BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive

Eleni Kosta, Fanny Coudert & Prof. Jos Dumortier
Interdisciplinary Center for Law & ICT (ICRI) – Katholieke Universiteit Leuven
Email: eleni.kosta@law.kuleuven.be, fanny.coudert@law.kuleuven.be

1. Introduction

The European Directive on data protection[1] regulated the issue of processing of personal data and their free movement, setting out the general principles that have to be followed. As highlighted by the European Commission, the harmonised set of rules incorporated in the directive is ensuring "a high standard of protection for personal data throughout the EU [and] has brought considerable benefits for citizens, business and authorities"[2]. It was further stressed that this framework protects "individuals against general surveillance or undue discrimination on the basis of the information others hold on them".[3]

However the processing of personal data carried out by law enforcement authorities is not regulated at European level. The data protection directive only applies to activities which do not fall outside the scope of Community Law, i.e. "areas of foreign and security policy, and justice and home affairs, where policing policy sits"[4]. Article 3§2 explicitly mentions that the directive does not apply with regard to activities that relate to a "common foreign and security policy"[5] or to "police and judicial cooperation in criminal matters"[6].

Although the issue of data protection in law enforcement is not covered by the European directive, it does not remain fully unprotected. Article 8 of the European Convention on Human Rights[7] explicitly states that "there shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"[8].

The processing of personal data that takes place in the filed of law enforcement falls also under the scope of application of the Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data. In order to foster police cooperation and thus the exchange of information safeguarding the fundamental right to privacy,

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, p. 31–50 (23 November 1995)
[2] Communication from the European Commission to the European Parliament and Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, 7 March 2007, p. 2.
[3] ibid.
[4] Hayes B., A failure to regulate: data protection and ethnic profiling in the police sector in Europe, in "Ethnic profiling by Police in Europe", ed. Open Society Justice initiative, 2005.
[5] Title V EU Treaty
[6] Title VI EU Treaty
[7] Council of Europe, European Convention of Human Rights (ECHR), Rome, 4 November 1950.
[8] Article 8 ECHR

the Council of Europe issued a recommendation in 1987 relative to the use of personal data in the police sector.[9]

Nevertheless, as already admitted by the European Data Protection Authorities, Convention 108 "is too general to effectively safeguard data protection in the area of law enforcement. Given the Union's obligation to respect human rights and fundamental freedoms, initiatives to improve law enforcement in the EU […] should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection"[10].

The difficult exercise of balancing the two public interests at stake, the protection of public order and the right of every individual to privacy is currently actually realised at national level. It appears important to find an adequate equilibrium, since, as highlighted by the Council of Europe, "criminal justice systems of the member states have a pivotal role in the enforcement of human rights. Whenever they investigate suspected crimes, whenever they execute judicial orders and every time they come into contact with the citizens, the conduct of the police symbolises how human rights are respected and protected within each country".[11]

The terrorist attacks of 2001 and the bombings in Madrid and London have given rise to the political interest in police cooperation throughout the European Union and its regulation in order to ensure greater efficiency. This regulation should respect human rights as provided by article 6 of the Treaty on European Union and particularly the right to privacy and data protection.

2. The impact of the ECJ decision on PNR data and the data retention directive on the need for a data protection legislation in the third pillar

The European Court of Justice with a recent Judgement[12] annulled the Council Decision concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of passenger name record (PNR) [13] data by air carriers to the United States Bureau of Customs and Border Protection (CBP) and the Commission Decision on the adequate protection of those data[14]. The Court ruled that the "transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law"[15]. Although the data have been initially collected for commercial purposes, the Court found that the actual purpose of their transfer falls outside the scope of protection of the data protection directive, which only applies to activities falling under Community Law, leaving however unanswered the question where the activities under discussion belong[16]. The Court followed the argumentation of the general advocate and

---

[9] Council of Europe, Recommendation nº R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, 17 September 1987

[10] Declaration of the European Data Protection Authorities, Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005, available online at http://www.datatilsynet.dk/attachments/200552514446/krakowdeclarationfinalversion%20-%20adopted.pdf (last visited on 21.03.2007)

