Common Market Law Review **46**: 1485–1525, 2009.

SHORTCOMINGS IN EU DATA PROTECTION IN THE THIRD AND THE SECOND PILLARS. CAN THE LISBON TREATY BE EXPECTED TO HELP?

HIELKE HIJMANS AND ALFONSO SCIROCCO*

1. Introduction

Data protection is recognized as a basic value of a democratic society under the rule of law. This is at EU level illustrated *inter alia* by Article 286 EC and by Article 8 of the Charter of the Fundamental Rights of the Union.

Data protection was introduced into the legal framework of the European Union within the First Pillar as an internal market related issue, with Directive 95/46/EC[1] on the protection of individuals with regard to the processing of personal data and of the free movement of such data. This article however discusses the role of data protection in the area of police and judicial cooperation ("Third Pillar"), as well as of the common foreign and security policy ("Second Pillar"). In other words, data protection in areas of activities of the State where there is significant growth in the importance of storage and exchange of information, and access to this information, as instruments for ensuring security. Reasons for this development are on the one hand the risks for security (terrorism, serious crime) and on the other hand the growing possibilities to use information effectively, due to technological developments. As a consequence, the importance of an effective system of data protection in these areas is also growing. Personal information that is stored and can be exchanged and accessed needs protection.

This article demonstrates that the present arrangements for data protection are not fully satisfactory. It focuses in particular on the shortcomings of the framework for data protection which are related to the pillar structure of the EU Treaty and are difficult to solve under the present EU legal framework. The next logical question is to what extent the Lisbon Treaty – and in particular the

* H. Hijmans and A. Scirocco both work as legal advisors to the European Data Protection Supervisor (EDPS). This article contains their personal opinions only. The authors thank H. Kranenborg for his contributions to earlier versions of this article, and A. Beach and M. Blondeau for their help in finalizing the text.

1. O.J. 1995, L 281/31 (hereinafter: Directive 95/46).

abolition of the pillar structure – provides instruments to address these shortcomings. The article analyses the Lisbon Treaty from this perspective.

The article is structured as follows. Part 2 sets the context and part 3 highlights the main shortcomings of the present legal framework of data protection in the Third and Second Pillars. Part 4 underlines that the strict dividing line between the EU pillars does not reflect the reality of data protection when personal data are used in a cross border context, as illustrated by the case law of the Court of Justice. The article will discuss the consequences of the *PNR* case[2] and the *data retention* case[3] as well as the case law on terrorist lists.[4] Part 5 addresses the future of this legal framework under the Lisbon Treaty. The Lisbon Treaty is characterized as an important step forwards, allowing – or even calling for – consistent and robust mechanisms for data protection. Some conclusions can be found in Part 6.

2. Data protection and activities of the State to ensure security

2.1. *Privacy and data protection*

2.1.1. *Are privacy and data protection important?*

A novel on a future society by the British writer Ben Elton contains the following passages[5] on a conflict between an individual and an authority:

> "He could not possibly confess that his decision ... had been the result of a strange force deep within him which desired a moment of privacy. A longing to keep something to himself, even if only for a short while. He could not say that. Nothing was more offensive ... to the community ... than privacy. 'Why would anyone wish to hide any aspect of themselves from the gaze of others?'
>
> 'Do you have something to hide?' 'I have nothing of which I'm ashamed if that's what you mean'. 'I'm fascinated then. If you had nothing to be ashamed of, why on Earth would you desire privacy?' [He] thought for a moment. "Because I consider it fundamental to my sense of self.' 'Or perhaps it's because you're a pervert and heretic'".

2. Joined cases C-317 & 318/04, *European Parliament* v. *Council and Commission*, [2006] ECR I-4721.

3. Case C-301/06, *Ireland* v. *Parliament and Council*, judgment of 10 Feb. 2009, nyr.

4. In particular, Joined cases C-402 & 415/05 P, *Kadi and Al Barakaat International Foundation* v. *Council*, [2008] ECR I-6351.

5. B. Elton, *Blind Faith*, (Bantam, 2007), pp. 29 and 331. The background of these passages is the reluctance of the protagonist of the novel to post the video of the birth of his child on his webpage.

It is clear that the perception of privacy and data protection in present times is not as negative as the example above might suggest. However, our society has more and more elements of a surveillance society.[6] Some say that we already live in such a society, as stated in a Report on the Surveillance Society by the Surveillance Studies Network of September 2006: "In all the rich countries of the world everyday life is suffused with surveillance encounters, not merely from dawn to dusk but 24/7."[7]

The Eurobarometer Survey[8] of February 2008 shows that in this society most European citizens show concern about data protection issues. However, this Survey also shows that a large majority of European citizens consider that "it should be possible to monitor passenger flight details (82%), telephone calls (72%) and Internet and credit card usage (75% and 69%, respectively) when this serves to combat terrorism." What is even more remarkable is that "Since 2003, the numbers of citizens approving the monitoring of people's Internet usage and telephone calls has increased by about 12 percentage points (in each case)."

In short, as far as privacy and data protection are concerned, the surveillance society emerging also as a result of technological developments poses new risks for privacy and data protection, which need to be addressed. It should thereby be taken into account that restrictions on privacy and data protection must be accepted, provided this serves the needs for security. Restrictions on privacy and data protection must serve specific needs. In other words: they must be necessary and proportional.[9]

2.1.2. *Data protection as a legal concept*

The legal concept of the right to data protection incorporates on the one hand obligations on (institutional) actors[10] who process personal data of individuals and on the other hand the rights of those individuals. The main obligations are that the data are collected fairly and lawfully and only processed for specified

6. As the former UK Information Commissioner Richard Thomas said on the occasion of the International Data Protection and Privacy Commissioners' Conference in London (November 2006): "Fears that society would 'sleep-walk into a surveillance society' have become a reality", BBC News, 2 Nov. 2006, news.bbc.co.uk/2/hi/uk_news/6108496.stm.

7. "A report on the surveillance society: for the Information Commissioner by the Surveillance Studies Network", Sept. 2006, www.ico.gov.uk/upload/documents/library/data_protection/practical_-application/surveillance_society_full_report_2006.pdf.

8. Data Protection in the European Union – Citizens' perceptions – Analytical report, Flash Eurobarometer Series 225, Jan. 2008, ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

9. These are the usual criteria for restrictions of fundamental rights applied by the Court of Justice and the European Court of Human Rights.

10. Compliance with these obligations must primarily be ensured by the data controller, as defined in Art. 2 (d) of Directive 95/46.

purposes. The processing should be proportionate to those purposes, the data should be accurate and the data should not be retained for a longer period than necessary. The most important rights of the individuals (the data subjects) are recognized as being the rights of access, rectification and erasure. Supervision by independent authorities is an inherent part of the legal framework.[11]

The legal concept emerged from the protection of privacy or private life.[12] In *Rotaru* v. *Romania*, the European Court of Human Rights held that all kinds of information about individuals – even public information – can fall within the scope of private life where it is systematically collected and stored in files held by authorities.[13] The Court furthermore recalled that the expression private life must not be interpreted restrictively and that there is no reason of principle to justify excluding activities of a professional nature from the notion of private life.[14] The European Court of Human Rights has given a number of important judgments relating to information about persons. In these judgments it stated that restricting measures can be taken but they should be accessible to the person concerned and foreseeable as to their effects. A rule is foreseeable "if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct".[15]

Data protection and privacy are closely related but not identical. This is best illustrated by the Charter of the Fundamental Rights of the Union which acknowledges – in its Article 8 – data protection as a fundamental right, connected to but separate from the right to privacy. In *Promusicae,* the Court of Justice acknowledged this status of "a further fundamental right, namely the right that guarantees protection of personal data and hence of private life".[16]

Article 1 of Directive 95/46 defines its objective as the protection of "fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." Personal data are protected even if the right to privacy is not at stake, as was further clarified by the Court of Justice in *Österreichischer Rundfunk.*[17] The Court underlined that

11. These are the essential elements of data protection; most of them are listed in Art. 8 of the Charter of the Fundamental Rights of the Union.

12. Art. 8 ECHR speaks about the right to private life.

13. Appl. 28341/95, *Rotaru* v. *Romania* [GC], judgment of 4 May 2000, ECHR 2000-V.

14. Appl. 27798/95, *Amann* v. *Switzerland* [GC], judgment of 16 Feb. 2000, ECHR 2000-II, para 65 and *Rotaru* v. *Romania*, cited *supra* note 13, para 43. See generally in this *Review:* Oliver, "The protection of privacy in the economic sphere before the European Court of Justice".

15. *Rotaru* v. *Romania*, cited *supra* note 13, paras. 50, 52 and 55, and *Amann* v. *Switzerland*, cited *supra* note 14, paras. 50 et seq. Also important is Appl. 8691/79, *Malone* v. *United Kingdom*, judgment of 2 Aug. 1984, ECHR A82.

16. Case C-275/06, *Promusicae*, [2008] ECR I-271, para 63.

17. Joined cases C-465/00, C-138 & 139/01, *Österreichischer Rundfunk and Others*, [2003] ECR I-4989.

data processing does not by definition fall within the scope of private life of Article 8 ECHR. However, insofar as the provisions of Directive 95/46/EC "govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, [they] must necessarily be interpreted in the light of fundamental rights, which, according to settled case law, form an integral part of the general principles of law whose observance the Court ensures."

