of personal data, in accordance with national law. However, a Member State may ask another Member State not to inform the data subject, if its national law so provides; in this case, the latter Member State may not proceed to do so without the prior consent of the other Member State. Indeed, informing the data subject may jeopardise the activities carried out during the investigation stage.

Member States shall provide that the competent authorities must implement appropriate technical and organizational measures to protect data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, especially where the processing is automated (Art. 22).

[15] The principle of accuracy of data is to be applied taking account of the nature and purpose of the processing concerned. For example, in judicial proceedings data are based on the subjective perception of individuals and in some cases are totally unverifiable. Consequently, the requirement of accuracy cannot apply to the accuracy of a statement but merely to the fact that a specific statement has been made (point 12 of the *Consideranda*).

[16] See below, § 4.

Finally, Member States shall lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted under the Framework Decision (Art. 24).

4 Transmission to Third States, International Bodies or Private Parties

Article 13 of Framework Decision 2008/977/JHA concerns cases where personal data transmitted or made available by the competent authority of a Member State are transferred to third States or international bodies by the receiving Member State. Transfer is possible only if: (a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; (b) the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; (c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and (d) the third State or international body concerned ensures an adequate level of protection for the intended data processing. While the conditions under (a), (b) and (d) are not decisive in order to provide sufficient safeguards for further transmission of data (the necessity principle is linked to very broad purposes, the competence of the receiving authority in the third State or international body is a preliminary condition for cooperation, and the adequacy principle refers to a standard which is different from the one provided by the Framework Decision and not easily verifiable),[17] the condition under (c) is the ultimate guarantee, as the consent of the Member State from which the data were first obtained allows to liken the further transfer to a direct transmission from the consenting Member State. However, a questionable derogation is permitted where the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State, and prior consent cannot be obtained in good time [Art. 13(2)]. Another derogation concerns the last condition (d), from which departure is

[17] The Framework Decision attempts to explain how the adequacy of the level of protection might be assessed. Particular consideration should be given to: the nature of the data; the purpose and duration of the proposed processing operation or operations; the State of origin and the State or international body of final destination of the data; the rules of law, both general and sector-specific, in force in the third State or international body in question; and the professional rules and security measures which apply [Art. 13(4)]. Nonetheless, the assessment of adequacy remains difficult to carry out. For some critical remarks see: De Busser (2010), pp. 131–133; De Hert and Papakonstantinou (2009), p. 412; and Hijmans and Scirocco (2009), p. 1499. It is noteworthy that recently EU Commissioner Viviane Reding, responsible for Justice, Fundamental Rights and Citizenship, stressed the need to ensure that the principle of reciprocity of protection enjoyed by data subjects applies when data are transferred and processed outside the EU. V. Reding (2011), p. 5.

permitted where the national law of the Member State transferring the data provides for the transfer because of legitimate specific interests of the data subject or legitimate prevailing interests, especially important public interests [Art. 13(3)(a)]. The same condition may be derogated from in cases where the third State or receiving international body provides safeguards deemed adequate by the Member State concerned according to its national law [Art. 13(3)(b)]. This last derogation is obscure, since it does not actually constitute a derogation (the fact that the third State or international body concerned must ensure an adequate level of protection is the rule), and ambiguous, since it is not clear which one is the Member State concerned (the one that first transmits the data or the one that further transfers the data originally transmitted?).

Article 14 of the Framework Decision concerns the transmission to private parties of personal data received from or made available by the competent authority of a Member State. This transmission is possible only if: (a) the competent authority of the Member State from which the data were obtained has consented to transmission in compliance with its national law; (b) no legitimate specific interests of the data subject prevent transmission; and (c) in particular cases, transfer is essential for the competent authority transmitting the data to a private party. In this last case, the transfer must be essential for: the performance of a task lawfully assigned to the transmitting authority; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; the prevention of an immediate and serious threat to public security; or the prevention of serious harm to the rights of individuals. The EU legislator has linked this transmission to strict conditions because of the serious consequences that may result from too an easy exchange of data with private parties. According to the purpose specification principle, it is also provided that the competent authority transmitting the data to a private party shall inform the latter of the purposes for which the data may exclusively be used.