[11] ibid

[12] Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 (30 May 2006)

[13] Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC), Official Journal L 183, page 83 (20 May 2004)

[14] Commission Decision of 14 May on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, Official Journal L 235, pages 11–22 (06 July 2004)

[15] Paragraph 56 of the Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 (30 May 2006)

[16] Elspeth Guid & Evelien Brouwer, The political life of data: the ECJ Decision on the PNR Agreement beween the EU and the US, July 2006, Centre for European Policy Studies, available online at http://www.libertysecurity.org/IMG/pdf/1363.pdf (last accessed 18 March 2007)

distinguishes between the activities of collection of data and the purpose of the (further) processing based on public safety, needs, in order to exclude the latter from the scope of application of the data protection directive. The Court Judgement can be briefly described as admitting that the data collected for commercial purposes fall within the protective ambit of the data protection directive but when the same data are transferred for public security reasons, they no longer enjoy the same protection. The Judgment of the European Court created a substantial *lacuna legis* in the protection of PNR data, raising the general problem of protection of personal data that are not covered by the data protection directive[17].

A few months before the Judgement, the European Union adopted the data retention directive[18], which creates an obligation for communications and internet service providers to retain traffic and location data for the purpose of the investigation, detection and prosecution of serious crime. The directive does not however deal with the access and actual use of the retained data after they have been accessed by competent authorities in the field of law enforcement. According to the European Data Protection Supervisor "the rules on the access, the use and the exchange of the data are inseparable from the obligation itself to retain the data"[19] and the fact that the data retention directive does not regulate how the data subject can be protected after the data are accessed by law enforcement authorities and further used, "makes it even more urgent to establish a legal framework for data protection in the third pillar"[20].

It is to be mentioned that the legal basis of the data retention directive has been challenged by the Irish Government[21], who claims that it should have been adopted under the third pillar. The application filed by Ireland follows the reasoning of the Court in the PNR Judgement which, as mentioned above, considered as purpose for the transfer of the PNR data not their collection from the airline companies within commercial activities, but their "processing for operations concerning public security and the activities of the State in areas of criminal law"[22]. Ireland contains that "the sole or, alternatively, the main or predominant purpose of the Directive is to facilitate the investigation, detection and prosecution of serious crime, including terrorism [and consequently] the only permissible legal base for the measures contained in the Directive is Title VI of the Treaty on European Union ('TEU'), in particular Articles 30, 31(1)(c) and 34(2)(b)".[23]

The aforementioned examples illustrate that the limits between data collected and used in the first and the third pillar are not always very clear. Data are collected within commercial activities and can be processed according to the rules set out in the data protection directive, but they can further be transferred to or accessed by law enforcement authorities for public security reasons. Although the data are the same, the protection offered by the European legal system is different. The pillar structure is in this case creating a legal loophole in the protection of personal data that could be resolved if the European Constitution is ratified, the pillar structure collapses and the

[17] See also the analysis made by Hielke Hijmans, in Hielke Hijmans 'De derde pijler in de praktijk: leven met gebreken Over de uitwisseling van informatie tussen lidstaten'. SEW 2006.91, under chapter 4.1

[18] Directive 2006/24/EC of the European Parliament and of the Council 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, Official Journal L105, pages 54–63 (15 March 2006)

[19] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public communications services and amending Directive 2002/58/EC (COM (2005)438 final), OJ C 298, page 1, §40

[20] First opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005) 475 final), OJ C 47, 25.02.2006, page 3, § 17

[21] European Court of Justice, C-301/06: Ireland v Council and Parliament, O.J.E.U. C 237/5, 30 September 2006

[22] op. cit., fn. 15.

[23] op.cit., fn 21.

Charter of Fundamental Rights of the European Union is legally binding.[24] With regard to the Charter it has however supported that it is already legally binding as it is "explicitly and directly referred to by international and national Courts"[25].