The protection of personal data was explicitly guaranteed for the first time in 1981 by Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data.[18] This Convention – ratified by all Member States – applies to all automated personal data files and automatic processing of personal data in the public and private sectors. Convention 108 was also the point of departure for Directive 95/46/EC, the central piece of data protection law in the First Pillar.[19] Convention 108 is still of specific importance in the Second and Third Pillars. Several EU instruments in the Third Pillar refer to Convention 108 as the minimum standard of data protection to be taken into account.[20]

2.2. *The growing need to use information*

Facilitating the exchange of and access to information for the fight against terrorism, but also more in general to ensure security is high on the political agenda of the European institutions. In its Communication of 10 June 2009 on an area of freedom, security and citizen serving the citizen, the Commission states: "Security in the EU depends on effective mechanisms for exchanging information between national authorities and other European players. To achieve this the EU must develop a European information model ...."[21] This emphasis is logical for two reasons. In the first place, in particular after 9/11

18. ETS No. 108, 28.01.1981 (hereinafter: Convention 108). To this Convention an Additional Protocol was added, regarding supervisory authorities and transborder data flows (ETS No. 181, 8.11.2001). Finally, Recommendation (87)15E of 17 Sept. 1987 regulating the use of personal data in the police sector, by the Council of Ministers of the Council of Europe, contains eight principles of data protection, specific to the police sector.

19. According to its Recital 11, the Directive gives substance to and amplifies the data protection principles of Convention 108, which was considered not specific enough to provide for sufficient protection.

20. See *infra* 3.1.1.

21. COM(2009)262 final, p. 15. See also Opinion of the European Data Protection Supervisor of 10 July 2009 on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen, available at www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-10_Stockholm_programme_EN.pdf.

and the terrorist attacks in Madrid and London, much emphasis was put on the toolbox of police and justice. New instruments were created – or are being created – in order to facilitate the effectiveness of the police work to fight terrorism and other forms of serious crime. There was a wide consensus that effective prevention requires more information.

In the second place, the institutions of the EU do not have the capacity to guarantee security themselves. There is no European police with executive powers to ensure security; the EU can not instruct the Member States to combat specific crimes[22] and the European Courts do not have the powers to give direct legal protection to individuals. The EU therefore focuses on measures that should enable the authorities of the Member States to fight crime, such as giving access to and exchange of information on the basis of the principle of availability, as introduced by the Hague Programme of 2004.[23]

Over the last years, a number of different legal instruments have been adopted, promoting the collection, storage and subsequent exchange of information. Access to this information has also been addressed in these legal instruments.[24] The logic behind this development is utilitarian.[25] Information must be seen as a tool for collective benefits like fighting terrorism or curtailing crime. Everything must be done to ensure that information is available when needed.

Additionally, in an area of freedom, security and justice without internal borders, external border control requires certain centralization. Once they have entered the territory of the EU, individuals can move freely, at least without being stopped at the internal borders. Such an area without internal borders "can not function ... without shared responsibility and solidarity in managing its external borders."[26] Member States must have tools to effectively protect their borders. In this context, the Schengen Information System was established as a necessary tool for the functioning of the area without internal borders (the Schengen area), and it has recently been adapted in order to allow the extension of the Schengen Area to the new Member States that acceded to the EU in 2004 and 2007.

22. Europol has a far more restricted competence**.**
23. O.J. 2005, C 53/1.
24. See for instance Council Decision 2008/633/JHA mentioned in 2.3.
25. See J. Rule, *Privacy in Peril* (Oxford University Press, 2007), amongst others p. 12.
26. Communication from the Commission 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, 13 Feb. 2008, COM(2008)69 final, para 1.1.

2.3. *The growing possibilities of information use*

Technological developments, such as information and communication technologies, are a second driver behind the growing importance of exchange of and access to information for the safeguarding of security. In the network society, there is more information available about individuals and there are more tools for using information in a more sophisticated way. For example, databases are used for data mining[27] and risk assessments of individuals can be made on the basis of profiling of persons.[28]

Interoperability is an important notion in this context. The Commission defines this notion as "the ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge".[29] The Commission explains this as a technical rather than a legal or political concept. This explanation can be questioned. It is based on the assumption that the choice of technology is a neutral one and that it is up to those using the technology to decide on the conditions under which use is allowed.

However, this assumption[30] ignores the fact that information tends to be used if it exists. A good example is Council Decision 2008/633/JHA of 23 June 2008 concerning the consultation of (access to) the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.[31] The Visa Information System is supposed to support the common visa policy; it is not an instrument for law enforcement. However, the Council Decision is designed to allow use for the latter purpose. Equally, the Commission proposes to provide law enforcement authorities with access to the database for the common asylum policy, Eurodac.[32] In short, databases established for specific purposes that have nothing to do with law enforcement are nevertheless made accessible for law enforcement.

27. Data mining is the process of sorting through large amounts of data and picking out relevant information (Wikipedia).

28. Profiling, the extrapolation of information about something, based on known qualities (Wikipedia). One can think about stereotypes, race, religion, cultural background, but also far more innocent qualities.

29. Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, 24 Nov. 2005, COM(2005)597 final.

30. Although technically correct.

31. O.J. 2008, L 218/129.

32. Proposal of 10 Sept. 2009 for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009)344 final.

Another trend is to ensure – as a preventive measure – that information is stored, even in situations where there is no direct link to a specific crime or to people specifically related to criminal acts. The most striking example here is Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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.[33] This Directive establishes the mandatory retention by providers of telecommunications and internet services of certain communications data of all their customers. The Directive must ensure that these data are available in the event of a future serious crime, for the purpose of the investigation, detection and prosecution of this crime.[34] In essence, the Directive is an illustration of a trend to preventively store personal data of all citizens.

The growing possibilities of information use are thus enabled by technological developments but also result from legislative measures. These developments support changing working methods within law enforcement in order to increasingly rely on proactive research methods. These research methods allow risk assessment and investigations based on available information even without the identification of a specific crime or a specific suspect.

2.4. *The result: A change of emphasis*

Legal instruments facilitating the access to and exchange of information are a priority for the EU legislature. The emphasis is on widening the possibilities for police and justice to collect, store and exchange information (including information relating to persons). However, these instruments must respect principles of data protection, in order to fulfil the conditions of Article 6(1) TEU. This is illustrated by the important recent judgment in *S. and Marper* v. *the United Kingdom*.[35] The European Court of Human Rights held that the storage of fingerprint and DNA information by the authorities of the UK violates Article 8 ECHR. The system allowed the indefinite retention of fingerprint and DNA material of any person of any age accused of any – even

33. O.J. 2006, L 105/54 (hereinafter: Directive 2006/24).

34. The data retention Directive was swiftly approved not only because of the political climate created by the London bombings of July 2005, but also because the European Parliament faced the "threat" of an analogous proposal with a Third Pillar legal basis. The current First Pillar instrument was then adopted by the Council with qualified majority, with the contrary votes of Ireland and Slovakia, while the Third Pillar proposal would have required unanimity. Those two Member States challenged the Directive before the ECJ (see *infra* 3.3.2).

35. Joined appl. 30562/04 and 30566/04, *S. and Marper* v. *United Kingdom*, judgment of 4 Dec. 2008, ECtHR nyr.

very minor – recordable offences. The Court also mentioned the risk of stigmatization, stemming from the fact that certain persons who have not been convicted of any offence are treated in the same way as convicted persons.

Respect of principles of data protection is not only needed because the individual is entitled to protection, but also because it enhances mutual trust between the authorities of the Member States and because only under those conditions data can be relied upon in criminal procedures before the Courts of the Member States.[36]

As a result, in the context of the EU, data protection has changed from an internal market issue to become a broader concern.[37] The main legal and political debates in recent years do not concern internal market issues, but relate to the complex relation between data protection and the activities of the State to ensure security.

3. An unsatisfactory legal framework in the Third and the Second Pillar

3.1. *The Third Pillar*

3.1.1. *Council Framework Decision 2008/977/JHA in combination with specific rules*

An important development is the adoption of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[38] Its provisions must be transposed into national law by 27 November 2010. The Framework Decision is based on Article 30(1)(b) TEU, which provides that common action in the field of police cooperation relating to the collection etc. of information is "subject to appropriate provisions on the protection of personal data". Its Recital 3 announces common standards, contributing to the efficiency of police and judicial cooperation, as well as its legitimacy and compliance with fundamental rights.

36. See Hijmans, "The Third Pillar in practice: Coping with inadequacies. Information sharing between Member States", available at www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2007/07-02-07_preadvies_NVER_EN.pdf, original article in Dutch published in (2006) SEW, 375.

37. It is illustrative that, in the organizational field, since 2005 data protection falls no longer within the portfolio of the Commissioner for Internal Market, but within the portfolio of his colleague for Justice, Freedom and Security.

38. O.J. 2008, L 350/60 (hereinafter: Framework Decision 2008/977).

The instrument can be characterized as a first step towards a legal framework with general application in the Third Pillar. It can however not be seen as an equivalent to Directive 95/46 – which provides such a legal framework in the First Pillar – due to several shortcomings.

In the first place, the scope of Framework Decision 2008/977 is limited. The common standards do not have general application. They do not apply to internal situations, when personal data originate within the Member State which uses them. They do not apply to the processing by Europol and Eurojust either. It is obvious that these limitations of scope have as an effect that individuals are not in all circumstances protected by Framework Decision 2008/977. It is moreover questionable how these limitations work in practice. At the moment of the collection of personal data by a police authority in a Member State, it will normally not be foreseeable whether those data might at a later stage be used in a cross-border context, which is the condition for the applicability of Framework Decision 2008/977.