5 Rights of the Data Subject

Four Articles of Framework Decision 2008/977/JHA are dedicated to the rights conferred upon the data subject, which are: the right of access; the right to rectification, erasure and blocking; the right to compensation; and the right to a judicial remedy.[18]

As far as the right of access is concerned, Article 17 provides that every data subject shall have the right to obtain a confirmation from the controller or from the national supervisory authority as to whether or not data relating to him have been transmitted or made available, information on the recipients to whom data have

[18] The right to information is implied in the obligation for the Member States to inform the data subjects about the collection or processing of their personal data. See above, § 3.

been disclosed, and communication of the data undergoing processing. As an alternative, the data subject shall have the right to obtain a confirmation from the national supervisory authority that all necessary verifications have taken place. The access right is to be considered one of the central axes of the European personal data system as it guarantees transparency[19] and provides for better prevention of potential abuses. However, this right may be restricted where such a restriction constitutes a necessary and proportional measure to preserve either State's prerogatives or to safeguard individual rights. In the first case, restriction shall be allowed: to avoid obstructing official or legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; or to protect public or national security. In the second case, restriction shall be allowed to protect the data subject or the rights and freedoms of others. Any decision on refusal or restriction, together with the factual or legal reason on which the decision is based, shall be communicated to the data subject. However, the reason on which the decision is based may be omitted where a reason for restricting access exists. The data subject must in all cases be advised that he may appeal to the competent national supervisory authority, a judicial authority, or to a court.

As to the right to rectification, erasure or blocking (Art. 18), it is for the Member States to lay down whether the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority. If the controller refuses rectification, erasure or blocking, the refusal must be communicated in writing to the data subject who must be informed of the mechanism provided for in national law for lodging a complaint or seeking judicial remedy. Upon examination of the complaint or judicial remedy, the data subject shall be informed whether the controller acted properly or not. Member States may also provide that the data subject be informed by the competent national supervisory authority that a review has taken place. Furthermore, if the accuracy of an item of personal data is contested by the data subject, and its accuracy or inaccuracy cannot be ascertained, referencing of that item of data—this meaning the marking of stored personal data without the aim of limiting their processing in future—may take place.

The Framework Decision also provides the right to compensation (Art. 19), under which any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation for the damage suffered from the controller or other authority competent under national law. Liability to the injured party always falls on the recipient. However, if the recipient pays compensation for damage caused by the use of incorrectly transmitted data, the transmitting competent authority shall refund to the recipient the amount paid in damages, taking into account any fault that may lie with the recipient.

Finally, the right to a judicial remedy (Art. 20) is granted to the data subject for any breach of the rights guaranteed to him by the applicable national law. It is

[19] Andoulsi (2010), p. 377.

noteworthy that this right is not granted to individuals in case of breach of the Framework Decision but instead for breach of national law (and not necessarily the piece of national legislation implementing the EU measure).

6 National Supervisory Authorities and the European Data Protection Supervisor

Crucial in the protection system envisaged by the European legislator is the role of national supervisory authorities.[20] Indeed, the application of the Framework Decision by the Member States in their territories is primarily advised and monitored by independent national supervisory authorities [Art. 25(1)], endowed with investigative powers, powers of intervention, and the power to engage in legal proceedings where the national provisions adopted pursuant to the Framework Decision have been infringed [Art. 25(2)]. Furthermore, each supervisory authority hears claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data [Art. 25(3)]. National supervisory authorities must also be consulted prior to the processing of personal data, forming part of a new filing system to be created where special categories of data are to be processed or the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject (Art. 23).

Of course, equally important in the EU data protection system is the role played by the EDPS, a figure that gives visibility to the system itself, provides for independence, and puts expertise at the service of the EU administration.[21] As pointed out by some scholars,[22] the main duties of the EDPS—which may be grouped into supervision (particularly significant the supervision of the EURODAC central unit as well as of large-scale databases such as the SIS II and the VIS), consultation (which implies monitoring of legislative proposals and technological developments as well as advising EU institutions and bodies), and cooperation with national supervisory authorities—permit the EDPS to claim a role as a main actor in the field of police and judicial cooperation in criminal matters.

[20] As explained under point 34 of the *Consideranda*, the supervisory authorities already established under Directive 95/46/EC will also be entrusted with the tasks to be performed under the Framework Decision.

[21] Hijmans (2006), pp. 1341–1342.

[22] De Hert and Bellanova (2009), p. 11.

7 The Way Forward: The Communication from the Commission

After Framework Decision 2008/977/JHA entered into force, Member States adopted the Treaty of Lisbon, which has changed the institutional and legal framework of the EU as a whole and in particular in the area of police and judicial cooperation in criminal matters.