3. Data protection and police and judicial cooperation in criminal matters: multitude of legislative proposals

In its communication of 16 June 2004, the European Commission pointed out that the "effectiveness of law enforcement activities should build upon observance of human rights and fundamental freedoms as protected by international, European and constitutional traditions common to Member States"[26], clarifying that "[t]he human rights challenge means striking the appropriate balance between robust data protection and due respect of other fundamental rights on the one hand and, high performing use of law enforcement information aimed at safeguarding essential public interests such as national security and the prevention, detection, and prosecution of crime on the other"[27].

Specific initiatives have already been proposed within the Hague Programme[28], with which the European Commission launched its 5 year action plan for freedom, justice and security. Among others the Hague Programme has as goal "to fight organised cross-border crime and repress the threat of terrorism, to realise the potential of Europol and Eurojust, to carry further the mutual recognition of judicial decisions and certificates both in civil and in criminal matters, and to eliminate legal and judicial obstacles in litigation in civil and family matters with cross-border implications. This is an objective that has to be achieved in the interests of our citizens by the development of a Common Asylum System and by improving access to the courts, practical police and judicial cooperation, the approximation of laws and the development of common policies"[29].

The Hague Programme introduced the principle of availability in the field of law enforcement, which means that, "throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State"[30]. On this basis the European Commission presented a proposal for a Framework decision on the exchange of information under the principle of availability (hereafter Draft decision on availability)[31], where it is foreseen that that information shall be provided when it is necessary for the fulfillment of lawful tasks by the equivalent competent authorities of a Member State for the prevention, detection or investigation of criminal offences"[32]. The objective of effective implementation of the availability principle is set up by the Hague Programme for the 1st of January of 2008.

---

[24] Op.cit., fn 16.
[25] Stefano Rodota, The European Constitutional Model for Data Protection, paper presented at the European Parliament's Public Seminar "PNR/SWIFT/Safe Harbour: Are transatlantic data protected? (Transatlantic relations and data protection), 26 March 2007.
[26] Communication from the Commission to the Council and the European Parliament of 16 June 2004 - Towards enhancing access to information by law enforcement agencies (EU information policy), COM/2004/0429 final
[27] ibid
[28] The Hague Programme: Strengthening freedom, security and justice in the European Union, 13.12.2004, Council of the European Union, 16054/04 (JAI 559)
[29] ibid, page 3
[30] ibid, page 18
[31] European Commission, Proposal for Framework decision on the exchange of information under the principle of availability, COM(2005) 490 final, 12.10.2005
[32] ibid, Art. 6

The principle of availability is introduced in order to counterbalance the lack of trust between authorities in various Member States that hinders the exchange of information. Although it is beyond doubt that it will enhance the cooperation between law enforcement authorities, it does not deal with the actual problem of lack of trust between them[33]. However, this decision has not yet been adopted, confirming –as of today at least- the doubts of the European Data Protection Supervisor whether the proposal for a Draft decision on availability will "eventually lead to the adoption of a legal instrument"[34]. The aforementioned decision shall be treated as part of a more general attempt to regulate the issue of police and judicial cooperation at European level, with a special focus on the protection of personal data[35].

The principle of availability is also introduced in the Prüm Convention[36], also referred to as "Schengen III", which was initially signed by seven Member States. According to Article 1 of the Convention it is open for any Member State of the European Union to join, an invitation that nine more Member States[37] have accepted or have already expressed the intention to accept. Although this initiative started as a multilateral agreement outside the European Union, the Contracting Parties aim to incorporate the provisions of the Convention into the legal framework of the European Union[38] and in any case the provisions of the Convention shall be compatible with European Union Law[39]. In fact the German presidency has already expressed the intention to integrate the Prüm Convention into the European legal framework. More specifically, according to a JHA Press Release "the Council agreed on the integration into the EU legal framework of the parts of the Prüm Treaty relating to police and judicial cooperation in criminal matters (the so-called third pillar), with the exception of the provision relating to cross-border police intervention in the event of imminent danger (Article 48). This particular issue will be further examined by the Council" [40].