In the second place, the level of protection raises questions. Processing of personal data by law enforcement authorities may need some specific adaptations of general data protection principles, reflecting for example the need to use personal data for crimes other than those for which they were collected, or to establish limits to the right of access to the data subject insofar as its exercise could prejudice investigations. These specificities are addressed by Recommendation (87)15 of the Council of Europe regulating the use of personal data in the police sector,[39] which influenced the legislation of many States even without having binding value. Unfortunately, Framework Decision 2008/977 establishes broad exceptions to some of the obligations of the data controllers[40] without providing the same guarantees as the Recommendation.[41] An example is the broad exception of the purpose limitation principle: Article 11(d) allows processing of personal data *for any other purpose* provided that the transmitting Member State[42] consents to this processing.

In the third place, although Framework Decision 2008/977 is meant to be a legal framework with general application in the Third Pillar, it does not set aside specific rules on data protection. On the contrary, its Article 28 lays down that specific conditions on the use of personal data take precedence over the provisions of the Framework Decision. This is all the more important in the perspective of the existence of quite a number of such specific rules, applicable

39. Cited *supra* note 18.

40. See *supra* 2.1.2 and note 10.

41. It has therefore been heavily criticized and sometimes considered as not providing an acceptable level of protection of personal data. See e.g. the opinions and comments of the EDPS, available on www.edps.europa.eu.

42. Or the data subject, but under that hypothesis there is no conflict with Recommendation R(87)15.

to specific activities of national and European authorities and contained in legal instruments with a main objective outside data protection.

The Convention implementing the Schengen Agreement of 1990[43] already had a chapter on the protection of personal data and the security of data in the Schengen Information System, building on the general framework of Council of Europe Convention 108.[44] Other older instruments with such provisions are the 1995 Europol Convention[45] and Council Decision 2002/187/JHA setting up Eurojust.[46]

All three instruments deal with data protection in the context of the exchange of data between Member States and a central database (SIS) or a European authority (Europol; Eurojust), as well as with the central storage of data. In the three cases a Joint Supervisory Authority[47] was set up, as a form of joint supervision by independent national authorities on the processing of personal data on the European level. Recently, all three instruments have been revised. Different solutions are chosen for the supervision of the processing of personal data.[48]

More recent are (proposals for) specific rules for data protection applicable to the exchange of personal data between authorities of the Member States carried out without establishing a central EU database or authority, such as:

– Article 9 of Council Framework Decision 2009/315/JHA on the organization and content of the exchange of information extracted from the criminal record between Member States,[49] *inter alia* specifying the purposes for which personal data from criminal records may be used in other than the originating Member States.
– Chapter 6 of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism

43. Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, O.J. 2000, L 239/19.

44. Art. 117 of the Convention.

45. O.J. 1995, C 316/1. The Convention will be replaced by Council Decision 2009/371/JHA establishing the European Police Office, O.J. 2009, L 121/37.

46. O.J. 2002, L 63/1, recently amended by Council Decision 2009/426/JHA on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, O.J. 2009, L 138/14.

47. Sometimes called Joint Supervisory Body.

48. For SIS, the Joint Supervisory Authority will be replaced by a system of "coordinated supervision" whereas for Europol and Eurojust the present system will be continued. For Eurojust the system is different because the Joint Supervisory Body consists of judicial magistrates.

49. O.J. 2009, L 93/23.

and cross-border crime (the "Prüm decision"),[50] containing a set of data protection rules aiming to specify the principles of Convention 108.

– Chapter III of the proposal for a Council Framework Decision on the use of Personal Name Records (PNR) for law enforcement purposes,[51] equally containing a set of data protection rules aiming to specify the principles of Convention 108, as well as Framework Decision 2008/977.

It is interesting to note that in all three examples reference is made to Convention 108 as the minimum standard on data protection.

3.1.2. *The result: A patchwork*

The legal system of data protection in the Third Pillar consists of a general framework, but which is not generally applicable, complemented by a number of specific instruments for specific situations. It is not always clear in what situations the specific instruments apply and what rules apply if more than one specific instrument might be applicable. This may be the case, for example, of personal data collected under the Prüm system, which is subsequently included in the SIS.

For these reasons, the EU legal framework in the Third Pillar can be best defined as a patchwork of data protection regimes. There is no legal framework which is stable and unequivocal, like Directive 95/46/EC in the First Pillar.

This state of play is in the first place the consequence of trends in society and subsequently in law making, calling for more security. Importance is given to quick responses, not always based on a master-plan or on an evaluation of existing legal instruments, as for instance shown by the Commission proposal for an EU PNR system.[52] In other words, creating a stable and unequivocal system of data protection was not a priority.

Another factor is the attitude of the Member States. They seem to be reluctant to hand over competences to the Union in this area. This reluctance is

50. O.J. 2008, L 210/1. The decision brings into the EU framework the Prüm Treaty, concluded by seven Member States in 2005. It creates a network of national databases where law enforcement authorities can gain automated access to each other's national databases containing DNA analysis files and fingerprints in what is called a hit/no hit system.

51. Not yet adopted by Council; the provisions on data protection were added by Council in the course of the negotiations; the Commission Proposal itself was more limited in this respect. Last available text on the Register of the Council from 29 June 2009, 5618/2/09.

52. Cited *supra* note 51. See also Opinion of 20 Dec. 2007 of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, O.J. 2008, C 110/1. One of the main points of criticism in this opinion was that no evaluation was made of the existing legal instruments.

reflected in the EU Treaty itself, for instance in the limitations in the powers of the Commission, the European Parliament and the Court of Justice. It is also reflected in the negotiations in the Council. The restriction of the scope of Framework Decision 2008/977 to personal data exchanged between Member States was not foreseen in the Commission proposal, but a few Member States introduced it in order to keep the processing of personal data by national authorities within the context of national law.[53]

3.2. *The Second Pillar*

In the Second Pillar, there is no general legal framework on data protection; there is no provision in the EU Treaty which – in the way Article 30(1)(b) TEU does for the Third Pillar – establishes that specific actions should be conditional upon the respect of certain adequate guarantees with regard to data protection; and there are no specific legislative provisions on data protection, comparable to those under the Third Pillar.

It is arguable that the absence of any reference to data protection is due to the fact that the common foreign and security policy is created as an area of intergovernmental cooperation in which legal instruments would be more likely to address general strategies and actions aimed at preserving peace and strengthening international security rather than to specifically address individuals. However, in recent years, and in particular after 9/11, restrictive measures on suspected terrorists – better known as "terrorists' blacklists" – were adopted, targeting specific individuals.

Terrorists' blacklists were first used in the context of the United Nations. In that context, a Committee operating within the Security Council[54] adopts sanctions targeting individuals or legal entities suspected of having links with international terrorism.[55] The EU transposes UN blacklists into internal instruments, but also compiles blacklists on own initiative.[56] The EU terrorists' blacklists

53. The second sentence of Recital (7) is remarkable: "No conclusions should be inferred from this limitation regarding the competence of the Union to adopt acts relating to the collection and processing of personal data at national level or the expediency for the Union to do so in the future." In short, the limitation has a political background, not a legal one.

54. Referred to as UN Sanctions Committee.

55. These kinds of sanctions replace traditional commercial or political measures targeting a country and are also referred to as "smart sanctions". The concept of "smart sanctions" refers to the idea that, being more selective and targeted, they reduce the suffering of the whole population of one country, while focusing on specific organizations or individuals.

56. In both situations, the EU implements the blacklists through Common Positions adopted in the framework of the Common Foreign and Security Policy, integrated in Community instruments adopted under Arts. 60 and 301 EC. See *infra* para 4.2.1.

directly affect specific individuals or organizations[57] since they consist of names of individuals and organizations which are collected, disclosed and publicized by EU institutions in order to subject them to certain restrictive measures, in other words processing of personal data (the inclusion of names, place of birth and residence, family links, documents numbers, etc. of individuals on terrorists' lists and subsequently the publication of these lists) within the meaning of data protection law. This is even more important since this processing and publication of personal data can stigmatize persons as terrorism-related.

The development of this instrument requires protection of the fundamental rights of the persons included on those lists. Article 6(2) TEU extends also to the Second Pillar the obligation to respect fundamental rights as guaranteed by the ECHR and by the constitutional traditions common to the Member States, as general principles of Community law. More specifically, data protection should be ensured as a basic value of a democratic society under the rule of law.[58]

The use of terrorists' blacklists at EU level has been repeatedly and quite successfully challenged before the Court of Justice. The bottom line of this recent case law, which has been described and analysed by a copious doctrine,[59] is that respect of fundamental rights is a key element of the lawfulness of Community action, irrespective of the (UN) origins of the decisions at stake.[60] It leads to a full recognition of fundamental rights.[61]

However, the right to the protection of personal data did not as yet play a significant role, despite the fact that restrictive measures relating to individuals are based on the processing of personal data. The Court did not explicitly address the right to the protection of personal data.[62]

57. See Nettesheim, "U.N. sanctions against individuals: A challenge to the architecture of European Union governance", 44 CML Rev. (2007), 567–600.

58. Indeed, at the heart of the Treaty lies the core principle of upholding the rule of law. See Lenaerts, "The rule of law and the coherence of the judicial system of the European Union", 44 CML Rev. (2007), 1625.

59. See, more recently, Kunoy and Dawes, "Plate Tectonics in Luxembourg: The ménage à trois between EC law, International law and The European Convention on Human Rights following the UN sanctions cases", 46 CML Rev. (2009), 73–104; Gattini, annotation on joined cases C-402/05 P & 415/05, 46 CML Rev. (2009), 213–239, and literature cited therein, as well as the annotation on these cases by Jacqué, 45 RTDE (2009).

