NOTE

DIRECTORATE GENERAL INTERNAL POLICIES OF THE UNION

EUROPEAN PARLIAMENT

Policy Department C
Citizens' Rights and Constitutional Affairs

DATA PROTECTION IN THE AREA OF FREEDOM, SECURITY AND JUSTICE: A SYSTEM STILL TO BE FULLY DEVELOPED?

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

MARCH 2009
PE 410.692

EN

PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Directorate General Internal Policies
Policy Department C
Citizens' Rights and Constitutional Affairs

DATA PROTECTION IN THE AREA OF FREEDOM, SECURITY AND JUSTICE: A SYSTEM STILL TO BE FULLY DEVELOPED?

BRIEFING PAPER

Abstract:

Data protection is one of the main issues of the development of the European Area of Freedom, Security and Justice (AFSJ). Indeed, the introduction of measures that touch upon data protection is coupled with growing dilemmas on how to best ensure individuals' fundamental rights. Is the current legislation on data protection adequate to the challenges posed by specific technologies and specific policies? Do the main actors have the adequate powers to shape legislation and enforce controls? Do the Data Protection Framework Decision and the Lisbon Treaty offer satisfactory means to cope with present loopholes?

The scope of this briefing paper is to provide updated background information concerning data protection in the area of freedom, security and justice. In particular, addressing the previous questions should offer an opportunity to discuss present shortcomings, identify best practices and provide recommendations for possible future activities of the LIBE Committee.

Therefore, this briefing paper aims at "deconstructing" the system in order to highlight specific shortcomings and current transformations. Part One focuses on the evolution of the European data protection framework on security issues; Part Two discusses powers, competencies and potential evolution of some of the main actors; Part Three recalls current debates on key measures and technologies, and questions their consequences on AFSJ data protection. Finally, conclusions are drawn from the previous sections and recommendations are advanced

PE 410.692

This study was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (**LIBE**).

This paper is published in the following languages: EN, FR.

Authors: **Paul De Hert** and **Rocco Bellanova**

Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS)

Manuscript completed in **March 2009**

Copies can be obtained through:

Mr Alessandro DAVOLI
Administrator Policy Department C
Tel: 32 2 2832207
Fax: 32 2 2832365
E-mail: alessandro.davoli@europarl.europa.eu

Information on **DG IPOL publications**:

http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

http://www.ipolnet.ep.parl.union.eu/ipolnet/cms/pid/438

Brussels, European Parliament

DATA PROTECTION IN THE AREA OF FREEDOM, SECURITY AND JUSTICE: A SYSTEM STILL TO BE FULLY DEVELOPED?

TABLE OF CONTENTS

INTRODUCTION: MULTIPLE CHALLENGES IN A TRANSITION CONTEXT

Maintaining and developing the European Union (EU) as an Area of Freedom, Security and Justice (AFSJ), is among the main objectives stated by the Treaty of the European Union (EU)([1]). Within this area, "the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime" (art.2 TEU). Therefore, the set up of AFSJ covers multiple fields and policies, pertaining to both the so-called first and third pillar([2]), and, within a context of increasing reliance on data, has a clear impact on the fundamental rights of individuals. Thus, data protection in AFSJ appears a crucial and sensitive issue. It is sensitive because AFSJ related measures might have important consequences on individuals' lives, and it is crucial because of the growing importance of AFSJ along national, European and international layers.

While the vision of the Future Group Report confirms the growing relevance of personal data in AFSJ (Future Group 2008), several policies proposed or adopted within the AFSJ have already raised harsh criticism, for their concrete or potential impact on data protection (Cf. i.a. Bunyan 2008). Furthermore, the cross-pillar nature of AFSJ, and thus the polyphony of decision-making systems and scattered responsibilities, implies and fosters limitations and fragmentations to data protection. This is especially the case when dealing with third pillar measures and instruments. Among the shortcomings frequently highlighted there are: lack of transparency and democratic debates; opaque understanding of the efficiency and purposes; limited safeguards against abuse and surveillance.

This briefing paper relies on the assumption that an effective data protection in AFSJ should be better understood not just as a mere patchwork of data protection provisions, but as a system, composed by legal frames, actors, policies and technologies, that still need to be fully developed. Furthermore, the context in which it operates is dealing with multiple transitions: the re-discussion of data protection community legislation([3]); the adoption of the first framework of data protection in the third pillar([4]); the possible entry into force of the Lisbon Treaty; the move towards a transatlantic agreement on data protection([5]), etc. The AFSJ data protection system appears also challenged by the growing internationalisation of data flows; the spreading of techniques such as data mining and profiling and a scattered distribution of decision-making powers.

Therefore, this Briefing Paper aims at "deconstructing" the system in order to highlight specific shortcomings and current transformations. Part One focuses on the evolution of the European data protection framework on security issues; Part Two discusses powers, competencies and potential evolution of some of the main actors; Part Three recalls current debates on key measures and technologies, and questions their consequences on AFSJ data protection. Finally, conclusions are drawn from the previous sections and recommendations are advanced.

---

[1] Art.2 para.4 Treaty of the European Union (TEU).

[2] Within the scope of TEU, AFSJ covers the policies of Title VI "Provisions on Police and Judicial Cooperation in Criminal Matters", the so-called third pillar. Within the Treaty establishing the European Community (TEC), it is the Title IV "Visa, Asylum, Immigration and other Policies related to Free Movement of Persons" explicitly links the adoption of its policies to the progressive establishment of AFSJ, cf.61 TEC.

[3] While the e-Privacy Directive is already under legislative re-discussion, the Commission has launched preliminary discussions on possible reform of the Data Protection Directive. Cf. European Data Protection Supervisor, *Strategic Challenges for Data Protection in Europe*, 9th Data Protection Conference 2008, Berlin, 6 May 2008.

[4] The Framework Decision on Data Protection, cf. Part One below.

[5] Cf. Council 2008, EDPS 2008b, and extensively De Hert & Bellanova 2008.

PART ONE: THE EVOLUTION OF THE EUROPEAN DATA PROTECTION FRAME ON SECURITY ISSUES

From an AFSJ perspective, there is not a harmonised and comprehensive legal framework covering data protection. Instead, there is a sort of living puzzle, made of a continuously increasing number of international conventions, bilateral agreements, community instruments, *ad hoc* provisions, and relevant cases-law.

Within this context, the main novelty is the recently adopted Data Protection Framework Decision, a so-called third pillar instrument. Further and positive developments are also supposed to come with the entry into force of the Lisbon Treaty.

1. Main existing legal instruments and relative shortcomings and limitations: floating between international and Community law

1.1. Data protection in AFSJ: a patchwork of measures

Protection of individual privacy and of personal data in Europe is based on several instruments of both international and Community law. Privacy protection is mainly relying on article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedom (ECHR)([6]) and on article 7 of the Charter of Fundamental Rights of the European Union([7]). Article 8 ECHR, and the related case-law of the European Court of Human Rights (ECtHR), contributes also to guarantee data protection (Cf. Part Three and De Hert 2005), together with: Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the movement of such data (Data Protection Directive)([8]); Directive 2002/58/EC on privacy and electronic communications([9]); Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)([10]), and article 8 of the Charter of Fundamental Rights([11]).

In order to understand the current state of play of data protection in AFSJ, and thus assess potential limits and shortcomings, it is important to focus on two of these instruments: (i) the Data Protection Directive and (ii) the Convention 108.

---

[6] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, 4 November 1950. Article 8 "Right to respect for private and family life", states: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

[7] Charter of Fundamental Rights of the European Union, OJ C364/1, 18.12.2000, adopted in Strasbourg on 12 December 2007 in Strasbourg. Article 7 "Respect for private and family life" states: "Everyone has the right to respect for his or her private and family life, home and communications".

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 19995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.95.

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L201/37, 31.7.2002.

[10] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS no. 108, Strasbourg, 18 January 1981. Hereinafter also: Convention 108.