The Prüm Convention introduces *inter alia* measures to improve information exchange for DNA, fingerprint data as well as vehicle registration data. It contains also general provisions on data protection[41] that determine the level of protection, the purposes for the processing of the personal data, interpret the general principles of data processing into the needs of the Convention and describe the rights of the data subjects. Nevertheless the Prüm Treaty suffers from two major inconveniences, from a data protection point of view. Firstly, it compels signatory states to create new databases of DNA data, through an obligation to open and keep DNA analysis files for

---

[33] See similar opinion in Mitsilegas Valsamis, "Police cooperation: What are the main obstacles to police co-operation in Europe?", available online at http://www.libertysecurity.org/imprimer.php?id_article=1379 (last accessed on 17.03.2007)

[34] European Data Protection Supervisor, Opinion of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005)490 final), OJ C 116, 17.05.2006, page 8

[35] According to the European Data Protection Supervisor "the availability of law enforcement information across the internal borders of the European Union will also be further facilitated by other legal instruments, such as the proposals regarding a Second Generation Schengen Information System (SIS II), the proposal for access for consultation to the Visa Information System (VIS) and the proposal for a Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States", see European Commission, Proposal for Framework decision on the exchange of information under the principle of availability, COM(2005) 490 final, 12.10.2005 §11. These initiatives will not be dealt with extensively within this paper.

[36] Convention between the Kingdom of Belgium, the federal Republic of Germany, the Kingdom of Spain, the French Republic, the grand Duchy of Luxemburg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed by the contracting parties in Prüm (Germany) on the 27 May 2005

[37] Italy, Portugal, Slovenia, Finland, Sweden, Romania, Bulgaria, Greece and Slovakia (status as of 01.03.2007)

[38] Article 1(4) of the Prüm Convention

[39] Article 47(1) of the Prüm Convention

[40] Press Release , 2781st Council meeting Justice and Home Affairs, Brussels, 15 February 2007 (5922/07 (Presse 16), page 7

[41] Chapter 7 of the Prüm Convention

investigation of criminal offences, with the correlative risks in terms of data protection. Secondly, it has been approved outside the scope of the European Institutions and thus creates the risks of creating a police cooperation in variable geometry, outside the control of European Institutions.[42]

Similar provisions are included in the Draft Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[43]. The proposal for this decision was submitted by the European Commission on 4 October 2005, but has still not been adopted by the Council of the European Union. Due to the fact that no consensus on the decision could be made among the Member States, the German presidency urged the European Commission to submit a revised document of the Draft Decision[44]. In lack of any response on behalf of the European Commission, the German Presidency has introduced a new draft on the 13th of March 2007 (hereafter Draft Decision on data protection in the third pillar)[45], revising the decision into several points.

4. Data protection principles and protection of data subject under the third pillar. The example of the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

In order to ensure consistency in the European data protection framework, as well as a high level of protection, the same general data protection principles shall apply to every processing, irrespective of its purposes. However, the modalities of law enforcement processing, i.e. for purposes of prevention, detection, prosecution of criminal activities, calls for an adaptation of certain rules. This does not mean derogation from and weakening of the protection, but an adjustment to the needs of police, guided by the principle of proportionality[46].

Data protection rules in police field should not only respond to "justified needs of law enforcement but should also protect the data subject against unjustified processing and access".[47] As stressed by the European Data Protection Supervisor, "to be in accordance with the principle of proportionality, the result of the considerations of the European legislator needs to reflect the respect of the two potentially opposite public interests".[48] As the data protection directive made a balance between the free flow of information and the right to privacy of the data subject, a data protection framework in the third pillar shall ensure the effective police action without lowering the right of data subject in an unjustified and disproportionate way. This exercise appears relatively difficult due to the sensitiveness of the field. However, if this framework is aimed to protect "individuals against general surveillance or undue discrimination on the basis of the information others hold on them"[49] as according to the European Commission the data protection directive has achieved in the first pillar, a strict proportionality test should be applied to every derogation introduced to general principles of protection.