60. *Kadi and Al Barakaat*, cited *supra* note 4, para 285. About the lack of sufficient guarantees at UN level, see Nettesheim, op. cit. *supra* note. 57.

61. See Kunoy and Dawes, op. cit. *supra* note 59.

62. Possibly also because it was not invoked by the plaintiffs. In Case T-49/04, *Hassan* v. *Council*, [2006] ECR II-52, the argument of a possible violation of the right to privacy, as guaranteed by Art. 8 ECHR, is explicitly invoked by the applicant. The Court recognizes the right to privacy as part of *jus cogens,* but then dismisses this argument in the specific case.

These cases show that the absence of a legal framework for data protection in the Second Pillar has real consequences for individuals.[63]

3.3. *Exchanges with third countries*

A separate issue is the legal framework relating to the exchanges of data with third countries. Restrictions on the exchange of data with third countries are needed to avoid a loophole in the protection afforded to personal data within the EU. National authorities could evade the internal data protection obligations by exchanging information with each other through third countries where these obligations do not apply. Moreover, lower standards for the exchange with third countries would be contrary to the concept of effective protection, since third countries do not necessarily protect personal data at the same level as Member States.

It is for these reasons that Article 25 of Directive 95/46 provides for a so-called adequacy finding, applicable to transfers of personal data under the First Pillar. In principle, exchanges with third countries are only allowed under Article 25 if that third country provides for an adequate level of data protection, recognized in a decision of the Commission.[64]

An equivalent mechanism is not foreseen for the Third Pillar. Article 13 of Framework Decision 2008/977 only imposes conditions on the transfer of data to a third country by an authority of a Member State insofar as those data are transmitted or made available by the competent authority of another Member State. Transfers to third countries of data where only one Member State is involved are not covered. The conditions of Framework Decision 2008/977, however, do not require a similar level of adequate protection in the third country concerned, although adequacy is mentioned in Article 13(1)(d) of the Framework Decision. This provision does not contain any parameters for adequacy: the assessment of adequacy is fully left to the Member States on the basis of very general criteria (Art. 13(4)).

Furthermore, on a case by case basis, agreements are concluded with third countries allowing the transfer of personal data to third countries. The most famous examples of agreements on the exchange of personal data with third countries are probably the agreements between the EU and the United States on passenger name record data (PNR)[65]. The first agreement of

63. See also *infra* section 4.2 where the terrorists' lists will be discussed in the light of the difficulties arising from the division between pillars.

64. Arts. 25 and 26 of the Directive also contain other mechanisms for the transfer of personal data to third countries; they are not discussed here.

65. See more extensively on the PNR Agreements: Papakonstantinou and De Hert "the PNR Agreement and transatlantic anti-terrorism cooperation: No firm human rights framework on either side of the Atlantic", 46 CML Rev. (2009), 885–919.

2004,[66] based on Articles 95 and 300 EC, was annulled by the Court of Justice on 30 May 2006[67] for reasons of legal basis. It was finally replaced by a new agreement – based on Articles 24 and 38 TEU and with different content based on experiences and new views – in July 2007,[68] for a period of seven years.[69] It should be noted that the new agreement was concluded without the consent of the European Parliament and is not subject to judicial control by the Court of Justice.

These agreements do not stand alone:

– Also in other contexts access to personal data of residents of the European Union are requested by third countries. A well-known example concerns financial transaction information data held by SWIFT, a Belgium-based cooperative that operates a worldwide messaging system. SWIFT stored copies of information of financial transactions between EU citizens (collected within the EU) in the United States. The transmission of those data to the US law enforcement authorities in the framework of a US anti-terrorism programme was found to be in breach of certain provisions of EU data protection law and called for specific actions both at SWIFT and at institutional level.[70]
– Member Stares are individually negotiating and concluding international agreements which include possibilities for exchange of personal data. The best known example is the agreement between Germany and the United

66. 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, O.J. 2004, L 183/84.

67. Judgment cited *supra* note 2.

68. Council Decision 2007/551/CFSP/JHA on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), O.J. 2007, L 204/16.

69. Also other countries require passenger data from European airlines. This has led to agreements with Canada (Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, O.J. 2006, L 82/14) in 2005 and with Australia (Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, O.J. 2008, L 213/49). Discussions are also taking place with further third countries.

70. See Working Party 29 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), available at www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf. As a result of this case, SWIFT decided to change its technical architecture and it no longer stores the data within US territory. On the institutional level, the result was, *inter alia,* an exchange of letters between the EU and the US, O.J. 2007, C 166/17, and the appointment of an eminent EU person reviewing the use of the data within the US.

States to grant each other access to databases of fingerprints and DNA of people suspected of terrorist activity.[71]

– Last but not least, personal data stored in EU databases are exchanged with third countries on the basis of specific agreements, notably the Agreement between the USA and Europol of 6 December 2001 and the Eurojust-USA Agreement of 6 November 2006.[72]

This situation was not considered fully satisfactory, *inter alia* because of the lack of political and judicial control on these initiatives. Discussions are taking place between the European Union and the United States on privacy and personal data protection in the context of the exchange of information for law enforcement purposes as part of a wider reflection on how best to prevent and fight terrorism and serious transnational crime.[73] These discussions resulted in a Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection. This report contains 12 privacy and personal data protection principles which are recognized on both sides.[74] The report could lead to a binding agreement applicable to all exchanges between the European Union and the United States in the police and judicial sector. One could imagine that this model would then be used for further exchanges with other third countries.

4. The division between the pillars

4.1. *Between First and Third Pillars*

4.1.1. *Large scale information systems*

Large scale information systems for external border control have been established in the area of freedom, security and justice (notably Eurodac,[75] SIS[76] and

71. US Homeland Security, Press release of 11 March 2008, www.dhs.gov/xnews/releases/pr_1205330012342.shtm.

72. These agreements are published on the websites of Europol and Eurojust.

73. Document of 28 May 2008, Council Register, Doc. 9831/08.

74. Discussion continues on one of these principles. The need for (judicial) "redress" is not understood in the same way by the EU and by the US.

75. Council Regulation (EC) No. 2725/2000 of 11 Dec. 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, O.J. 2000, L 316/1.

76. Convention implementing the Schengen Agreement of 14 June 1985, cited *supra* note 43. See also Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 Dec. 2006 on the establishment, operation and use of the second generation Schengen

VIS[77]) with a legal basis in the First Pillar.[78] In substance however, external border control does not only take place for the purposes of an immigration, visa and asylum policy but is also a tool in the fight against crime, whether related to immigration or not.[79] Moreover,[80] the large-scale information systems exclusively designed for immigration purposes might also be used for law enforcement purposes. Furthermore, the Schengen Information System extends to both pillars. It enables the authorities designated by the Contracting Parties, by means of an automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks carried out within the country in accordance with national law.[81]

4.1.2. *The scope of Directive 95/46 and the PNR judgment*

In *Österreichischer Rundfunk*,[82] the Court of Justice defined the system of data protection as having a wide scope. The EU system of data protection applies even when data of a non-sensitive nature are processed and when the person concerned is not actually harmed. The wide scope is even better illustrated by another case, *Lindqvist*,[83] about a volunteer in a parish of the Swedish Church who shared news about her colleagues within the parish on the website of the local church. The Court confirmed that the Directive applies to these facts despite the absence of a direct link to the internal market since no economic activity was involved.

It is good to emphasize that *Österreichischer Rundfunk* and *Lindqvist* show a difference of views between Advocate General Tizzano and the Court. In both cases the Advocate General advocates a restrictive interpretation of the scope of application of Directive 95/46, stressing the limitations arising from the legal basis and from the scope of Community law. The Court did not follow the Advocate General. In *Österreichischer Rundfunk*, the Court decided for a wide scope of the Directive, *inter alia* by highlighting that if an effective

Information System (SIS II), O.J. 2006, L 381/4. This instrument does not stand by itself, but is connected to several other legal instruments, relating to SIS II.

77. Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), O.J. 2008, L 218/60.

78. Part Three, Title IV of the EC Treaty.

79. For example, the Communication from the Commission of 13 Feb. 2008, (cited *supra* note 26), envisages the creation of an integral entry/exit system to be also used for the identification of overstayers (third country nationals staying in the EU after the expiry of their visa).

80. See section 2.3 *supra*.

81. Art. 92 of the Convention, cited *supra* note 43.

82. Cited *supra* note 17. See on this case also 2.1.2 *supra*.

83. Case C-101/01, *Bodil Lindqvist*, [2003] ECR I-12971.

connection to the internal market had to be checked in each case, the scope of application of the Directive would be "particularly unsure and uncertain".[84] Also in *Lindqvist*, the Court interprets the Directive widely, by limiting the exception to the scope in its Article 3(2). According to the Court, Article 3(2) mentions activities which are, in any event, "activities of the State or of State authorities and unrelated to the fields of activity of individuals" and therefore the exception "applies only to the activities which are expressly listed there or which can be classified in the same category (ejusdem generis)".[85]

Against this background, the *PNR* judgment[86] was unexpected. The judgment concerned a request for annulment by the European Parliament of a decision of the Council[87] and a decision of the Commission,[88] allowing the transfer by airlines of certain personal data (PNR data) of their passengers to the authorities of the United States. In these cases, Advocate General Léger favoured a restrictive interpretation of the scope of Directive 95/46/EC and of its legal basis, suggesting the Court to annul both decisions because they relate to activities concerning public security and the activities of the State in areas of criminal law. The Court followed the Advocate General despite the fact that the PNR data are collected by private operators for commercial purposes and that these private parties arrange the transfer. The Court considered in a concise way that Article 3(2) is applicable also when the transfer of data "falls within a framework established by the public authorities that relates to public security".[89]

According to the *PNR* judgment, Article 3(2) does not only cover those cases when law enforcement is carried out by public authorities, but also when private parties are obliged to support this activity. In other words, the test *ratione materiae* (i.e. activities outside the scope of Community law) is no longer limited *ratione personae* to activities carried out by public authorities, but is expanded in order to include activities of private and commercial entities falling within a framework established by public authorities.