The most striking novelty brought about by the new Treaty is the abolition of the pillar structure. As far as protection of personal data is concerned, this has led to the adoption of a legal basis applying to all EU policies,[23] prominently placed in Title II on "Provisions of general application:"[24] Article 16 TFEU grants individuals the right to protection of personal data, and provides that the European Parliament and the Council—acting in accordance with the ordinary legislative procedure—shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.[25] Compliance with these rules is subject to the control of independent authorities. In addition, the Lisbon Treaty (Art. 6 TEU) confers binding force upon the EU FRCh, thereby strengthening the value of Article 7 on the right to privacy, and Article 8 on the right to the protection of personal data.[26] Clearly, this new framework calls the current scenario into question, since at the moment two different measures (the Directive and the Framework Decision) having different legal capacity and different contents apply to different sectors of EU law.

Following a roadmap towards a comprehensive new framework for the protection of personal data in the EU,[27] in 2010 the Commission addressed a Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions[28] in which it put forward some

[23] With the only exception of protection of personal data in the area of Common Foreign and Security Policy, specifically ruled under Article 39 TEU.

[24] Scirocco (2008) (emphasis added).

[25] Preservation of national security interests is guaranteed, however. In the Declaration 20 attached to the Lisbon Treaty, the Conference has declared that, "whenever rules on protection of personal data to be adopted on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter." It has been rightly pointed out that this declaration does not add much to the current legal framework, in which exceptions for public interests and national security are already possible. See Scirocco (2008).

[26] As pointed out by Mitsilegas (2009), p. 279, "[t]he incorporation of the Charter into EU law may prove to be extremely significant in allowing European judges to develop privacy standards to be taken into account in both the implementation of existing legislation and the formulation of subsequent laws."

[27] Available at: http://ec.europa.eu/governance/impact/planned_ia/docs/72_jls_data_protection_-strategy_and_legal_framework_en.pdf.

[28] COM (2010) 609 final, Brussels, 4 November 2010.

suggestions on how to review the current legal framework. This communication followed a number of initiatives on the subject: a conference in May 2009, a public consultation that remained open until the end of 2009,[29] and a number of studies. In the public consultation in particular, all stakeholders stressed the need for an overarching instrument applying to data processing operations in all sectors and policies of the Union (p. 4 of the Communication), thereby confirming the motion, often subscribed to in the academic circles, that the protection of fundamental rights is a horizontal issue that has an impact on all EU policies.[30]

The idea suggested by the Commission—as already presented in the Communications on the Stockholm Programme and the Stockholm Action Plan[31]—is to revise and build upon the Data Protection Directive, considered to set "a milestone in the history of the protection of personal data in the European Union" (p. 2), so as to have a comprehensive protection scheme. However, this does not exclude the possibility of having specific rules for data protection for the police and the judicial cooperation sector (p. 14). Indeed, notwithstanding the abolition of the pillar structure brought about by the Treaty of Lisbon, a certain degree of differentiation between the processing of personal data for commercial purposes and the processing of personal data for crime prevention and investigation purposes is still justified. Actually, the possibility of different rules is already enshrined under Declaration 21, attached to the Lisbon Treaty, where the Conference has acknowledged that:

> specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.[32]

Under the heading "Revising the data protection rules in the area of police and judicial cooperation in criminal matters" of the Communication (pp. 13–15), it is possible to recognize four main changes that the Commission wishes to undertake as far as data protection in the criminal law sector is concerned. First of all, the distinction between cross-border exchange, to which Framework Decision 2008/977/JHA currently applies, and domestic processing operations in the Member States is difficult to make in practice and can complicate the actual implementation

[29] "This public consultation was intended to reach a broad range of stakeholders, based on three very open questions, leaving them as much leeway as possible in identifying new challenges, signalling out areas that would need improvement, and making suggestions on how a future legal framework could better tackle certain problems." Reding (2010), p. 27. It is noteworthy that, in the same period, the Commission organized also a public consultation on the possibility of an agreement with the United States on data protection principles to be applied to transatlantic exchanges.

[30] Andoulsi (2010), p. 370.

[31] Respectively, COM (2009) 262, 10 June 2009, and COM (2010), 20 April 2010.

[32] Thus, such a Declaration does not favour the co-existence of different legal instruments, but actually supports the creation of a single legal framework, with some specific rules where needed. Andoulsi (2010), p. 371.

and application of the Framework Decision itself. Thus, a comprehensive data protection system should not rest on that difference. Secondly, data protection as presently envisaged in the area of police and judicial cooperation in criminal matters is undermined by too wide an exception to the purpose limitation principle, thereby opening the door to potential abuses by public authorities. Limitations on certain data protection rights should be harmonized so as to guarantee legal certainty and the respect of the rule of law throughout the EU. Thirdly, no distinction between different types of data and different categories of data subjects is currently made, despite being urgently needed. For instance, different rules may apply to the processing of genetic data for criminal law purposes, or to the categories of victims, witnesses and suspects. Fourthly, the various sector-specific data protection regimes adopted at EU level—in particular those relating to Europol, Eurojust, the SIS and the CIS—have not been replaced by Framework Decision 2008/977/JHA. This situation has led to a multi-level data protection regime where different legal instruments, and therefore different standards affecting individuals in exercising their data protection rights, apply. Indeed, some of these sector-specific instruments provide particular data protection rules while others refer to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and Recommendation R(87) 15, both adopted outside the EU by the Council of Europe and before the widespread rise and use of new information technologies.[33] A coherent data protection system should cover all the relevant areas with a single instrument.[34]