[11] Article 8 "Protection of personal data" states: "(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority".

i. Directive 95/46/EC, the so-called Data Protection Directive, is the main piece of legislation concerning data protection Community law. The objective of the Data Protection Directive is twofold: it both aims at protecting "the fundamental rights and freedom of natural persons, and in particular their right to privacy with respect to the processing of personal data" (art.1(1)), as well as ensuring the free flow of personal data (art.1(2)). However, it does not apply to the processing of data "in the course of an activity which falls outside the scope of Community law, such as those provided for by Title V and VI of the Treaty of the European Union and in any case to processing operations concerning public security, defence, State security (…) and the activities of the State in areas of criminal law" (art.3(2) 1st para.). The ECJ judgement on the PNR cases has further curtailed the reach of the Data Protection Directive by establishing the criterion of the primacy of the final purpose of processing over the very nature of data collection([12]). Notwithstanding such limitations, the Data Protection Directive remains a relevant reference for the development of data protection in AFSJ for at least three reasons: it covers AFSJ policies of the first pillar, such as those related to illegal immigration, visa and asylum([13]); it created two of the main actors of data protection: the national data protection authorities and the Art.29 Working Party([14]) and, finally, the definitions and principles of the directive remain the main reference of data protection provisions of other instruments.

ii. Convention 108 provides a legally binding enumeration of data protection principles: data quality (including a range of principles from the fairly and lawful collection to purpose limitation and adequate, relevant and not excessive collection – art. 5); special categories of data (art.6); data security (art.7) and data subjects' rights (art.8). Given the scope limitation of the Data Protection Directive, Convention 108 is the main reference in the fields of police and judicial cooperation. Several third-pillar instruments providing for *ad hoc* data protection provisions, use this Convention as a threshold([15]). However, also its data protection guarantees could be submitted to legitimate derogations when they are provided by law of the Contracting Party and they constitute "a necessary measure in a democratic society in the interest of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences" (art.9)([16]). Furthermore, the Convention has been drafted before the development of the massive offer and use of new information technologies such as data mining and profiling, and risks failing short in offering new safeguards from new challenges.

For the scope of the study, it is also important to underline that other *ad hoc* instruments contribute to AFSJ data protection, especially in the field of security, such as: *ad hoc* data protection rules of AFSJ instruments([17]); *ad hoc* data protection rules of EU or European agencies([18]); *ad hoc* data protection rules of international agreement on data exchange between the EU and third countries([19]); *ad hoc* data protection rules of international

[12] Cf. Paragraphs 55-59 of Joined cases C-317/04 and C-318/04.

[13] Therefore, the Data Protection Directive covers the EURODAC database and will partially cover the Schengen Information System II (SISII) and Visa Information System (VIS) databases.

[14] On the establishment of independent data protection supervisor authorities, cf. art.28 and recitals 62 and 63; on the establishment of the Art.29 Working Party, cf. artt.29 and 30 and recitals 64 and 65. On Art.29 competencies, tasks and powers, cf. Part Two. For an overview on those actors, cf. González & Paepe, 2008, pp. 131-132.

[15] Cf. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up f cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210/1, 6.8.2008 (the so-called Prüm Council Decision) as well as the EU PNR proposal (see below, Part Three).

[16] The wording of art.9 of Convention 108 echoes art. 8(2) ECHR.

[17] Prüm Council Decision and VIS.

[18] Concerning Europol: Title IV "Common Provisions on Information Processing", of Europol Convention – Consolidated Version, artt.13-25; concerning Eurojust: Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, OJ C 68/1, 19.3.2005.

[19] EU-US PNR, EU-Australia PNR, SWIFT.

agreement on data exchange between Europol and third countries([20]) and, finally, national legislations.

1.2. Three considerations on main legal instruments covering AFSJ data protection

i. As it appears from this overview, data protection in AFSJ is very scattered. The present context of increasing internationalisation of data flows and of growing use of commercial data for security purposes contributes to foster such fragmentation. The continuous recourse to partial *ad hoc* measures does not seem to offer a real solution: even if those provisions can ensure a contingent issue, in the long run they risk to just ensure some procedural safeguards and undermine the very nature of data protection.

ii. Council of Europe Convention 108 remains among the main common references of Member States when negotiating third pillar data protection provisions. Moreover, it has the added value of being free of inter-pillar limitations. However, the text has been drafted before the massive introduction of technologies such as profiling and data mining, that are becoming the backbone of most of proposed security measures([21]).

iii. Within the puzzle, there are also very positive approaches, and they have to be underlined. Among them, the new Europol data protection framework seems to offer a pragmatic and effective solution to an increased possibility of data access against more detailed data protection provisions.

2. Recent developments: addressing the loopholes? The Data Protection Framework Protection and the Lisbon Treaty

2.1. Data Protection Framework Decision (DPFD)

Finally adopted on 27 November 2008, after a three-years-period of debates and discussions([22]), the Data Protection Framework Decision([23]) is called to offer a comprehensive framework of data protection in the field of police and judicial cooperation. In fact, as mentioned above, if the AFSJ data protection is already scattered in itself because of the European pillar structure, the situation of third pillar data protection was a real jigsaw puzzle of *ad hoc* data provisions and national legislation. However, as critics have pointed out, 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. Moreover the European Parliament's amendments, that could have contributed to address some major issues, have not been integrated in the final text([24]).

---

[20] Europol has the possibility to apply two kinds of international agreement with third countries or international bodies and institutions: strategic and operational agreements. Only the latter implies exchange of personal data. Europol has concluded this kind of agreements with, among others, United States, Canada, Iceland, Switzerland and Eurojust. A full and updated list of international agreements is available at: http://www.europol.europa.eu/index.asp?page=agreements.

[21] Cf. Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data, *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee (T-PD)*, Strasbourg, 13-14 March 2008.

[22] For an overview of the main debates and the main issues at stake, cf. De Hert et al. 2008, pp. 162-169.

[23] Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 30.12.2008.

[24] European Parliament – LIBE Committee, *Report on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal*

In its press release following the adoption of the Framework Decision, the European Data Protection Supervisor advanced some critical remarks to the text adopted (EDPS 2008). The measure is seen as a "first step", because "the level of data protection achieved in the final text is not fully satisfactory"([25]).

It is important to present and discuss at least four central issues of the Framework Decision on Data Protection ([26]): (i) scope; (ii) automated individual decisions and special categories of data; (iii) National Data Protection Authorities and (iv) Transfer to third countries.

i. The scope of the Framework Decision has been restrained to data exchanged among Member States, and among Member States and authorities or information systems established on the basis of the Treaties (art.1(2)(a), (b) and (c)). Apart from the exclusion of domestic data, other two sets of data are out of the DPFD scope: data exchanged in the frame of "existing obligations ad commitments incumbent upon Member States or upon the Union by virtue of bilateral agreements with third States" (recital 38) and acts adopted on the basis of Title VI TEU that contain *ad hoc* data protection provisions (recital 39). Among the latter set are, Europol, Eurojust, Schengen Information System and Customs Information Systems acts, as well as the Prüm Decision. Such limited scope has been, and is still, one of the main *foci* of criticism, from both the European Parliament and the European Data Protection Supervisor (EDPS 2007)([27]). Such a limited scope risks to undermine the level of protection of personal data, foster divergences in the national standards and finally add complexity to the field.

ii. Given the increased relevance of profiling techniques, the issue of "automated individual decisions" (art.7) and "processing of special categories of data" are very sensitive. On these topics, the DPFD has a "yes, but…" approach: processing of sensitive data is allowed under strict necessity and if adequate safeguards are provided by national law (art.6); "automated individual decisions" are permitted if authorised by law which also lay down safeguards of data subjects' legitimate interests (art.7). In both cases, the Data Protection Directive adopted the opposite wording, establishing a general prohibition and permitting processing as an exception (art.15 on "Automated individual provisions" and art.8 on "the processing of special categories of data"), and the same does the Council of Europe Convention 108 on "Special categories of data" (art.6).

iii. The Data Protection Framework Decision states that each Member States "shall provide that one or more public authorities are responsible for advising and monitoring the application within its territory of the provisions adopted by the Member States" pursuant to [the] Framework Decision" (art.25). The DPFD specifies also certain powers of those data protection authorities: investigative powers (art.25(2)(a)); effective powers of intervention (art.25(2)(b)) and the power to engage in legal proceedings (art.25(2)(c)). As stated in recital 33, these data protection authorities should be independent. It is important to underline that even if the Data Protection Framework Decision follows the example of the Data Protection Directive, it does not set up any working party parallel to that of Directive Art.29, and contrary to the amendment proposed by the European Parliament. However, recital 34 leaves open the

---

matters [16069/2007 - C6-0010/2008 - 2005/0202(CNS)]. As discussed in a previous study (De Hert & Bellanova 2008, pp.11-13), the amendments of the European Parliament focused on six main issues: (i) scope of the Framework Decision, (ii) proportionality and purpose limitation; (iii) sensitive data; (iv) national supervisor authorities; (v) transfer of data to private sector and (vi) transfer to third countries.