---

[42] op cit., fn 31.
[43] Proposal for a Draft Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM (2005) 475 final, 04.10.2005
[44] Point 7 of the Presidency note to the Article 36 Committee, EU doc 5435/07 (18 January 2007). The Article 26 Committee, provided for by Article 36 of the Treaty on European Union, also known as CATS, is a Council working group. The Committee is made up of senior officials and its role is to coordinate the competent working groups in the field of police and judicial cooperation (third pillar). Its mission is also to prepare the relevant work of the Permanent Representatives Committee.
[45] Council of the European Union, Proposal for a Council Framework Decision on the protection of personal data
processed in the framework of police and judicial cooperation in criminal matters, EU doc no: 7315/07, 13 March 2007)
[46]ibid, § 10.
[47] Op.cit., fn. 20, § 10.
[48] ibid
[49] op. cit., fn. 2.

4.1 Scope of application

The existing rules set out in the data protection directive can not apply as such when personal data are being processed in the course of activities that fall under the third pillar. These rules shall serve as a basis in order to ensure consistency within the European Union but additional rules that apply to the special needs of law enforcement shall be deployed as well[50]. Following the declaration of the European Data Protection Authorities that supported the adoption of a legal instrument regulating the issue of data protection in the third pillar, the European Commission submitted as already mentioned on the 4th of August 2005 a proposal for the already mentioned Draft Decision on data protection in the third pillar.

An important point in the discussion is whether the framework should apply only to the exchange of personal data between law enforcement agencies of the different Member States or should cover every data processing in the law enforcement field. This question is of paramount importance as it conditions the effectiveness of the protection ensured by the draft decision. As underlined by the European Data Protection Supervisor, in case the sole exchange of information between law enforcement authorities of the different Member States would be covered, "it would make the field of application of the framework decision particularly unsure and uncertain, which would be contrary to its essential objective"[51]. The Draft Decision on data protection in the third pillar follows this statement aiming at ensuring that national data-processing fulfil the conditions for transmitting data since the data are collected.[52]

One main issue that needs to be decided upon with regard to regulating the issue of data protection in the third pillar is who can have access to the data. The main problem is whether the decision will also apply to Europol, Eurojust and the third-pillar information system. Although the Commission proposal was explicitly excluding Europol, Eurojust and the Customs Information System, the German Presidency in the recent draft on the decision admits that "[i]mproving data protection within the third pillar depends on the Framework Decision covering the whole of the third pillar, including Europol, Eurojust and the third-pillar Customs Information System. Care must be taken to ensure that more extensive specific data protection rules in the relevant legal instruments remain unaffected. Where the Framework Decision is to replace existing specific data protection provisions, the Data Protection Framework Decision stipulates this explicitly."[53] However, the European Data Protection Supervisor has already pointed out[54] that there is no urgent need to adapt the data protection systems Europol and Eurojust have at their disposal to the principles set out by a draft decision on data protection in the third pillar.

Closely related to the issue of who can have access to the data, is who will supervise and monitor the observance of data protection rules in the processing of personal data. Having different authorities in charge of supervising data protection rules in the First and the Third Pillar areas of activities entails the risk of diverging interpretation and conception of data protection rules. For the first time a joint supervisory authority[55] is proposed in the Draft Decision on data protection in the third pillar that will replace the existing systems of supervisions regarding Schengen, Europol, Eurojust and Customs Information System.

4.2 Principles for the processing of personal data under the third pillar

[50] Declaration of the European Data Protection Authorities, Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005, available online at http://www.datatilsynet.dk/attachments/200552514446/krakowdeclarationfinalversion%20-%20adopted.pdf (last visited on 21.03.2007)
[51] op. cit., fn. 20.
[52] Recital 6(a) of the Draft Decision on data protection in the third pillar
[53] Recital 20 of the Draft Decision on data protection in the third pillar
[54] op. cit., fn. 20, par. 46
[55] Art. 26 Draft Decision on data protection in the third pillar

The data protection directive sets out the rules that apply to the processing of personal data. Due to the special character of law enforcement, however, these principles can not be used as such in a new legal instrument for law enforcement in the third pillar. These rules have to be taken into consideration and serve as the basis for a "tailor-made set of rules"[56] that will apply to the third pillar.