This Communication has constituted the basis for further discussion on the subject-matter and has represented one of the first steps toward a legislative proposal for the adoption of a single EU data protection instrument.[35]

8 Opinion of the European Data Protection Supervisor

After the Commission adopted the Communication on a comprehensive approach on personal data protection in the EU, the EDPS was consulted and delivered an Opinion in January 2011.[36]

[33] De Hert and Bellanova (2009), p. 4.

[34] It must be pointed out, though, that Europol and Eurojust pleaded for taking into account the specificities of their work regarding the coordination of law enforcement and crime prevention (see p. 4, footnote 7).

[35] A proposal was expected from the Commission within the first half of 2011. At the time of writing no proposal is yet available.

[36] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Region—"A comprehensive approach on personal data protection in the European Union," Brussels, 14 January 2011.

In general, the EDPS has shared the view of the Commission that a strong framework for data protection is necessary, especially following the adoption of the Lisbon Treaty. The EDPS has stressed that a strong framework serves both private and public interests. Not only does it promote individual rights to privacy, but it also fosters security, especially in the area of police and judicial cooperation (para. 18–24 of the Opinion).

In particular, the EDPS has assessed the proposed solutions in the Communication against two criteria: ambition and effectiveness (para. 7). In this respect, the "ambitious" objective of comprehensiveness, i.e. the adoption of a single EU instrument for data protection including police and judicial cooperation in criminal matters, is considered essential by the EDPS for "effective" data protection. In support of such single instrument, the EDPS has highlighted that: the distinction between activities of the private sector and of the law enforcement sector is blurring[37]; there is no fundamental difference between police and judicial authorities and other authorities delivering law enforcement (such as taxation, customs, anti-fraud, immigration) subject to Directive 95/46/EC; Framework Decision 2008/977/JHA is inadequate; and most Member States have implemented Directive 95/46/EC and Council of Europe Convention 108 making them applicable also to their police and judicial authorities (para. 33–35). As underlined by the EDPS, the adoption of a single instrument would also mean that EU data protection rules will no longer apply only to cross-border data exchanges but will apply also to domestic processing (para. 130). In line with this comprehensive approach, the EDPS believes that the new instrument should replace the various sector-specific legislative instruments for police and judicial cooperation in criminal matters, such as those relating to Europol, Eurojust, the SIS and Decision 2008/615/JHA (para. 135–136).

However, a comprehensive measure should not prevent the adoption of additional sector-specific regulations for police and judicial cooperation (para. 48). The EDPS too has considered the need for special rules and derogations in consideration of the unique nature of the police and justice sector, as recognized by the Commission and according to Declaration 21 attached to the Lisbon Treaty. In particular, distinctions should be drawn between different categories of data (data based on facts should be distinguished from data based on opinions and personal assessments), different categories of data subjects (criminal suspects, victims, witnesses, etc.) and different types of files (permanent, temporary, intelligence files) (para. 131–133).

Moreover, in conformity with the Communication from the Commission, the EDPS has expressed agreement with the need for harmonisation: since data protection is now recognised as a fundamental right under Article 8 EU FRCh and

[37] This has been demonstrated by the ECJ rulings in the cases of PNR and the data retention Directive (respectively, joined cases C-317 & 318/04, *European Parliament v. Council and Commission*, 2006, and Case C-301/106, *Ireland v. Parliament and Council*, 2009). On this issue see: Kosta et al. (2007), pp. 2–3; Hijmans and Scirocco (2009), pp. 1501–1508; and Scirocco (2008).

everyone is granted the right to the protection of personal data under Article 16 TFEU, an equivalent level of protection must be guaranteed throughout the EU. To this end, the most relevant areas for harmonisation recognised by the EDPS are: definitions, lawfulness of processing, grounds for data processing, data subject rights, international transfers and National Data Protection Authorities (para. 49–59).