This judgment raises many questions regarding the applicable law and the effective protection of citizens when commercial data are further processed for law enforcement purposes. Article 13 of Directive 95/46 explicitly establishes the cases and the conditions for restricting certain data protection principles with a view to pursuing a public interest, in line with Article 8(2) ECHR.

84. *Österreichischer Rundfunk*, para 42.

85. *Lindqvist*, paras. 43–44.

86. Cited *supra* note 2. See more extensively on this judgment, Papakonstantinou and De Hert, op. cit. *supra* note 65.

87. To include an international agreement with the United States. Cited *supra* note 66.

88. On the adequate level of data protection guaranteed by the US authorities.

89. *PNR* judgment, para 58.

However, an extensive interpretation of Article 3(2) entails the reduction of the scope of application of Article 13 and might even result in depriving it of its *effet utile*.

4.1.3. *The data retention case*

The scope of First Pillar data protection law was again at stake in *Ireland* v. *European Parliament and Council*[90] about the legal basis of Directive 2006/24 on data retention. This Directive,[91] adopted on the basis of Article 95 EC, harmonizes the obligations of electronic communication providers to keep certain traffic data for possible use in the fight against serious crime. Therefore, the Directive establishes that certain categories of data generated by electronic communications should be kept for a period between 6 and 24 months, according to the implementing provisions adopted by Member States.[92] It derogates from Article 6 of Directive 2002/58/EC,[93] which obliges service providers to delete data when they are no longer needed for specific commercial purposes, such as billing their customers.

Ireland, supported by the Slovak Republic, lodged an action for annulment, arguing that the legal basis was incorrect, since the predominant purpose of the Directive is to fight serious crimes and thus requires a Third Pillar action. Also in this case, personal data are generated by private parties for commercial purposes. However, there are differences with the *PNR* cases. According to Directive 2006/24, personal data will not be systematically transferred to public authorities, but will remain under the control of communication service providers. Law enforcement authorities will receive the data only in specific cases, which are not regulated by the Directive and remain within the competence of Member States or possible Third Pillar initiatives.[94] Moreover, the data retention Directive imposes obligations on private parties rather than on law enforcement authorities. These private parties are, insofar as they retain data for commercial purposes, bound by Directive 95/46.[95] The Irish position implies that that Directive would not apply to data retained for law enforce-

90. Cited *supra* note 3. See also case note by Herlin-Karnell in this *Review*.

91. See on this Directive *supra* section 2.3.

92. Furthermore, it amends Art. 15 of Directive 2002/58/EC, which allows Member States to restrict some data protection obligations for certain public interest purposes laid down by the directive itself.

93. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. 2002 L 201/37.

94. This is made clear by Recital 25 of the Directive, stating that these issues fall outside the scope of Community law and thus "may be subject to national law or action pursuant to Title VI of the Treaty on European Union".

95. And Directive 2002/58/EC, cited *supra* note 93.

ment. Service providers would therefore have to comply with different legal obligations for the same data, depending on whether the retention period arises from commercial purposes or from law enforcement obligations. It goes without saying that this would affect legal certainty and ultimately the uniform competition between service providers.[96]

On 10 February 2009 the Court dismissed the action for annulment. It recalled standard case law on the choice of a legal basis, for instance that this choice must rest on objective factors. Article 95 EC provides a legal basis where disparities exist between national rules which are such as to obstruct the fundamental freedoms or to create distortions of competition and thus have a direct effect on the functioning of the internal market, or when such obstacles are likely to emerge.[97] There is sufficient evidence submitted to the Court that is likely to be the case.[98] The Court also noted that a derogation from Directive 2002/58/EC would not be possible by an instrument of the Third Pillar without infringing Article 47 TEU.

The Court then examined the substance of Directive 2006/24/EC. It emphasized that the provisions of this Directive are essentially limited to the activities of service providers and do not govern access to data or the use thereof by the police or judicial authorities. They do not, in themselves, involve intervention by the police or law enforcement authorities of the Member States. The data at stake are solely those which are closely linked to the exercise of the commercial activity of the service providers. Here lies, according to the Court, the difference with the *PNR* cases. In *PNR,* the subject-matter was data processing which was not necessary for a supply of services by the air carriers, but which was regarded as necessary for safeguarding public security and for law enforcement purposes.[99] The Court then came to a crucial and very concise conclusion: "Unlike Decision 2004/496 [PNR] which concerned a transfer of personal data within a framework instituted by the public authorities in order to ensure public security, Directive 2006/24/EC covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law enforcement purposes."

One can easily criticize this concise approach of the Court. In the first place also in the *PNR* case the emphasis was on activities of service providers in the internal market. Indeed, the airlines are obliged to transfer the data that had been collected for commercial purposes. However, the differences mentioned above are, albeit implicitly, taken into account by the Court. In the second

96. Case C-301/06, EDPS pleading of 1 July 2008, www.edps.europa.eu ("consultation"-"court interventions").

97. Paras. 60–64 of the judgment, cited *supra* note 3.

98. Ibid., Para 71.

99. Cited *supra* note 2, paras. 80–88.

place, Advocate General Bot had come in his Opinion to a much more precisely worded dividing line.[100] Arguably such a precise dividing line is preferable from the perspective of legal certainty. However, as the Advocate General admits himself, this dividing line is subject to criticism and – more important – maybe not applicable in all situations. Therefore, the concise approach of the Court has its benefits. It acknowledges the need to keep a broad scope of application for First Pillar instruments on data protection so as to ensure a consistent and effective protection to personal data of European citizens. The data retention case represents an important landmark which brings more clarity on the dividing line between First and Third Pillar, and also on the guarantees to be provided for personal data collected in the framework of commercial activities.

However, the judgment does not solve the problem created by the fact that personal data collected for commercial purposes are used by law enforcement authorities. The division in pillars in the Treaty does not necessarily reflect this reality.

4.1.4. *The broader perspective*

Article 47 TEU as interpreted by the Court of Justice is crucial for defining the borderlines between pillars, and in particular for the correct legal basis for legislation on the use of commercial data for law enforcement purposes.

In the *ECOWAS* case[101] the Court makes clear that Article 47 TEU should be interpreted as meaning that a measure adopted under the Second or the Third Pillar affects the EC Treaty whenever it could have been adopted on the basis of the EC Treaty.[102] In other words, if a measure could be properly adopted on a First Pillar legal basis, Article 47 TEU precludes adopting it under the Second or Third Pillar. In the previous environmental sanctions case,[103] the Court went even further. According to the Court, the fact that in principle criminal law and procedure fall outside the Community competence cannot prevent Community legislators from taking measures related to criminal law that are

100. A.G. Bot suggested that "[m]easures which harmonize the conditions under which providers of communications services must retain traffic and location data which are generated or processed in the course of their commercial activities belong to the Community pillar" (para 106) while "[...] measures harmonizing the conditions under which the competent national law-enforcement authorities may access, use and exchange retained data in the discharge of their duties belong to the Third Pillar" (para 107), Opinion in Case C-301/06, paras. 106–114.

101. Case C-91/05, *Commission* v. *Council*, [2008] ECR I-3651. See on this case and on the meaning of Art. 47 TEU, Hillion and Wessel, "Competence distribution in EU external relations after Ecowas: Clarification or continued fuzziness?", 46 CML Rev. (2009), 551–586.

102. Ibid., para 60.

103. Case C-176/03, *Commission* v. *Council*, [2005] ECR I-7879.

necessary to guarantee the full effectiveness of the environmental law measures.[104]

The judgment of the Court in the *data retention* case follows *ECOWAS*, stating that since the measures can be properly adopted on the basis of Article 95 EC, Article 47 TEU would prevent their adoption on a legal basis outside the First Pillar. However, the Court does not clarify whether and to which extent the First Pillar competence could provide a valid legal ground for other measures – such as guarantees for data processing by law enforcement authorities – which, even if falling outside the scope of Community competence, would be necessary to guarantee the effectiveness of the Community instrument.

This is all the more interesting in view of the existence of a number of legal instruments under the EC Treaty laying down obligations on private parties to process certain personal data in view of possible use for law enforcement purposes, in particular in the banking and financial sector. For example, the anti money-laundering Directive[105] obliges financial institutions to retain data concerning their customers with a view to making them available to judicial and police authorities in the framework of investigations on money-laundering activities. It also defines the establishment of public authorities, including the way they should handle information collected.[106] The appropriateness of the legal basis was confirmed by Advocate General Saggio in *Commission* v. *Austria*.[107]

Personal data collected for commercial purposes by private parties (such as airlines, banks or telecommunications providers) are further used or exported for an objective – for example, fighting terrorism – not envisaged at the moment when they were collected or generated. On the basis of the case law and legislative practice mentioned above, it could be defended that the regime applicable to personal data collected or generated for commercial purposes

104. In this case, A.G. Ruiz-Jarabo Colomer highlighted that "[j]ust as the Community lacks any general power in criminal matters, it likewise does not have any 'natural capacity' under the Third Pillar either, which would act as a magnet attracting all issues of that type which arose in the European Union. The solution must be reached via a different path, along the lines intimated by the case-law when it develops the power to impose penalties as a means of protecting the Community legal order", Opinion, para 82.