[25] EDPS 2008. The title of the Press Release is very explicit in this sense: 'EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step".

[26] For a more detailed analysis of the text and the provisions of the DPFD, cf. De Hert & Bellanova 2008, pp. 9-13.

[27] "In particular, I regret that the Framework Decision only covers police and judicial data exchange between Member States, EU authorities and systems, and does not include domestic data", EDPS 2008c.

possibility to entrust the already established data protection authorities with the new responsibilities. As discussed below in Part Two, in that case, a certain degree of coordination and harmonization could be assured through existing channels of cooperation.

iv. Finally, among the main shortcomings of DPFD, there are the rules on the "Transfer to competent authorities in third States or to international bodies" (art.13). The Framework Decision defines four criteria of transmission, linked to the principle of purpose limitation; quality of the recipient; prior consent of the originally transmitting Member State and adequate level of protection (art.13(1)). However, the latter criteria is weakened by three major derogations: "legitimate specific interests of the data subjects"; "legitimate prevailing interests, especially important public interests" or "the third State or receiving international body provides safeguards which are deemed adequate by the Member States concerned according to its national laws" (art.13(3)). All these criteria leave a huge margin of appreciation to the governments, especially because the criteria on which assess the level of adequacy remain quite vague (art.13(4)).

2.2. Lisbon Treaty

When the Lisbon Treaty, signed on 13 December 2007, will enter into force, it could offer a stronger basis for the development of a clearer and more effective data protection system. Two sets of reforms might have a major impact in the data protection in AFSJ: (i) a strengthened recognition of the right of data protection, and (ii) a different distribution of decision-making powers.

i. The new Treaty of the Functioning of the European Union (TFEU) provides for a general provision on data protection: art.16 TFEU. In fact, this article goes far beyond the pure rewording of art.286 TEC, it also states that "[e]veryone has the right to the protection of personal data concerning them" (art.16(1) TFEU). Furthermore, it indicates the use of the "ordinary legislative procedure" in laying down rules on the protection of personal data processed, among others, by Member States "when carrying out activities which fall within the scope of Union law, and the rules relating the free movement of such data" (art.16(2) TFEU). Finally, as pointed out by Scirocco (2008): "the 'constitutional' need for rules on data protection and for their independent supervision are enshrined in primary law for personal data processed not only by European Union institutions, but also by Member States". Such a strengthening of the recognition of the right of data protection is fostered also by article 6 of the new Treaty of the European Union (TEU-L). It recognises the rights and freedoms set out in the Charter of Fundamental Rights of the European Union (art.6 TEU-L) and provides for the accession of the Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms (art.6 TEU-L).

ii. The second set of reforms provides for a different distribution of decision-making powers. Given the trans-pillar nature of AFSJ and its policies, the collapse of the pillars' structure, with the inclusion of Title V on AFSJ in the TFEU (artt.67-89 TFEU), would be a major development in the field. Title V incorporates also third-pillar policies such as a police cooperation (artt.87-89 TFEU) and judicial cooperation in criminal matters (artt.82-86 TFEU) where data exchange is a main issue([28]). Furthermore, as it is the case in art.16(2) TEU-L, the "ordinary legislative procedure"

[28] Chapter 5 Police cooperation of the Title V TFEU explicitly indicates the "collection, storage, processing analysis and exchange of relevant information" among the main measures of police cooperation between Member States' competent authorities (art.87(2)(a)) and the main tasks of Europol (art.88(2)(a)).

generally applies([29]). This procedure (art.294 TFEU) is analogous to the co-decision decision-making. Its impact is important on data protection in AFSJ: on the one side offers to the European Parliament more powers than the mere consultation on third-pillar policies, and on the other, it could limit the "race to the lowest common denominator" by introducing qualified majority voting in the Council (Cf. Scirocco 2008)([30]). Given the increasing "internationalisation" of data access and flows, and the relevance of international agreements on anti-terrorism and police cooperation, the introduction of the "ordinary legislative procedure" has a major impact on AFSJ data protection because it guarantees, on the basis of art.218(5)(V), the need for European Parliament's consent in the conclusion of international agreements.

2.3. Two considerations on the DPFD and the Lisbon Treaty

i. The Data Protection Framework Decision is not satisfying: too many flows risk to prejudice its very purpose of providing a "high level of protection of the fundamental rights and freedoms of natural persons" (art.1(1)DPFD). Instead of bringing simplicity, it appears to foster complexity in the AFSJ data protection puzzle. Moreover, it does neither adequately address new technologies, nor offer solid ground to ensure data protection in flows towards third countries. Finally, the inclusion of art.1(4) on "essential national security interests and specific intelligence activities" poses a question mark on its very utility([31]).

ii. On the contrary, the entry into force of the Lisbon Treaty will bring very positive, and needed, inputs and *stimuli* for the AFSJ data protection system. However, the still existing uncertainty on the timing and modus of entry into force creates doubts on the effectiveness of AFSJ's work on data protection. Furthermore, the main impacts are "derivative", and its mere entry into force will not modify the entire picture in one step, there will still be the need for amending or modifying the Data Protection Directive and for repealing the DPFD.

PART TWO: THE MAIN ACTORS OF DATA PROTECTION: TOWARDS INCREASED POWERS?

The panorama of actors dealing with data protection is at least as vast as its legislative panorama. It ranges from independent data protection authorities and officers, to legislative actors that establish primary legislation on data protection. It is also important to recall the international level: international organisations, such the Organisation for Economic Co-operation and Development (OECD)([32]) and the United Nations([33]); as well as third countries, such as the United States, enforcing measures touching European citizens' personal data([34]).

---

[29] Concerning the extension of the "ordinary legislative procedure" under Title V TFEU, cf. Chapter 2 Policies on Border Checks, Asylum, and Immigration: artt.77(2), 78(2) and 79(2); Chapter 3 Judicial Cooperation in Civil Matters: art.81(2); Chapter 4 Judicial Cooperation in Criminal Matters: artt.82(2), 83(1) and 84; Chapter 5 Police Cooperation artt.87(2) and 88(2).

[30] On the impact of the Lisbon Treaty on the European Parliament, cf. Part Two.

[31] Art.1(4) DPFD states: "[t]his Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security".

[32] Organisation for Economic Co-operation and Development – OECD, *Recommendation of the Council Concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, 23 September 1980.

[33] United Nations – UN, *United Nations Guidelines Concerning Computerized Personal Data Files*, adopted by the General Assembly on 14 December 1990.

[34] Among those measures: the Passenger Name Record agreement and the relative exchange of Letters, as well as the recently introduced Electronic System of Travel Authorization (ESTA). On PNR, cf. 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

The relevance of the Council of Europe has been already discussed in Part One. Among the actors it is necessary to also mention the national, international and European courts ([35]). Finally, non-institutional actors, ranging from civil society ([36]) and individuals ([37]) to private sector([38]), should be increasingly taken into account.

However, when it comes to AFSJ, and in particular to security policies, not all these actors enjoy the same powers and competencies. As mentioned in Part One, all the legislations covering data protection imply exceptions limiting these rights, especially in security management. Next to that, third pillar limitations potentially marginalise even crucial actors such the European Parliament and independent data protection authorities. Nevertheless, their current and prospective roles deserve a special attention within the scope of the analysis of AFSJ data protection.