One of the basis principles for the protection of personal data as laid down in the data protection directive is the finality principle: "Data can only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"[57]. This principle shall also be respected when personal data are processed in activities that fall under the third pillar and the specific law enforcement purposes shall be well-defined[58]. In the field of law enforcement it might not always be very clear whether the further processing of data is compatible with the initial purposes or not. This rule shall be interpreted in such a way that the authorities are not hindered in the carrying out of their legitimate tasks and more specifically that the data can be used only when "it is strictly necessary, in a specific case, for the prevention, investigation, detection and prosecution of criminal offences or for the protection of the interests or fundamental rights of a person"[59]. Additional exceptions to the purpose limitation principle shall be justified, well defined and guaranteed by adequate safeguards, such as the consent of the data subject, whenever the context guarantees that it is freely given, specific and informed or when the processing appears necessary to protect his interests.

According to Article 6(1)(a) of the data protection directive personal data must be processed fairly and lawfully. The fairness principle is closely related with the aforementioned purpose limitation one. The grounds on which processing is allowed shall be clearly defined in the legal framework. Nevertheless the relevant provisions shall be formulated in such a way that they don't hinder the authorities to fulfil their legal obligations[60]. Suffice it to say that the data processed in an illegitimate way shall not be allowed as evidence in judicial proceedings[61].

The data protection directive entails specific provisions for the processing, or more precisely for the prohibition of processing of sensitive data, meaning "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life"[62]. Whenever the processing of such data is absolutely necessary for law enforcement purposes, it shall be clearly justified that the processing has to take place for a legitimate, well-defined and specific purpose[63]. According to the European Data Protection Supervisor the explicit consent of the data subject shall be used as a ground for data processing only when it is carried out for his own interest and if the refusal of the consent would not lead to negative consequences for him. In consistency with the *rationale* of the data protection directive, the processing of sensitive data shall be in principle prohibited and shall be allowed only under additional specific safeguards for clearly defined purposes.

In the field of law enforcement special consideration shall be given to DNA, fingerprint and biometric data in general, as these data play a significant role in police investigations. Such data are already mentioned in the Prüm Convention and in the draft decision on availability. Although these data do not always qualify as sensitive data[64], they can reveal a lot of information about the data subject and should therefore enjoy special protection in a legal instrument regulating the

[56] op.cit., fn. 50
[57] Art. 6(1)(b) data protection directive.
[58] Op. cit., fn. 50
[59] Op. cit., fn. 20 § 62. Similar approach has been adopted in the draft framework decision on data protection in the third pillar.
[60] Op. cit., fn. 20 § 69.
[61] Op. cit., fn. 20 § 70.
[62] Article 8§1 data protection directive
[63] Op. cit., fn. 50
[64] Article 29 Data Protection Working Party, Working document on biometrics, WP80, 1 August 2003, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf, Paragraph 3.7

protection of personal data in the third pillar. The use of vague and broad expressions, such as declaring that the processing of data is allowed "when this is strictly necessary and when suitable additional safeguards are provided"[65], should be avoided.

4.3 Rights of data subjects

The rights granted by the data protection directive, and especially the right of access, constitutes the core of data protection system as it empowers the data subject to control the processing of his personal data. It thus ensures the transparency of the processing, a crucial point for a data protection system effectiveness. According to Article 12 of the directive, the data subject has the right to obtain information about the data relating to him that are processed, and the right to ask the rectification of those data, mainly when they are incomplete or inaccurate. He also has the right to object to the processing of the data relating to him, as foreseen in Article 14 of the data protection directive. The exemptions to these rights should be in line with Article 13 of the directive[66], which refers, amongst others, to law enforcement activities. This exemption reflects not only the limits in the application of the directive but also the fact that the actual needs of law enforcement have to be taken into consideration as far as the right of access is concerned. This right could actually collide with the rights of third parties or even hinder the efficiency of law enforcement activities, particularly when the data subject is the one who is under investigation. However, a strict proportionality test should apply to any exemption introduced to a general rule. This means that the exception should be limited and well defined, and that restrictions should be, where possible, partial and limited in time. [67]