105. Directive 1991/308/EEC, repealed by Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, O.J. 2005, L 309/15.

106. See, for example, Art. 21 of the Directive.

107. Case C-290/98, *Commission* v. *Austria*, [2000] ECR I-7835, where A.G. Saggio states: "I am persuaded that the money laundering directive is fully consonant with the basic substance of the provisions of the EEC Treaty – Articles 57 and 100a – on the basis of which the Council adopted the directive". The Court did not adopt any judgment, since the infringement procedure was closed further to the compliance by Austria with the obligations stemming from the Directive.

should always be laid down by Community law. This however is not what the Court decided in the *PNR* judgment.

4.1.5. *The result: A discretionary dividing line is unavoidable*

Even if the Court had decided otherwise, there would be a somewhat discretionary dividing line between the First and the Third Pillar, because from a certain stage on the use of data will be an instrument of police and judicial cooperation. The case law on the use of commercial data for law enforcement purposes is a good example of the shortcomings in the system of the EU Treaty due to the pillar structure. On the one hand, it makes clear that there will always be a discretionary dividing line between the pillars and on the other hand it demonstrates that the protection rendered under First Pillar instruments will not apply to all circumstances, in particular when the data are in the hands of the police or of judicial authorities. It is for these reasons that the case law of the Court in this area drew much attention from practitioners of EU law and has an importance which goes far beyond data protection.

4.2. *Between First and Second Pillars*

4.2.1. *Once more, the terrorists' lists*

In section 3.2, we concluded that the absence of a legal framework for data protection in the Second Pillar is a shortcoming with consequences for the individual, in particular due to the developments relating to terrorists' lists. The present section will discuss these developments from the perspective of the division between pillars.

The applicability of data protection law is a complex issue, also due to the legal structure characterizing these blacklists, where measures against certain individuals are taken on the basis of a combination of a Council Regulation (First Pillar) and a Council Common Position (Second Pillar). This complexity is reflected in the case law. The Court did not extend its assessment to Second Pillar measures directly: for example, when the Court of First Instance was asked to annul a listing made by both a Common Position and a Community Regulation, it limited the annulment to the listing in the latter instrument, declaring its incompetence to address the listing made in the Common Position.[108] Moreover, up until now the Court has not applied data protection law to terrorists' lists. It was not applied by the EU legislature either. However, there is a clear trend leading towards recognition of data protection principles in this area.

108. Case T-228/02, *Organisation des Modjahedines du peuple d'Iran (OMPI)* v. *Council*, [2006] ECR II-4665.

In a first stage, Council adopted regulations, for instance Regulation (EC) No 881/2002 on restrictive measures with regard to Al-Qaida and the Taliban [109] without any reference to the protection of personal data, nor to the protection of fundamental rights in a more general sense. In a second stage, the Court gradually recognized in its jurisprudence the need for the protection of fundamental rights without any explicit reference to data protection, but with an implicit use of elements of data protection. In a third and recent stage, the EU institutions seem to recognize the need for data protection also in this area. On 22 April 2009, the Commission adopted as a reaction to the *Kadi* judgment[110] a Proposal amending Regulation 881/2002,[111] which enhances the protection of fundamental rights, also by explicitly recognizing the necessity to ensure the protection of personal data in this area.

This trend is logical. It can even be argued that Directive 95/46 and Regulation (EC) No 45/2001 are applicable to the extent the processing of personal data in blacklists falls – even if only partly – within the scope of Community law,[112] since part of the legal framework is laid down in a Council Regulation and thus based on the EC Treaty, despite the fact that it is closely linked to a Council Common Position (Second Pillar) and activities of the United Nations.

4.2.2. *The Court uses elements of data protection*

In its case law, the Court used elements of data protection so as to ensure the protection of other fundamental rights, such as the right to defence and judicial protection.[113]

A first element of data protection in the case law of the Court is the right of access to personal data by the persons concerned, a core element of data

109. Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, O.J. L 2002, 139/9, and Common Position 2002/402/CFSP of 27 May 2002 concerning restrictive measures against Usama bin Laden, members of the Al-Qaida organization and the Taliban and other individuals, groups, undertakings and entities associated with them, O.J. 2002, L 139/4.

110. Cited *supra* note 4.

111. Proposal for a Council Regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, COM(2009)187 final.

112. Art. 3 of Regulation (EC) No. 45/2001 is in this context illustrative. The regulation applies to all "processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law".

113. Which has led some authors to define the protection of personal data as a "fundamental fundamental right". See Rouvroy, Poullet, "Self-determination as 'the' key concept", presentation delivered at the Conference "*Reinventing Data Protection*", held in Brussels on 12–13 Oct. 2007.

protection included in Article 8 of the EU Charter of Fundamental Rights. This right, which is often confused with the right to public access under Regulation (EC) No. 1049/2001[114] to documents, was of importance in *Sison*.[115] Under the latter Regulation the Council had refused access on the basis of considerations relating to public security and international relations. It also refused to disclose which Member States had provided information relevant for the blacklisting. Sison claimed a legitimate interest to obtain consultation of the documents at stake, which concern him directly and led to his listing. Therefore, according to him the access to these documents is necessary and instrumental to the effective exercise of his right of defence. The Court however emphasized that the purpose of Regulation 1049/2001 is to give the general public a right of access to documents of the institutions, and not to lay down rules designed to protect the particular interest which a specific individual may have in gaining access to one of them. Therefore, the specific interest of the applicant is irrelevant in the context of Regulation 1049/2001.[116] Nevertheless, both Advocate General Geelhoed and the Court explicitly refer to the possibility that Sison may have a right to be informed in detail of the accusation made against him and that this right may entail access to the documents held by the Council. But this right should be enforced by recourse to mechanisms other than Regulation 1049/2001.[117] Against this background, it can be argued that one of these mechanisms is the right to access one's own personal data under Regulation 45/2001. Under this Regulation, the blacklisted person has in principle a right of access to any information which has been collected and processed about him with a view to take the blacklisting decision. This right must be balanced against a possible conflicting public interest which would justify a restriction to this right. In this context, a particularly interesting and controversial issue is the access by persons concerned to their own personal data contained in EU classified documents.

Closely linked to the right of access is the right to be informed, a second element that can de deducted from the Court's case law: persons should be

114. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, O.J. 2001, L 145/43.

115. Case T-47/03, *Sison* v. *Council,* [2007] ECR II-73, and Case C-266/05 P, *Sison* v. *Council*, [2007] ECR I-1233. Sison, member of National Democratic Front of Philippines, was blacklisted by Council Decision 2002/848/CE of 28 Oct. 2002.

116. Case C-266/05 P, cited *supra* note 115, paras. 43–47. See also Opinion A.G. Geelhoed, which notes that "in the context of the application of Article 4(1)(a) of Regulation No 1049/2001 there is no place for the balancing of the public interest in respecting the confidential character of certain documents against the personal interests a citizen or entity may have in the disclosure of that document", para 82.

117. Ibid., para 48; Opinion AG, para 35.

proactively and timely informed about the processing of personal data relating to them. In this regard, one of the crucial points of the case law on terrorists' lists is the need to duly inform blacklisted persons of the reasons on which the blacklisting decision is based. In one of the latest cases concerning *OMPI* the Court found that the listing decision was in breach of the rights of defence, since the Council adopted the decision without first informing the OMPI of the new material in the file which in its view justified the blacklisting.[118]

A third element is liability. Any person who has suffered damage as a result of an unlawful processing of personal data is entitled to receive compensation for the damage suffered.[119] The Court has so far focused on the effects of freezing assets. However, the effects of blacklisting on individuals go further. It goes without saying that the mere publication of personal information – associated with the label of terrorist – is as such an interference with private life, irrespective of any restrictive measures, and is likely to damage the reputation of the individuals concerned.[120]

A fourth element is the obligation to keep personal data accurate and up to date. In this perspective, the Court has made clear that periodical revisions of the lists should be effectively carried out, otherwise the names could not be maintained on the list.[121] These are crucial guarantees not only for the rights of persons concerned, but also for the effectiveness of the fight against terrorism, as also highlighted by the US General Accounting Office:[122] inaccurate and incomplete data may lead to restrictive measures being adopted on innocent people ("false positives"), at the same time impinging on the capacity to effectively target their real addressees ("false negatives").

A fifth element relates to remedies available for persons concerned: judicial review and enforcement by data protection authorities. EU data protection standards require that persons concerned have a right to a general judicial remedy before a Court also with regard to issues relating to the processing of

118. Case T-284/08, *Organisation des Modjahedines du peuple d'Iran (OMPI)* v. *Council,* judgment of 4 Dec. 2008, nyr, para. 36.

119. Data protection laws specify this general legal principle. See Art. 10 of Convention 108, Art. 23 of Directive 95/46/EC and Art. 32 of Regulation 45/2001.

120. As put forward by the plaintiffs in different cases: Case T-49/04, *Hassan* v. *Council,* [2006] ECR II-52, para 70); Case C-229/05 P, *Ocalan* v. *Council*, [2007] ECR I-439, para 110; Case T-315/01, *Kadi* v. *Council and Commission,* [2005] ECR II-3649, para 136; Case T-47/03, *Sison,* cited *supra* note 115, para 228(f)). See also EDPS opinion, cited *infra* note 132, point 44.