3. The European Parliament and the new role under the Lisbon Treaty

3.1. Present role of the European Parliament in AFSJ data protection

At present, the European Parliament role to ensure a high level of data protection in the AFSJ is limited by two overlapping factors. First, AFSJ policies involving data access (and thus data protection) are both first and third pillars, and even increasingly cross-pillar in nature. Secondly, the European Parliament enjoys very limited powers on third pillar decision-making.

Legislative initiatives under Title VI of the Treaty of the European Union (TEU), "Provisions on Police and Judicial Cooperation in Criminal Matters", are forced to undergo a process of decision making that leaves to the European Parliament a mere power of consultation. In fact, the adoption of instruments such as framework decisions (art.34(2)(b) TEU), Council decisions (art.34(2)(c)) and conventions (art.34(2)(d)) imply only the consultation of the European Parliament (art.39(1)). Furthermore, the 2006 ECJ judgement on PNR has contributed to further marginalise the position of the EP on decision-making concerning use of commercial data (cf. the decision to use a third pillar instrument for the proposal on EU PNR system). Finally, the European Parliament has also a power of consultation in case of international agreements.

Homeland Security (DS) (2007 PNR Agreement), OJ L284/18, 4.8.2007. On ESTA, cf. US Federal Register / Vol.73, No.111/ Monday, June 9, 2008 / Rules and Regulations, p. 32440, and De Hert & Bellanova 2008, pp. 22-25.

[35] The Online Searching Judgment of the German Federal Constitutional Court of February 2008 is a clear example of the role played by national courts in data protection. In fact, this judgement establishes a new "fundamental right to confidentiality and integrity of information technology system", cf. Hornung, G., *The Federal Constitutional Court and the Online Searching Judgement of February 27th 2008*, intervention at the Computers, Privacy and Data Protection conference 2009, available at: www.cpdpconferences.org/Resources/HornungGerrit.pdf. The relevance of the European Court of Human Rights is discussed in Part Three. The ECJ judgements on PNR and Data Retention Directive highlight the role of the European Court of Justice, cf. Joined Cases C-317 and C-318/04 and Case C-301/06.

[36] Notwithstanding the EU civil society panorama shows a certain lack of activism if compared to the United Sates, also in the EU are emerging NGOs focusing, or at least dealing, with privacy and data protection. Among them: the German Data Retention Working Group, that had brought to the German Federal Constitutional Court the German law implementing the Data Retention Directive; as well as the European Digital Rights (EDRI) pooling privacy and civil rights organisation from different countries in Europe.

[37] For example the applicants that bring before the courts infringements of their rights to privacy and data protection, cf. the case of Mr. S. and Mr. Marper, Part Three.

[38] AFSJ policies can engage private companies by imposing them obligations (the transmission of PNR) or by creating economic opportunity (need for information technology tools).

However, in case such as the establishment of the Visa Information System, the European Parliament has succeeded in partially curtailing the pillars' limitations by linking two different instruments to the same negotiations. Furthermore, the ECJ judgement on the legal basis of the Data Retention Directive could offer a pragmatic approach to decision-making on policies concerning access to data collected by private parties.
Notwithstanding a relative weak position, the European Parliament has frequently raised its concerns on data protection in AFSJ, and adopted positions showing a certain consensus on some important topics such as the EU-US PNR agreement and the Data Protection Framework Decision. It has also frequently advanced the request to extend the "passerelle" provision of the Treaty of the European Union (art.42) to other fields of AFSJ, in order to increase decision-making powers.

3.2. European Parliament new powers under the Lisbon Treaty

Apart from the potential improvements to AFSJ data protection discussed above (Cf. Part One), the entry into force of the Lisbon Treaty would further contribute to a more coherent and higher level of data protection in AFSJ through a consistent increase of European Parliament powers. In fact, with the collapse of the pillars' structure and the generalisation of the 'ordinary legislative procedure', the increased role of the EP in decision-making could implicitly provide three main *stimuli* to foster data protection in the AFSJ.

i. According to art.16(2) TFEU, the European Parliament might have the last word on data protection legal instruments, including data protection frames related to justice and home affairs. This would be particularly important if the Data Protection Framework Decision will be repealed or amended, or if legislation will be proposed on specific techniques and technologies, such as profiling.

ii. According to artt.87(2)(a) and 88(2)(b), the European Parliament could strongly influence the set up of security measures based on data access, whether framed as police cooperation or Europol tasks. This kind of influence is potentially twofold, because on the one side it could contribute to define security measures that are privacy and data protection friendly in themselves. On the other side, the European Parliament could ensure the eventual integration of specific provisions aiming at reinforcing the protection of special categories of data, and/or the recourse to less intrusive techniques and technologies.

iii. Finally, on the basis of the previously quoted articles (comporting "ordinary legislative procedure") and the wording of art.218(6)(V), the European Parliament might have a final say in the conclusion of international treaties covering both data protection and data access for security purposes. This power seems particularly important in the context of the "internationalisation" of data access, and in the light of the past experience of PNR and SWIFT agreements, and the possible move towards data protection agreement with the US.

3.3. Two considerations on EP new role

i. As discussed above, the entry into force of the Lisbon Treaty is surrounded by a certain degree of uncertainty. Besides this partial deadlock, the AFSJ remains a very dynamic area, especially with respect to data access and processing. A series of policy issues and options are already under discussions, such as the proposal for a EU PNR system, the introduction of a European Entry-Exit System and Electronic System of Travel Authorization, as well as the possible conclusion of a transatlantic data protection agreement covering data exchanges for security purposes. All those issues relate to data protection in AFSJ, and they need to be addressed even in case of delayed entry into force of the Lisbon Treaty.

ii. The adoption of the Prüm Treaty and its partial adoption within the EU framework, as well as the conclusion of bilateral agreements between the US and Member States appear to confirm the difficult relation among the national, European and international

layers. Such layering frequently comports a decrease of powers of legislative institutions, in favour of executive agencies and ministries (Hosein 2004 and Bellanova forthcoming). The negative effects implicit in this re-distribution of decision-making powers could be, partially, addressed by a further strengthening of coordination among parliaments. Not only the European Parliament offers the ideal forum, but he could also offer a more comprehensive view of the issues at stake. Furthermore, such strengthened coordination could also contribute to pave the way to the prospective Lisbon regime, where national parliaments will play an increased role in AFSJ (art.12(c) TEU-L).

4. Independent Data Protection Authorities: the European Data Protection Supervisor and the Working Group Art. 29

4.1. European Data Protection Supervisor (EDPS)

The first European Data Protection Supervisor took office only few years ago, on January 2004, but should be considered one of the main actors in the field of data protection. The legal basis of the European Data Protection Supervisor are article 286(2) of the Treaty of European Community([39]) and art. 41 of Regulation No. 45/2001/EC([40]). In fact, while art. 286 TEC requires the extension of data protection rules to Community institutions and the establishment of a relative independent supervisory body, Regulation 45 introduces both.

The duties of the EDPS imply a wide range of activities (art.46 Reg.) that could be clustered in three main tasks: (i) supervision; (ii) consultation and (iii) cooperation([41]). From an AFSJ perspective, they all permit to the EDPS to claim a role of main actor in the field.

i. In fact, even if supervision duties cover exclusively Community institutions and body, they also grant the EDPS the supervision of the EURODAC central unit as well as of foreseen large-scale databases such as the SIS II and the VIS.

ii. In practice, the consultation task has been understood by the EDPS as covering a larger set of policies than those covered by supervision (Hijmans 2006, p. 1321). Consultation implies monitoring of legislative proposals and technological developments as well as advising Community institutions and bodies. Given the possibility to advise on his own initiative, and the effective use of this role on third-pillar policies, the EDPS has the possibility to intervene on the policy debates, providing his expertise. The advisory role of the EDPS has been further strengthened by the order of the ECJ to grant the EDPS the possibility to intervene on the PNR case (Hijmans 2006, pp. 1321-1322).

iii. Finally, the cooperation tasks are based on art.46(f) and (g) of the Regulation 45. The EDPS has thus the duty to cooperate with both national supervisory authorities (art.46(f)(i)) and with "the supervisory data protection bodies established under Title VI of the Treaty of the European Union" (art.46(f)(ii)) as well as to participate in the activities of the Art.29 WP. Those duties bring the EPDS in a strategically pivotal role, in between not only national and European layers, but also different policies and pillars.