At national level, specific provisions have been implemented in order to guarantee both the protection of the data subject and the maintenance of public order, usually through the supervision of an independent authority. This authority is entitled to obtain the information required and to directly evaluate the legitimacy of the denial of the right of access of the data subject. Its independency guarantees an objective protection of the data subject. The Draft Decision on data protection in the third pillar opted for such a solution at supranational level and aims at establishing strong safeguards for the data subject. In case of denial of his petition of access, the controller should justify in a written form the reasons, the factual or legal basis for such denial and his right to appeal the decision to the supervisory authority appointed by the national legislation (or any other alternative way established by the national legislation).[68]

4.4 Transmission of personal data to third parties

As already mentioned, the data retention directive has been criticised for not dealing with the further processing of data for law enforcement purposes and, amongst others, for not regulating the access on the retained data from the law enforcement authorities, leaving this point to the national legislators of the Member States. As the European Data Protection Supervisor pointed out, this situation creates a gap in the protection which needs to be filled.[69]

The transmission of personal data entails a double concern. The fact that personal data are transferred from third parties, public or private, creates concerns regarding the legitimacy of the transfers and the accuracy of the data. The question of the legitimacy of the transfers raises the problem of 'leaky containers'[70]. The problem consists in determining to what extent personal data

---

[65] Article 7 of the Draft Decision on data protection in the third pillar

[66] Article 29 Data Protection Working Party, Working document on Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP12, 24 July 1998, available online at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf

[67] op. cit., fn. 20

[68] Article 17 of Draft Decision on data protection in the third pillar.

[69] op. cit., fn. 20, parag. 17

[70] Lyon. D, Surveillance society, monitoring everyday life, ed. Open University Press, MC Graw-Hill education, 2001.

collected for one purpose can be transmitted to a third party in order to be processed for a different purpose.

On one hand, the generalisation of exchanges of personal data between European law enforcement authorities will create the risk of further use of personal data for purposes possibly incompatible with the original purpose of the transmission. In the field of police cooperation this general principle set up by the data protection directive needed to be clarified in order to avoid broad interpretations. Article 3(2) of the Draft Decision on data protection in the third pillar does not only demand that the further processing of personal data is permitted insofar as it is compatible with the purposes for which the data are collected, but also that this processing appears essential and appropriate to these purposes. Moreover, in the specific case of transfers of personal data to law enforcement authorities of other Member States, article 12 restricts the processing to a series of limited purposes.

On the other hand, the increased possibilities of access by law enforcement authorities to personal data processed by private companies for commercial purposes raise concerns regarding the legitimacy of their further processing. This issue is in the core of the debate originated by the PNR agreement and it appears of paramount importance in our 'surveillance' society[71], where private companies are compelled to increase their collaboration with law enforcement agencies for the prosecution of crime, as money laundering or terrorism. As mentioned above, the principle of purpose specification constitutes one of the main safeguards of the European data protection system. The processing should be perfectly transparent. There can be no collection of data without prior definition of the purpose which the data subject should be informed of and it must be clear who the possible addressees of the data collected are. Further processing of personal data for law enforcement purposes appear contrary to these fundamental principles and thus should be subject to the proportionality test, which means that only when the processing of personal data is strictly needed for achieving the purpose and when there is no other way to achieve it, the processing can be carried out. The democratic debate plays here a fundamental role in defining the acceptable exemptions the purpose specification principle can be subject to.

Furthermore, the issue of the accuracy of the data received from third parties, either private or public, and irrespective of the purposes for which they have been collected is particularly sensitive in the field of police cooperation. An important part of the information collected does not necessarily reflect the reality. Rumours and witness statements play an important role in police investigation. In order to assess this specific issue, the actual Draft Decision on data protection in the third pillar compels law enforcement authorities to verify the accuracy of the data as far as practicable, before they are transmitted or made available[72].