121. See Case C-229/05 P, cited *supra* note 120, para 111.

122. See GAO, "Report on Terrorist Watch List Screening", October 2007, www.gao.gov/new.items/d08110.pdf, p. 43: "*TSC* ["Terrorist Screening Center"] has ongoing quality-assurance initiatives to identify and correct incomplete or inaccurate records that could contribute to either false negatives or false positives. The [...] quality of data is a high priority and also is a continuing challenge, particularly given that the database is dynamic, changing frequently with additions, deletions, and modifications".

personal data.[123] With regard to the need for an effective judicial review the Court called for procedural guarantees for reviewing blacklisting decisions.[124] In later cases, the Court reaffirms its competence to a full review on terrorist blacklists according to EU standards on fundamental rights.[125] In those cases where important restrictive measures are taken to pursue public interests, the judicial review "is all the more imperative because it constitutes the only procedural safeguard ensuring that a fair balance is struck between the need to fight international terrorism and the protection of fundamental rights".[126] According to the Court, this review cannot be effective without access to certain documents on which the listing decision is based, even if they are classified.[127]

Independent data protection authorities may also play a role in checking the lawful processing of personal data in terrorist blacklists. These authorities shall not only hear claims regarding the processing of personal data, but they are also endowed with broad enforcement powers, including both investigative powers, such as access to relevant information and premises, and effective powers of intervention, such as ordering the rectification or blocking of data and ensuring that data subjects' rights are complied with.[128] This quasi-judicial role of data protection authorities[129] may thus effectively complement the review carried out by judicial authorities.

4.2.3. *The new Commission proposal recognizes data protection*

The Commission Proposal amending Regulation 881/2002 explicitly recognizes the necessity to ensure the protection of personal data in this area and the applicability of the rights of persons concerned stemming from Regulation 45/2001.[130] This proposal does not stand alone.[131] It might even trigger a future

123. See Art. 22 of Directive 95/46 and Art. 32 of Regulation 45/2001.

124. Since concerned persons cannot address themselves directly to the UN Sanctions Committee, Member States should ensure that the case is brought before the Committee and that at national level an appeal is possible against a denial. See Case T-49/04, *Hassan*, cited *supra* note 120, paras. 116–119. On this point, see also Kunoy and Dawes, op. cit. *supra* note 59.

125. The Court rejects the arguments that blacklisting is a political question in which it has no jurisdiction and that in any case its review should be limited to "flagrant and glaring" violations of human rights, *Kadi*, cited *supra* note 4, para 272. See also Opinion A.G. Poiares Maduro, paras. 33–34.

126. Case T-228/02, *OMPI* v. *Council*, cited *supra* note 108, para 155.

127. Case T-248/08, *OMPI* v. *Council,* cited *supra* note 118, paras. 74–76.

128. See Art. 28 of Directive 95/46/EC and Art. 47 of Regulation No. 45/2001.

129. See Hijmans, "The European Data Protection Supervisor: The institutions of the EC controlled by an independent authority", 43 CML Rev. (2006), 1313–1342.

130. Cited *supra* note 111, notably Recitals 10 and 2 and Art. 7d.

131. On 29 July 2009 the Commission adopted similar proposals for Council Regulations imposing certain specific restrictive measures directed against certain natural and legal persons,

legal framework of data protection in the common foreign and security policy, in particular after the Lisbon Treaty which requires the adoption of data protection law also in this area, and grants the Court the competence to assess the legality of restrictive measures on natural or legal persons. The Commission proposal addresses several elements of data protection, which were already – implicitly – taken into account in the case law of the Court:

– It addresses the access of the persons concerned. However, Article 7d of the proposal makes the release of documents conditional upon the consent of the originator, entailing a restriction to the right of access leaving a full discretion to the originator of the document, which includes States and organizations not subjects to the EU standards of protection of fundamental rights. This may impinge on the data subjects' right of access under Article 13 of Regulation 45/2001.[132]
– It recognizes the right to be informed about the reasons for the inclusion in the blacklist and ensures that also other information is supplied to the data subject, in accordance with Article 12 of Regulation 45/2001.
– It includes procedures for revision, and thus rectification and deletion of inaccurate information.[133]
– It implies that the classification of certain documents should not stand in the way of the effectiveness of the remedies available to persons concerned both before judicial and data protection authorities.[134]

4.2.4. *The result: The pillar structure leads to more difficulties*

The Court has so far given a substantive contribution by highlighting the need to respect fundamental rights also in this area, and as a result the Commission in its proposal amending the blacklisting procedure relating to Al-Qaida and the Taliban has explicitly recognized the importance of the right to protection of personal data as well as the applicability of Regulation 45/2001 to the processing of personal data carried out by the Commission.[135] This progressive recognition confirms the relevance of a whole range of data protection principles.

entities and bodies in view of the situation in Somalia (COM(2009)393 final) and Zimbabwe (COM(2009)395 final).

132. See Opinion of the European Data Protection Supervisor of 28 July 2009 on the proposal for a Council Regulation amending Regulation (EC) No 881/2002, available at www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-28_Restrictive%20measueres_AlQaida_Taliban_EN.pdf.

133. See Arts. 7a and 7c of the proposal.

134. See, in particular, Art. 7d of the proposal. See also the criticism expressed in the EDPS opinion, cited *supra* note 111, chapter III.3.

135. See, in particular, Recitals 10 and 12 and Art. 7e of the proposal.

However it is paradoxical that due to the EU pillar structure, a clear breach of fundamental rights in the blacklisting procedure may lead to the deletion of the name from the Community list, but does not entail similar consequences for the Common position also listing specific persons. This inconsistency highlights once again the difficulties of the current data protection legal framework which has to cope with the cross-pillar reality of processing of personal data.

5. Future changes under the Lisbon Treaty

5.1. *Introduction*

This part of the article discusses to what extent the Lisbon Treaty[136] – and in particular the abolition of the pillar structure – provides instruments to address the shortcomings described before. The point of departure is that the Lisbon Treaty necessarily leads to a fundamental change in the system of data protection within the EU. It abolishes the pillar structure, which is the cause of a number of the deficiencies and it introduces a provision on data protection (Art. 16 TFEU) with general application, which means that all areas of EU law are covered. This new Article 16 TFEU is designed to be the central source of data protection within the EU.

5.2. *Article 16 of the Treaty on the Functioning of the European Union*

This new provision replaces the Treaty provision on data protection in the First Pillar (Art. 286 EC)[137] and reads as follows:

> "1. Everyone has the right to the protection of personal data concerning him or her.
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
> The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on the European Union."

136. The relevance of this part depends on the outcome of the second referendum in Ireland.
137. Art. 286 EC has a much more limited objective, as follows from its text.

Article 16 TFEU leads to important changes. It upgrades the provision on data protection from an obscure corner in the Treaty to its Title II "Provisions of general application". This title lists some important principles, such as the consistency of EU law, combatting discrimination, and public access to documents. Moreover, it has a general scope. It applies to all processing in the private and in the public sector, which includes the processing in the area of police and judicial cooperation. It also applies to processing *by the EU institutions*[138] in the area of the common foreign and security policy (the current Second Pillar). Furthermore, under Article 16(1), every natural person has a right to data protection. Article 16 TFEU mirrors Article 8 of the Charter of the Fundamental Rights of the Union which has a comparable content. Article 16(1) TFEU and Article 8(1) of the Charter are even identical.

At first sight, Article 16 TFEU solves many of the deficiencies of the current system. It requires the EU legislator to establish a stable and unequivocal legal framework for data protection under Article 16(2) TFEU. The Treaty provides all the means to do so.

5.3. *Remaining elements of the pillar structure*

However, on further examination, the solution offered by the Lisbon Treaty is more nuanced, as far as the Second and the Third Pillar are concerned.

As to the present Second Pillar: Article 39 TEU Lisbon is a specific provision for the common foreign and security policy. It applies to processing *by the Member States*,[139] which means that processing by EU institutions in this area is covered by Article 16, discussed above. Article 39 is drafted as a derogation from Article 16(2) TFEU. The main difference with Article 16 TFEU is that the European Parliament is excluded as co-legislator.

For the Third Pillar, the consequences are rather complicated. The Lisbon Treaty may lead to the end of the pillar structure, but that does not mean that Directive 95/46/EC will automatically apply to police and judicial cooperation. The scope of this Directive is limited by its Article 3(2).[140] This provision excludes the activities outside the scope of Community law and lists specifically the excluded activities (e.g. activities of the State in the area of criminal law). Arguably, the exclusion "outside of the scope of Community law" will be without substance under the Lisbon Treaty, since Community law with a lim-

138. The processing in this area by the Member States is subject to the specific rules under Art. 39 TEU.

139. See Scirocco, "The Lisbon Treaty and the protection of personal data in the European Union", Dataprotectionreview.eu, Feb. 2008, nr. 5.

140. See *supra* section 4.1.2.

ited scope excluding the Second and the Third Pillar no longer exists. However, this does not change the exclusion of the specifically listed activities (which covers more or less the same). Moreover, Declaration 21[141] states "that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the TFEU may prove necessary because of the specific nature of these fields". The meaning of this Declaration may not be completely clear, but it clarifies that in the view of the Member States the current Third Pillar will not be a normal area of law where just the general framework for data protection applies.