The entry into force of the Lisbon Treaty would have no impact on the legal status of the EDPS. However, the collapse of the pillars' system and the introduction of the "ordinary

[39] Art.286(2) TEC states: "Before [1 January 1999], the Council (…) shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate".

[40] Regulation No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L8/1, 12.1.2001. Hereinafter: Regulation 45 or Reg. As argued by Himans (2006, pp. 1324-1332), the EDPS is not, *stricto sensu*, a Community institution, neither is an agency, or a regulator, or an Ombudsman or a judicial body. However, the EDPS shares some of the specificities of each of these institutions, making of it a singular entity in the European panorama.

[41] On such "clustering", cf. Hijmans 2006.

legislative procedure" on the entire AFSJ, could indirectly reinforce its position and its relevance. In fact, on the one side, the EDPS has already contributed to give visibility to data protection (Hijmans 2006) and thus, the wording of article 16 TFEU should even reinforce his "symbolic" power. On the other side, EDPS' opinions and recommendations are generally not only welcomed but also integrated into the European Parliament own positions. Thus, if this special relation continues, the new powers of the European Parliament could indirectly foster EDPS options.

4.2. Article 29 Working Party (Art.29 WP)

The Article 29 Working Party could be considered a "derivative" body (González & Paepe 2008, p. 132), with an independent advisory status (art.29(1) Data Protection Directive). It is a "derivative" body because, as mentioned in Part One, it has been established by the Data Protection Directive, and is composed of "a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission" (art.29(2)).

Notwithstanding the "first pillar nature", and its implicit limits, certainly downsizes the potential impact of Art.29 WP in data protection of AFSJ, it should be fully considered an important actor for third pillar policies. This is due to at least two sets of factors, grounded in some of its competencies and tasks as well as to its "derivative" nature.

i. Very often, national data protection authorities have competencies covering also justice and home affairs, and thus the possibility to influence their governments, that are the main actors at EU level of third pillars policy-making([42]). The "derivative" nature of the Working Party offers a pivotal role, in-between national and European layers, fostering "vertical and horizontal" co-operation([43]). Even if the Data Protection Framework Decision does not provide for the establishment of a parallel Working Party, the Art.29 WP already potentially offers a similar, unofficial, socialisation platform([44]).
ii. Art.29 WP "shall" deliver to the Commission an opinion on the level of protection not only in the Community but also in third countries (art.30(1)(b)). Furthermore, it may "on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data" (art.30(3)). On the one side, despite the pillars' limits on competencies, the Art.29 WP members have made a "generous" interpretation of the scope of their recommendations (González & Paepe 2008) ([45]). On the other side, given the increasing internationalisation of data flows and the related issues of adequate level of protection, the position of the Art.29WP could indirectly influence the discussions even on third pillar international agreements.

[42] As discussed above in Part One, such powers over third pillar data protection are now provided also by the Framework Decision on Data Protection, and especially art.25.

[43] Furthermore, as González and Paepe state: "the Art. 29 WP has functioned as an instrument allowing the supervising authorities *as a community* to voice out and defend their own agenda on EU data protection in general at EC level" (González & Paepe, 2008, p. 132).

[44] Such ability to bridge and co-operate, as well as the will to maintain a collective supervision of the third pillar policies are confirmed by the set up of the Working Party of Police and Justice (WPPJ), a sub-group of the Spring Conference of the Data Protection Authorities. Its mandate is to "monitor the developments in data protection as for the so-called Third Pillar" (WPPJ, 2008, p. 1).

[45] For example, despite the third pillar nature of the 2007 US-EU PNR agreement and of the Commission Proposal on a EU PNR system, the Art.29 WP has published an opinion on each topic. Cf: Opinion 5/2007 (WP138) on the follow-up agreement between the European Union and the United States of America on the processing of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007; and Joint Opinion (WP145) on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 – November 2007.

As in the case of the EDPS, the entry into force of the Lisbon Treaty would not have, in itself, a major impact on the role of Art.29 WP. In fact, given an already established presence even on third pillar fields, the collapse of the pillars' structure could contribute to further legitimise existing activities, such as informal supervision and opinions and recommendations delivery. Only the repeal of the Framework Decision on Data Protection and the amendment of art.3(2) of the Data Protection Directive can offer an occasion to modify and increase its powers.

4.3. Two remarks on supervision authorities

i. The Art.29 WP has proved a certain ability to maintain a strong position in AFSJ, even despite the potential limits drawn by art.3(2) Data Protection Directive, especially by cooperating and working on multiple layers and contexts. The EDPS has integrated such kind of cooperation and proved to be influential with the European Parliament. It is worth to note the function of visibility provided by the appointment of a European Data Protection Supervisor. As Hijmans says: "it is important that the EDPS is visible, or in other words gives a face to data protection. This makes it difficult to ignore that data protection is a public interest that has to be taken into account" (Hijmans 2006, p.1341).

ii. National data protection authorities are among the main actors when it comes to the implementation of security measures affecting data protection. It is important to remark the ability and the will of those authorities and of the Art.29 WP to maintain and foster coordination on this field by the creation of the Working Party on Police and Justice([46]). Finally, as discussed below, national supervisor authorities might be the "recipient" of specific powers provided as complementary data protection measures in security policies (cf. EU PNR proposal discussed in Part Three). However, such potential benefits should be assessed within a context of frequently limited resources.

PART THREE: FUTURE AND PRESENT DILEMMAS FOR DATA PROTECTION: TECHNOLOGIES AND SECURITY POLICIES

The content of the Future Group Report highlights a strong appeal of ever-increasing use of technologies and personal data as the solution to several AFSJ challenges([47]). Such a trend towards increased use of personal data, especially processing through highly technological tools such as data mining, is already evident. Policies allowing such kind of processing have been already adopted within certain Member States and close partners such as US and Australia. Furthermore, EU-wide measures, generally echoing parallel US existing measures, are currently discussed. In sum, most of the main future dilemmas of AFSJ data protection are already posed and need solutions.

At present, three, and partially overlapping, shortcomings appear particularly relevant: scattered and dispersed decision-making([48]); growing use of profiling techniques and

[46] Cf. footnote nº44.

[47] According to the report, "[d]atabases and new technologies will play a central role in further developing Home Affairs policies in the areas of border management, migration, the fight against organised crime and terrorism", and "[e]ven if technology can never completely replace the human factor, technological progress can provide the necessary means to optimise mobility, security and privacy simultaneously" (Future Group 2008, p.18).

[48] As Husein points out, several policies affecting civil rights are proposed, modelled and adopted by national governments within the less reluctant international *fora*, in order to avoid or limit national debates that could stop the adoption of the measures (Hosein 2004). With a similar approach, Balzacq et al. underline the use of a two-level game strategy of some EU Member States in order to develop international law to be, later, implemented within the EU frame (Balzacq et al. 2006).

technologies([49]); and recourse to secret surveillance and large-scale data retention([50]). Therefore, it is particularly important, for the purpose of this study, to analyse some of those dilemmas, concerning both technologies and measures.

On the one side, the European Court of Human Rights has recently discussed two cases touching upon very sensitive issues: use of data mining in secrete surveillance programs, and massive retention of sensitive information of not-convicted individuals. On the other side, the proposed EU PNR system appear to condensate all the debates on democratic decision making and policy laundering, proportionality and efficiency, profiling and possible discrimination.