Finally, it is noteworthy that the EDPS has suggested reconsidering the type of legal instrument to be used to review the framework of data protection. Instead of a Directive, as suggested by the Commission, the EDPS is of the opinion that a Regulation would be the best instrument to intervene in the area under consideration, as it is directly applicable at national level and leaves no much discretion to Member States in its implementation, without precluding the possibility to adopt additional rules as needed. The EDPS argues that this type of instrument would reduce room for contradictory interpretations and reduce the importance of determining the law applicable to processing operations within the EU—one of the most controversial aspects of the present system (para. 64–67).

9 Final Remarks

The protection of individuals against the exchange of personal data for crime prevention and investigation purposes is of utmost importance: it contributes to striking the right balance between security and privacy. Although in the last few years significant progress has been made, the European legislator has not yet found a satisfactory balance between these conflicting interests, and security has prevailed at the expense of privacy.

The goal emerging from the current public debate carried out at institutional level, the alignment of the current regime applying to police and judicial cooperation in criminal matters to the regime provided for by Directive 95/46/EC, is to be welcomed for two main reasons.

Firstly, the need for a single overarching instrument springs from the increasingly blurry line dividing data processing for commercial purposes from data processing for crime prevention and investigation purposes. Secondly, Framework Decision 2008/977/JHA is disappointing as it is the result of a lengthy and difficult decision-making process affected by the requirement of unanimity in the Council.[38] Its content is poor and leaves many questions open, with the assessment of the proportionality principle and of the principle of adequacy of protection being perhaps the most striking ones. Now that the Lisbon Treaty expressly provides

[38] "[...] discussions in the Council appeared a race to the lowest common denominator, and the final text appears too weak to substantially modify the previous context [...T]he European Parliament's amendments, that could have contributed to address some major issues, have not been integrated in the final text." De Hert and Bellanova (2009), p. 5. See also Mitsilegas (2009), pp. 273–274.

for the ordinary legislative procedure for the adoption of measures concerning personal data protection, whatever area of law is concerned, the hope is that braver and more coherent choices will be possible.[39] Expectations for a new comprehensive instrument on personal data protection in the EU are high. Soon, it will be possible to assess whether these expectations have been met.

References

Andoulsi I (2010) Personal data protection and the first implementation semester of the Lisbon Treaty: achievements and prospects. NJECL 3:362–384

Ciampi S (2009) Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea. In: Peroni F, Gialuz M (eds) Cooperazione informativa e giustizia penale nell'Unione europea. Edizione Università di Trieste, Trieste, pp 34–100

De Busser E (2007) The architecture of data exchange. Revue Internationale de Droit Pénal 78:35–55

De Busser E (2010) Transatlantic adequacy and a certain degree of perplexity. Eucrim 1:30–36

De Hert P, Bellanova R (2009) Data protection in the Area of Freedom, Security and Justice: a system still to be fully developed? Study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE). Policy Department C, Citizens' Rights and Constitutional Affairs. http://www.europarl.europa.eu/activities/committees/studies/download.do?language=en&file=25213

De Hert P, Papakonstantinou V (2009) The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – a modest achievement however not the improvement some have hoped for. Comput Law Secur Rev 25:403–414

Gialuz M (2009) La cooperazione informativa quale motore del sistema europeo di sicurezza. In: Peroni F, Gialuz M (eds) Cooperazione informativa e giustizia penale nell'Unione europea. Edizione Università di Trieste, Trieste, pp 15–33

Gutwirth S, De Hert P (2008) Regulating profiling in a democratic constitutional state. In: Hildebrandt M, Gutwirth S (eds) Profiling the European Citizen. Springer, pp 271–293

Hijmans H (2006) The European data protection supervisor: the institutions of the EC controlled by an independent authority. CMLR 43:1313–1342

Hijmans H, Scirocco A (2009) Shortcomings in EU data protection in the third pillar and the second pillars. Can the Lisbon Treaty be expected to help? CMLR 46:1485–1525

Hustinx P (2010) Editorial. Eucrim 1:1

Kosta E, Coudert F, Dumortier J (2007) Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive. BILETA, 2007 Annual Conference, Hertfordshire 16–17 April: 1–12

Mitsilegas V (2009) EU criminal law. Hart Publishing, Oxford and Portland, Oregon

Reding V (2010) Data protection in the EU – challenges ahead. Eucrim 1:25–30

Reding V (2011) The upcoming data protection reform for the European Union. Int Data Privacy Law 1:3–5

Scirocco A (2008) The Lisbon Treaty and the protection of personal data in the European Union. Digital magazine Dataprotectionreview.eu. "Experts opinion":1. http://www.dataprotectionreview.eu/

[39] As affirmed by the current EDPS, Peter Hustinx (2010), p. 1, "[o]n the basis of Article 16, a comprehensive legal framework for data protection, combining consistency and solidity, will no longer be wishful thinking but a feasible policy objective."