4.5 International police cooperation

In the last years, international police cooperation has substantially increased. The absence of binding international rules and practices in this field, however, and "the processing of personal data from different sources on an unprecedented scale"[73] creates uncertainties as regards the accuracy of the personal data received from law enforcement authorities of third countries which have not adopted the same practices as Europe.

European data protection legislation provides a high level of protection that is not always ensured when personal data are processed outside the European Union. The transfer of personal data to countries that do not ensure the same level of protection can be problematic, as the safeguards established at European level are not always guaranteed in the country of destination. The

[71] Surveillance Society Network, A report on surveillance society, September 2006, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

[72] Article 9 of Draft Decision on data protection in the third pillar

[73] op. cit, fn. 4.

question here remains whether the solution adopted by the data protection directive, compelling third countries to ensure an adequate level of protection[74], can be transposed as such to the third pillar. In this field, the PNR agreement provides a valuable example. This agreement was made in compliance with the data protection directive, in order to guarantee the protection of the personal data of air travellers collected in Europe, once they were transferred to the United States for public safety and national security purposes. Even if the agreement managed to ensure a series of guarantees, as for instance, certain limitation of the personal data transferred, it received criticism from the Article 29 Working Party[75], the European Parliament and the civil society. It was argued that the agreement did not comply with European data protection principles as regards the purpose of the transfers, the principle of proportionality relative to personal data to be transferred, as well as to the time of the transfer of the data and the retention period, the processing of sensitive data, the strict control on further transfers to other Government or Foreign Authorities, or the guarantees for and rights of data subjects, etc.[76] The agreement[77] taken in response to the decision of the European Court of Justice on PNR showed that without similar pre-existing culture of data protection, it appears difficult to guarantee the same level of protection in a country outside the European Union, as the proportionality test is not carried out in the same way.

The current absence of uniform rules in the European Union can lead to the pessimistic prognostic of Ben Hayles that "if and when the EU does introduce rules on data protection in the police sector, they are likely, in the current context of law enforcement 'globalization', to meet a very low standard"[78]. The European Union should therefore take a strong position in the defence of data protection rights, similar to the one taken in the First Pillar, in order to impose a high standard in international negotiations. Moreover, as underlined by the European Data Protection Supervisor, it will be very difficult for the EU to defend a high level of protection in international scene if it has not doted itself with a specific framework with such level[79].

5. Conclusion

Establishing a coherent, consistent and effective data protection framework in the Third Pillar constitutes a real challenge for the European Union. Not only it has to find a balance between the data protection right and public order, which should satisfy every national concept and culture, but it also has to face the heterogeneous patchwork of national law enforcement authorities, their historical distrust and lack of common culture of data protection. The initiative of the Council of Europe through its Programme "Police and Human Rights" aiming to raise awareness about human rights standards in policing organisations throughout Europe is significant. The differences have emerged from the difficult negotiations taking place around the draft decision on data protection in the third pillar and the variety of initiatives presented, each one ensuring a different approach to the balance which needs to be realised.

However, there is an urge to adopt a coherent framework in the third pillar and a common approach to the problem at European level in order to be able to face the challenge to data protection principles made by increasing collaboration between private entities and law enforcement authorities because of the fight against organised crime. Further processing of

[74] See Chapter 4 of the data protection directive
[75] See for instance, Working Party 29, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)
[76] ibid
[77] Council of Europe, Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, 11.10.2006, 13216/06 (JAI 466)
[78] op. cit, fn. 4.
[79] Hustinx P., Intervention at the European Parliament public seminar on an efficient and accountable police cooperation in the EU: the way forward, Brussels, 18 December 2006.

personal data infringing the main data protection rule of purpose specification and previous information to the data subject are becoming more common. A comprehensive framework in the Third Pillar establishing a high level of protection of the data subject, as in the First Pillar needs to be agreed upon in order to give legal certainty to the processing of personal data and enable the European Union to speak as one voice and to impose a high level of protection on the international scene.