5. Data mining and data retention: the Liberty and the Marper ECHR cases

5.1. Liberty: secret surveillance and data mining

The case of Liberty and others v. the United Kingdom([51]) concerns a program of secret surveillance, involving data mining, of a massive amount of national and international public communications, operated by an Electronic Test Facility in the United Kingdom (UK). Therefore, this case touches upon sensitive issues of data protection, internal security and recourse to data mining and profiling. It could provide an important insight on the debates surrounding data protection and security measures based on data mining. Below: (i) the facts and the alleged violation of art.8 ECHR; (ii) the position of the UK Government and, (iii) the conclusions of the ECtHR.

i. The Electronic Test Facility was alleged to be able to intercept 10.000 simultaneous telephone channels, covering much of Ireland's telecommunications traffic (§5 ECtHR 2008a). The applicants were three civil liberties organisations: Liberty (based in London), British Irish Rights Watch and Irish council for Civil Liberties (both based in Dublin). They alleged the continuous use of this massive and secrete surveillance measure between 1990 and 1997, period in which they "were in regular telephone contact with each other and also providing, *inter alia*, legal advice to those who sought their assistance" (§5). Therefore, they alleged that their "telephone, facsimile, e-mail and data communications between them were intercepted (…), including legally privileged and confidential material" (§42). Moreover, given the secret nature of the program and the procedure adopted to capture and sift communications (§43), the applicants contented that the safeguards for individuals were not adequate, and that the UK measure constituted an interference with the right of privacy (art.8(1) ECHR) that was not "in accordance with law", as in requested by art.8(2) ECHR, in particular because the UK legislation breached the requirements of foreseeability (§44 and 45). Finally, the applicants contested the legitimate aim of the interference and the criteria of proportionality of the measure (§46).
ii. The UK Government argued that not only there were enough guarantees and safeguards in place in the process itself (§50 and 51), but also that "the provisions of primary legislation were (…) sufficient to provide reasonable notice to individuals to the degree required in this particular context, and provided adequate protection against arbitrary interference" (§52).
iii. The ECtHR conclusion was that safeguards provided by the UK Government were not sufficient and that the interference with the applicants' rights was not in "accordance with law" (§69). In fact, "the Court does not consider that the domestic law at the

[49] For an overview of the growing use of profiling in Europe, and the challenges that it raises, cf. Hildebrandt & Gutwirth 2008.
[50] Cf. below the ECtHR Liberty and Marper cases; for a discussion of different approaches to secret data mining in the EU and US, cf. De Hert & Bellanova 2008, pp.21-22.
[51] European Court of Human Rights – ECtHR, *Case of Liberty and others versus United Kingdom*, Application no. 58243/00, Strasbourg, 1st July 2008.

relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material" (§69).

The ECtHR conclusion seems very important for the development of the AFSJ: it implicitly calls for an increased use of a mix of transparency and opacity tools([52]) in the framing of security measures, in order to avoid secret data mining programs and put under control the official ones. This case contributes also to shape a European approach to data mining, based on coupling use of new techniques with more precise data protection measures.

5.2. Marper: data retention and proportionality

The case of S. and Marper v. the United Kingdom([53]) covers the retention of biometrics' samples and profiles (DNA and fingerprints) after criminal proceedings against individuals have ended in acquittal or have been discontinued (§3 ECtHR 2008b). This judgement deserves attention because retention and processing of biometrics is one of the main issues and trends of the AFSJ development([54]). Furthermore, they are also open issues at the international level, both in the transatlantic and the wider context([55]). Furthermore, UK is managing the biggest DNA database in the world, and represents itself at the vanguard of the use of DNA comparison for law enforcement activities (cf. §111). Therefore, it is important to recall: (i) the facts and the alleged violations of art.8 ECHR; (ii) the position of the UK Government; and (iii) the conclusions of the ECtHR.

i. Both applicants, Mr. S. and Mr. Marper, were arrested in 2001, and their fingerprints and DNA samples were taken (§10 & 11). Mr. S. was a minor at the moment of the arrest, and it was acquitted some months later (§10). Mr. Marper had his case formally discontinued (§11). Both asked for the destruction of their fingerprints and DNA samples, but the police refused (§12). The same did the Administrative Court (§12), the Court of Appeal (§13) and the House of Lords (§15). The applicants not only claimed that retention of their data was an interference with their right of privacy under art.8 ECHR, but they also argued that the retention of fingerprints and DNA samples "created suspicion in respect of persons who had been acquitted" (§21). However, the House of Lords rejected both applicants' complaints (§24). Before the ECtHR, Mr. S. and Mr. Marper further argued that "the retention of fingerprints, cellular samples and DNA profiles was not justified under the second paragraph of Article 8" (§87): the purposes related to data processing were "vague and open to abuse"; procedural safeguards against misuse or abuse of the information were "insufficient" (§87); indefinite retention of biometrics of non-convicted persons could not be regarded as "necessary in a democratic society" (§88) and the retention was disproportionate (§89).

ii. Even if the Government accepted the definition of personal data for the biometrics collected, it disputed that: "their retention did not interfere with the physical and psychological integrity of the persons; nor did it breach their right to personal development, to establish and develop relationships with other human beings or the

[52] "Opacity tools protect individuals, their liberty and autonomy against state interference and also interference from other (private) actors. (…) On the contrary, transparency tools tend to regulate accepted exercise of power. Transparency tools are not prohibitive but aim at channelling, regulating and controlling legitimate powers", De Hert & Gutwirth 2008, pp. 276-277.

[53] European Court of Human Rights – ECtHR, *Case of S. and Marper versus the United Kingdom*, Application nos. 30562/04 and 30566/04, Strasbourg, 4 December 2008.

[54] Example of measures implying retention and processing of biometrics are: the Prüm Council Decision; EURODAC, SIS II and VIS.

[55] Cf. The issue of the retention of European citizens fingerprints in the US-VISIT system; the conclusion of several bilateral transatlantic agreements on DNA exchange (Bellanova forthcoming); as well as the future European obligation on third countries' nationals to provide fingerprints for the VIS.

right to self-determination" (§63). Moreover, it claimed that "the interference was necessary and proportionate for the legitimate purpose of the prevention of disorder or crime and/or the protection of the rights and freedoms of others", and the retained material was of "inestimable value in the fight against crime and terrorism and the detection of the guilty" (§90).

iii. The ECtHR judgement intervenes on the issue of the interference with art.8(1) ECHR and its proportionality assessed on the criteria of art.8(2) ECHR. On the one side, the Court "reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data" (§121). On the other side, the ECtHR "finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society" (§125).

5.3. Three considerations on the Liberty and Marper cases

i. The two cases are particularly relevant for the development of data protection in AFSJ. Firstly because they mark an important benchmarks in the use and adoption of sensitive technologies. Furthermore, if the Lisbon Treaty enters into force, the EU accession as a to the Convention will further strengthen the relevance of ECtHR judgements.

ii. Both judgments highlight the need for adequate transparency tools, able to canalize governments' and executive agencies' powers when processing personal data. Foreeseability and specific, clear safeguards are essential components of use of personal data for security reasons.

iii. Nevertheless, it seems important to affirm the need to bring back the debate on what should be allowed and what should not be allowed in the public *fora*, Notwithstanding their essential role as watchdog, courts can not offer the only occasion to re-discuss security policies that have an impact, potentially or effectively, on all individuals([56]).

6. Mobility, risk assessment and commercial data: the EU-PNR framework decision

6.1. A symbolic and practical issue

Access and process of passenger name record (PNR) are still among the main key debates surrounding the so-called post 9-11 measures. Since the adoption of the US Transportation and Security Act in November 2001, access and process of PNR have been the object of (among others): three agreements signed by EU and US([57]), one agreement signed by EU and Canada([58]) and another by EU and Australia([59]); one proposal of the European Commission

[56] It is worth to note that both cases are focusing on the application of surveillance measures to large numbers of individuals, both citizens and foreigners.

[57] 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 (DHS) (2007 PNR Agreement), OJ L204/17, 4.8.2007; cf. *in extenso*: De Hert & Bellanova 2008, pp. 31-38.

[58] Agreement between the European Community ad the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L82/15, 21.3.2006.

on a EU system([60]); one judgment of the European Court of Justice([61]); several opinions of the European Parliament, the EDPS, the Art.29 WP([62]); two reports of the House of Lords([63]). Next to that, it is worth to note that some EU Member States have adopted similar measures at national level([64]), and the EU a Directive on the access and process of APIs data([65]).

The PNR issue could be only understood within a broader, and complex, context, where it polarises both symbolic and practical issues. PNR are commercial data that contribute to mobility and whose use, access and processing, is claimed necessary by law enforcement agencies and interior ministries, as a powerful tool to fight a wide range of "security threats". On the one side they are on the forefront of a still developing concept of "internal security", strongly based on a massive use of large quantities of personal data. On the other side, the very process of those data for security purposes raises a set of practical problems ranging from the legal aspects to the effective use and value of the measure. Finally, as highlighted by the 2006 ECJ judgment, the use of PNR has been the occasion of inter-institutional debate over competencies.

6.2. The January 2009 version of the proposal: the main relevant points([66])

Several studies already offer insightful analysis of PNR issues and policies (among others, cf. Brouwer 2009). However, given the centrality of the EU PNR proposal in the development of the AFSJ, it is important to come back on its latest version, as amended after an intense period of debate under the French Presidency in the second half of 2008. Three points appear particularly relevant for the data protection in AFSJ: (i) risk assessment; (ii) data protection provisions and, (iii) transfer to third countries.

i. According to the Commission Impact Assessment accompanying the EU PNR proposal, one of the main added values of a PNR system is the possibility to carry out risk assessment on the passengers (Commission 2007b, pp. 10-12). However, the proposal still lacks a comprehensive and clear definition of risk assessment, although art.3 provides for three main types of processing: real time risk assessment (art.3(3)(a)); specific, case-by-case, processing on request of competent authorities (art.3(3)(b)) and analysis for the identification of trends and creation of new risk criteria (art.3(3)(c)). All those processes should be carried out by Member States' Passenger Information Units (PIUs), established by art.3(1). While the case-by-case process is purpose-limited to "specific investigations or prosecutions concerning a terrorist offences and serious

---

[59] Agreement between the European Union and Australia on the processing and transfer of European Union-source passenger name record (PNR) data by air carriers to the Australian customs service, OJ L213/49, 8.8.2008.

[60] Commission of the European Communities, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, Brussels, 6.11.2007.

[61] Joined cases C-317/04 and C-318/04.

[62] Among others: Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, adopted by the Article 29 Working Party on 5 December 2007 and by the Working Party on Police and Justice on 18 December 2007, WP 145, WPPJ 01/07.

[63] House of Lords 2007 & 2008.

[64] The UK pilot project Semaphore, part of the wider e-Border project, seems to be the most advanced, in terms of effective implementation, among the Member States PNR-like programs. On Semaphore, cf. http://ukba.homeoffice.gov.uk/managingborders/technology/eborders/ and House of Lords 2008, pp. 1-25 (oral evidence). According to the Commission Impact Assessment accompanying the Framework Decision proposal, France and Denmark have already enacted primary legislation on the same issue.

[65] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24, 6.8.2004.

[66] Council of the European Union, *Proposal for a Council Framework Decision on the use of Passenger Name record (PNR) for law enforcement purposes*, doc. 5618/09, Brussels, 23 January 2009.

crime", no indication is provided on the kind of processing that could be involved, neither on specific safeguards. The other two paragraphs, real-time assessment and trends analysis, highlight some of the main concerns of PNR use: how effectively risk assessment works (and thus which is the impact on individuals) and who is responsible for the definition of risk criteria. Firstly, art.3(3)(c) allows, *de facto*, PIUs to contribute to the update and creation of new risk criteria, even if it is not clear if they will be part of the list of "competent authorities" to which such activity is restricted, according to art.3(4). Who will audit such updating process? Secondly, real-time risk assessment aims at identify persons who may be involved in a terrorist offence or serious crime, by running the PNR data both against pre-determined risk criteria ad against relevant databases. The focus on "person who may be involved", and the two possibilities quoted, presumes the adoption of profile techniques. Furthermore, the use of data mining and profiling appears possible if PNR use will be in line with present use in the US, where PNR data are run by the Automatic Targeting System Passenger Module (ATS-P), a specific branch of the data-mining program ATS (DHS-Privacy Office 2008, pp. 15-18).

ii. While the Commission proposal included a generic reference to the Council Framework Decision on Data Protection as the relevant framework of data protection for PNR processing, the Council adopted the approach of multiple layers and *ad hoc* measures. In the present proposal, specific rules apply to the PNR use (artt.11-12), along with the DPFD covering transfer of data among authorities of different Member States. Specific rules are based on national laws that should correspond at least to the DPFD standards, or to Convention 108 standards. Moreover, processing of special categories of data should be coupled by a reinforced set of protections and limitations (art.11a), but the "adequate safeguards" are not explicitly defined. All the other main principles of data protection are also addressed in the text and submitted to a special framework. Among them, it is worth to note that the present text of the proposal defines a series of powers and competencies of national supervisory authorities(artt.11d(1)(b) and 11i).

iii. The provision on the "Transfer of Personal Data to Third Countries" (art.8), establishes a set of conditions, and exceptions, pretty identical to the one of the Data Protection Framework Decision. The last version of the text introduces a "case-by-case" clause of data transfer, but leaves to the Member States the decision on the satisfaction of the mentioned conditions. Furthermore, recital 21 excludes from the adequacy exams the bilateral agreement already concluded before the entry into force of the Framework Decision.

6.3. Three considerations on the EU PNR framework decision

i. According to the scarce and indirect description provided in the text, the EU PNR system might introduce a large scale, partially networked, profiling system. It is important to note that the term "profiling" is not used in the proposal, even if a series of elements go in this direction: the aim of identifying potentially risky individuals, the running of data against pre-determined risk-criteria, a highly automated process. However, as highlighted by the EDPS in his opinion, the related concerns is not just a matter of definition, but "the fact that decisions on individuals will be taken on the basis of patterns and criteria established using the data of passengers in general" (EDPS 2008a, para.22). Leaving apart the debates on the legitimacy of such measures, it is important to recall that the transparency in the set up of risks assessment criteria and the adoption of explicit safeguards and limitations is a crucial issue in definition of the quality of law (see above, section on ECtHR).

ii. Even if the present text provides for a detailed set of data protection provisions, and even multiple layers covering different parts of processing and dissemination of data, the transfer from the private sector to PIUs is still in a partial legal vacuum. This

element highlights the problematic use of commercial data for security purposes: how to ensure data accuracy, avoid loopholes in data protection and respect purpose limitations? And, in general, is it always admissible the recourse to commercial data? From a AFSJ data protection point of view, access to commercial data highlights once again all the limitation implicit in the pillars' structure.

iii. Finally, as outlined again in the European Parliament resolution (drafted by Sophie In't Veld) adopted on 20 November 2008 (EP 2008), PNR processing has still to prove its effectiveness in the fight against terrorism. Even considering PNR processing just as a piece of a larger "jigsaw puzzle" of security policies([67]), there is striking need to establish such effectiveness in order to proceed to a real assessment on proportionality. The first joint review fn the EU-US PNR agreement, as well as the following DHS Privacy Office review (DHS – Privacy Office 2008), do not offer substantial ground to assess PNR added value as anti-terrorism tool. This lack of public available evidence underlines once again the relevance and the need of open debates and transparency in decision-making covering third pillar issues.

CONCLUSIONS AND RECOMMENDATIONS

7. A not fully developed data protection framework

The Area of Freedom, Security and Justice remains a very dynamic field, covering several policies under different pillars. Such a cross pillar nature implies limits and fragmentation in the decision-making process, as well as in the reach of data protection main instruments.

Nevertheless, data protection in AFSJ is both a crucial and sensitive issue. Prospective developments in AFSJ rely on wide access to personal data, and thus not only confirming the present need for a high level of protection, but even calling for further attention.

The present legal frame of AFSJ data protection does not seem particularly well equipped to respond to present and future dilemmas. This overview has underlined that the present legal framework is too scattered and complex.

In particular, the Data Protection Framework Decision does not appear ambitious enough to harmonize, simplify and respond to growing challenges. The Lisbon Treaty might prove more useful in this sense, especially by empowering actors through a redistribution of decision-making powers and competencies.

In fact, at present, the European Parliament has not sufficient powers in the so-called third pillar and in the international dimension of AFSJ. Both fields cover increasingly relevant AFSJ policies: EU internal security and transatlantic security cooperation.

The European Data Protection Supervisor and the Art.29 Working Party have greatly succeeded in voicing their concerns, even in fields where they had more limited competencies. They have also succeeded in positioning themselves as EU data protection watchdog. Even if the adoption of the Data Protection Framework Decision or the eventual entry into force of the Lisbon Treaty will bring only minor changes on their status, their present capacities to cooperate within a multilayered context could be indirectly strengthened by renewed powers of other actors, such as the European and national parliaments.

[67] "PNR is an additional tool, additional to the API data, to the visa, to other information, the aim of which should be to fit them into a jigsaw puzzle which we then present as tools to law enforcement next to other instruments which should allow law enforcement to look at particular ways of people entering our countries", Ms. Cecilia Verkleij answering to Q149, House of Lords 2008, p. 45 (oral evidence).

Specific technologies and specific policies appear as the main challenges not only of future but also present AFSJ data protection. In particular, profiling is increasingly diffused in Member States' and third countries security legislations (UK, Germany, US, etc.); massive data retention is already in place both at national level and, soon, at EU level (establishment of SIS II and VIS). Finally, anti-terrorism and crime-fighting policies focusing on control of mobility by profiling are proposed at EU level (EU PNR system and EU ESTA).

8. Which possible ways forward? Best practices and recommendations

Given this context, the assumption of the briefing paper is that an effective data protection in AFSJ is to be understood as a system, composed by legal frames, actors, policies and technologies. Notwithstanding the fact that currently such a system is highly "polyphonic", and can only partially address present challenges, it should be highlighted that some "components" of the system is either providing forms of protection (ECtHR), or even already able to articulate multilevel cooperation (EDPS and Art.29 WP).

However, debates on the limits to be imposed on technology use and security policies should not be confined to courts. Where data protection law applies to an issue or technology, this issue is not cancelled, but at most highlighted. New technologies create power shifts, and power shifts need a political assessment. An effective data protection system is one in which data protection law and watchdogs contribute to make new developments and technologies visible (legally speaking) and thus simplify the identification of problems and potential tensions. However, they cannot completely solve problems; relevant issues should be discussed and addressed politically.

Therefore, the European Parliament has a crucial role to play, and it is, potentially, in a pivotal position. On the one side, even within the present limited powers, it can foster and voice concerns about the political choices that should be addressed in public *fora*. In fact, only within open debates, it could be made effective use of transparency and opacity tools, stopping illegitimate use of power and channelling the legitimate one (De Hert & Gutwirth 2006 & 2008). On the other side, it is in a privileged position to maintain an overview of local and international policy developments, and can attract national parliaments attention on the most relevant issues. Therefore, European Parliament, as well as national parliaments, should pay increasing attention to data protection issues, because they are the best entitled to re-balancing powers.

The present shortcomings linked to the scattered distribution of decision-making powers strongly endanger the functioning of the system, and they risk reducing problems only to a "technical" data protection level. Such a context calls for a further integrated system, based on sustained relations among the "political" components of the system. This seems particularly important in the present vague of reinforcement of executive powers in the field of security.

In front of the rapid introduction of specific security policies, a different re-distribution of decision-making powers seems particularly needed. In fact, on the one side, the European Parliament has already opened important dossiers such as PNR and profiling. On the other side, the political back up that it can offer to independent data protection supervisor is still limited.

REFERENCES

Selected European Legislation

Commission of the European Union – Commission, *Communication from the Commission of the European Union to the European Parliament, the Council, the European Economic and Social committee and the Committee of the Regions, Preparing the next steps in border management in the European Union*, doc. 6666/08, Brussels, 13.2.2008.

—, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, Brussels, 6.11.2007 (2007a).

—, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, Impact Assessment, SEC(2007) 1453, Brussels, 6.11.2007 (2007b)

Council of the European Union – Council, *2008 EU-US Summit Declaration*, doc. 10562/08 (Presse 168), Brdo 10 June 2008.

—, *Proposal for a Council Framework Decision on the use of Passenger Name record (PNR) for law enforcement purposes*, doc. 5618/09, Brussels, 23 January 2009.

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, OJ L 281, 23.11.1995, pp. 31–50.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, pp. 37–47.

European Court of Human Rights – ECtHR, *Case of Liberty and others versus United Kingdom*, Application no. 58243/00, Strasbourg, 1st July 2008.

—, *Case of S. and Marper versus the United Kingdom*, Application nos. 30562/04 and 30566/04, Strasbourg, 4 December 2008.

European Court of Justice – ECJ, European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), Joined cases C-317/04 and C-318/04. European Court reports 2006 Page I-04721.

—, Ireland v European Parliament and Council of the European Union, Case C-301/6, 10 February 2009.

European Data Protection Supervisor – EDPS, *Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, OJ C 110/1, 1.5.2008 (2008a)

—, *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 11 November 2008 (2008b)

—, *Third 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*, OJ C139/1, 23.06.2007.

European Parliament, *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes* [B6-0615/2008], Strasbourg, 20 November 2008.

European Parliament – LIBE Commitee, *Report on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters* [16069/2007 - C6-0010/2008 - 2005/0202(CNS)].

—, *Working Document on problem of profiling, notably on the base of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control*, Brussels, 30.9.2008.

Future Group, *Freedom, Security, Privacy – European Home Affairs in an open world. Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ('Future Group')*, June 2008.

Bibliography

Balzacq T., Bigo D., Carrera S. and Guild E., 'Security and the Two-Level Game : The Treaty of Prüm, the EU and the Management of Threats', CEPS – Working Document, No.234/January 2006.

Bellanova, R., 'Prüm: A 'Prêt-À-Exporter' Model? The 2008 German-US Agreement on Data Exchange', CEPS – Challenge Research Paper, N.18, forthcoming.

Brouwer, E., 'Towards a European PNR System? Questions on the Added Value and the Protection of Fundamental Rights', Study for CEPS on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 2009.

Bunyan, T., 'The Shape of Things to Come – EU Future Group', *Statewatch*, 2008. Available at: http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf

Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data, *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee (T-PD)*, Strasbourg, 13-14 March 2008.

De Hert, P., 'Balancing security and liberty within the European human rights framework. A critical regarding of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11', *Utrecht Law Review*, Vol. 1, 2005, pp. 68-96.

De Hert P. and Bellanova, R., 'Data Protection from a Transatlantic Perspective: The EU and US Move Towards an International Data Protection Agreement?', Study for CEPS on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 2008.

De Hert P. and Gutwirth, S., 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006.

—, 'Regulating Profiling in a Democratic Constitutional State', in Hildebrandt, M. and Gutwirth, S. (Eds.), *Profiling the European Citizen*, Springer, Dordrecht, 2008.

De Hert, P. and De Shutter, B., 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT', in Martenczuk, B. & van Thiel, S. (Eds.), *Justice, Liberty and Security: New Challenges for EU External Relations*, VUB Press, Brussels, 2008.

De Hert, P., Papakonstantinou, V. and Riehle, C., 'Data protection in the third pillar: cautious pessimism', in Mike, M. (Ed.), *Crime, rights and the EU: the future of police and judicial cooperation*, Justice, London, 2008.

Department of Homeland Security – Chief Privacy Officer, *2008 Report to Congress. Data Mining: Technology and Policy*, Washington, December 2008.

European Data Protection Supervisor – EDPS (2008c), *EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step*, Press Release, Brussels, 28 November 2008 (2008c).

González Fuster, G. and Paepe, P., 'Reflexive Governance ad the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects', in Guild, E. and Geyer, F. (Eds.), *Security versus Justice?*, Aldershot, Ashgate, 2008.

Hildebrandt, M. and Gutwirth, S. (Eds.), *Profiling the European Citizen*, Springer, Dordrecht, 2008.

Hijmans, H., 'The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority', *Common Market Law Review*, Vol. 43, 2006, pp. 1313-1342.

Hosein, I., 'The Sources of Laws: Policy Dynamics in a Digital and Terrorized World', *The Information Society*, Vol. 20, 2004, p. 187-199.

House of Lords – European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, London, 5 June 2007.

—, *The Passenger Name Record (PNR) Framework Decision – Report with Evidence*, London, 11 June 2008.

Scirocco, A., 'The Lisbon Treaty and the Protection of Personal Data in the European Union', *Dataprotectionreview.eu*, Issue 5, 2008.