Furthermore, there are specific positions for certain Member States. In the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice,[142] a new Article 6a will be inserted, according to which the United Kingdom and Ireland will not always be bound by the rules laid down on the basis of Article 16 TFEU which relate to processing of personal data in the fields of police and judicial cooperation. If one of these countries does not participate in rules of police and judicial cooperation in a certain area[143] it does not have to protect data either, in that area. For Denmark a similar, even more complicated exception exists.[144]

A further complication follows from Protocol No. 36 on transitional provisions. Its Article 10 provides that the legal effects of all acts adopted before the entry into force of the Lisbon Treaty shall be preserved, until the acts are repealed, annulled or amended. According to this provision, Framework Decision 2008/977 will continue to apply although it may not fulfil the criteria of Article 16 TFEU. The same goes for international agreements published before the entry into force of the Lisbon Treaty, such as the PNR agreements between the EU and the United States[145] and between the EU and Australia.[146] Also according to Article 10 the limited competences of the Court of Justice shall not change in respect of acts adopted before the entry into force of the Lisbon Treaty, until such acts are amended or 5 years have passed. Equally, the

141. Declaration on the protection of personal data in the field of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference that adopted the Treaty of Lisbon, O.J. 2008, C 115/345.

142. Protocol No. 21, O.J. 2008, C 115/295.

143. E.g., if the UK (or Ireland) decided not to participate in EU instruments on the exchange of information on criminal records, it would not be bound by EU data protection rules as far as these Member States process data from their criminal records (NB: This example is fictitious).

144. Protocol No. 22, O.J. 2008 C 115/299.

145. Cited *supra* note 68.

146. Cited *supra* note 69. NB: The agreement with Canada was adopted under the First Pillar, so is not covered by Protocol No. 36.

infringement procedure (Art. 258 TFEU, presently Art. 226 EC) will not be applicable for a maximum period of 5 years. This means for instance that the limitations in the Court's competence under Article 35 TEU remain untouched *vis-à-vis* Framework Decision 2008/977, as long as this instrument is not repealed or modified. Only courts in Member States that made a declaration under Article 35(2) TEU can for instance request a preliminary ruling relating to is validity or interpretation.

This leads to a picture in which the basic idea of Article 16 TFEU – one stable and unequivocal legal framework for data protection in the EU – is seriously weakened by a number of exceptions. This is at least the case until the legislature uses its powers to establish such a stable and unequivocal framework and to repeal or amend existing rules, or, in the absence of such legislative activity, until the transitional period of 5 years has passed.

5.4. *A closer look at Article 16 TFEU*

5.4.1. *Article 16(1) TFEU: Direct effect*

There are strong arguments in favour of the point of view that Article 16(1) TFEU introduces the right to data protection as a right with direct effect. Firstly, it is formulated in a similar way as for instance the right of the EU citizen under the present Article 18 EC to move and reside freely within the territory of the Member States. According to the case law of the ECJ, the latter provision has direct effect. In *Baumbast*[147] the Court confirmed that "the right to reside within the territory of the Member States under Article 18(1) EC ... is conferred directly on every citizen of the Union by a clear and precise provision of the EC Treaty". Secondly, it is identical to Article 8(1) of the Charter of the Fundamental Rights of the Union. Under the Lisbon Treaty, the Charter – although not included in the EU Treaty itself – will have binding status and thus the provisions in the Charter will have direct effect, insofar as they are clear and precise enough. The status of the rights in the Charter will thus be changed, although the Court of Justice currently already acknowledges the importance of the Charter.[148] Moreover, Article 16(1) copies Article 8(1) into the body of the TFEU and by doing so gives additional value to the fundamental right. It aims at ensuring that the right can be exercised effectively, through secondary law. Thirdly, its inclusion in Title II "Provisions of general application" confirms a strong and undeniable status within the Treaty.

147. Case C-413/99, *Baumbast and R*, [2002] ECR I-7091, para 84.

148. See e.g. Case C-540/03, *European Parliament* v. *Council*, [2006] ECR I-5769 (on the right to family reunification).

These three elements are strongly connected and it is interesting to elaborate them further, starting with the parallel with Article 18 EC (after Lisbon, Art. 21 TFEU). It has been argued that the case law of the Court gave a constitutional dimension to Article 18 EC.[149] In *Grzelczyk*[150] the Court developed the assertion that Union citizenship is destined to be the fundamental status of the nationals of the Member States; a citizen has the right to move and reside freely in another Member State. In *Baumbast* the direct effect of this right was recognized.

As a consequence of the above Article 16 (1), and more in general, the right to data protection will have a similar constitutional dimension. One can even argue that all persons would have a right to data protection, even in the absence of rules specifying the right, and those persons can invoke the right before a court.

However, arguably, the right to data protection itself cannot be exercised without rules specifying the right. The right does not prohibit processing of personal data but basically formulates the conditions under which processing is legitimate.[151] Article 8 of the Charter of the Fundamental Rights of the Union lists elements of the conditions for legitimate processing. However, these elements are probably not precise enough to be invoked before a court and further rules may be needed to clarify their substance in concrete situations. Indeed, the need for precision was one of the reasons behind the adoption of Directive 95/46/EC: to give substance to and to amplify the principles contained in Convention 108.[152]

Finally, the constitutional dimension of Article 16(1) has an additional consequence: it limits the margin of appreciation of the legislature. Restrictions of the right are subject to the principle of proportionality. This consequence is not fundamentally new, since presently the test of proportionality of limitations of the right to data protection is already carried out, based on Article 8 ECHR.[153] However, this dimension can influence the interpretation of data protection law, for instance when derogations to the right to protection are analysed by the Court. This influence can possibly even extend to already existing data protection legislation.

149. See the very interesting overview by Dougan, "The constitutional dimension to the case law on Union citizenship", 31 EL Rev. (2006), 613–641.

150. Case C-184/99, [2001] ECR I-6193, paras. 31–33.

151. See Kranenborg, "Access to documents and data protection in the European Union: On the public nature of personal data", 45 CML Rev. (2008), 1086.

152. See Recital (11) of Directive 95/46/EC, cited *supra* note 20.

153. See *supra* 2.1.2.

5.4.2. *Does Article 16(2) oblige the EU legislature to provide full protection?*

Article 16(2) provides that the European Parliament and Council *shall* lay down rules on data protection. The intention of the drafters of the Treaty is clear: these institutions have an obligation to act and, more precisely, the Commission has an obligation to adopt a proposal (or more proposals).

Within the First Pillar, processing of personal data is in principle covered by Directive 95/46 and, as far the EU Institutions process data, by Regulation (EC) No. 45/2001.[154] At first sight there is no compelling reason for immediate legislative action, although Article 16 TFEU obliges European Parliament and Council to lay down rules on data protection. The main argument can be that these rules have already been enacted, albeit on another legal basis. The conditions for recourse to Article 95 EC as a legal basis will still be fulfilled[155] – although it is no longer the most appropriate choice under the new Treaty – and the choice of legal basis does not encroach upon the powers of any of the institutions.[156] Moreover, Directive 95/46/EC includes the substantive elements of Article 16 TFEU, such as control by independent authorities.

The situation with regard to the area of police and judicial cooperation is different. Here, Directive 95/46/EC does not apply. Framework Decision 2008/977 provides for a legal framework for data protection that is not applicable to domestic processing of personal data. Pursuant to Protocol No. 36, the legal effects of this Framework Decision are to be preserved, until the act is repealed, annulled or amended.

The obligation of Article 16 TFEU on the European Parliament and Council to lay down rules on data protection, also applies to the area of police and judicial cooperation. However, for two main reasons Framework Decision 2008/977 does not fulfil the criteria of Article 16 TFEU: the Council Framework Decision does not apply to all processing of personal data, since domestic processing is excluded from its scope. Furthermore, it is a legal instrument adopted by Council, not by the European Parliament and Council. Under these circumstances, the choice of legal basis encroaches upon the powers of an institution (namely, the European Parliament). In other words, since Framework Decision 2008/977 does not fulfil the criteria of Article 16 TFEU there is an obligation to replace it by a new legislative instrument.

154. The Directive is based on Art. 95 EC, the Regulation on Art. 286 EC (the Article that will be replaced by Art. 16).

155. See e.g. Case C-380/03, *Germany* v. *European Parliament and Council* (*Tobacco Advertising II*), [2006] ECR I-11573, para 39.

156. Prejudice to the institutional balance is a main reason for invalidity of EU instruments because of the choice of the legal basis. See Prechal, "Institutional balance: A fragile Principle with uncertain contents", in Heukels et al. (Eds.), *The European Union after Amsterdam. A legal analysis* (Den Haag, 1998), p. 273.

In the present Second Pillar there is currently no EU framework for data protection. Under the Lisbon Treaty, Article 39 TEU obliges the Council to lay down rules on processing by the Member States. Processing by the EU institutions in this area is covered by Article 16 TFEU. In both cases, legislative action is needed. For procedural reasons this must necessarily lead to different instruments applicable to the institutions and the Member States. In substance, these instruments can be similar.

5.4.3. *Is the obligation legally enforceable before a Court?*

Assuming that there is an obligation for Council and European Parliament[157] to lay down rules on data protection, would that obligation be legally enforceable before a Court? There are good arguments that this would indeed be the case and that an action would be possible for failure to act under Article 265 TFEU (presently Art. 232 EC). In its famous decision on the common transport policy,[158] the Court acknowledged such a possibility, provided that the failure to act relates to measures that are defined with sufficient specificity for them to be defined individually. Arguably, the obligation to adopt rules on data protection may be qualified as sufficiently specific. Of course, the Court will have to solve this matter only further to an action for failure to act lodged by an EU institution or a Member State.[159] It would be interesting to see how the Court dealt with such an action, also in the light of Protocol No. 36 on transitional provisions.[160]

5.5. *Other changes under the Lisbon Treaty*

5.5.1. *The new legal framework for judicial cooperation in criminal matters and police cooperation: Changes in substance*

On the substance, the powers of the European Union to adopt measures in the areas of judicial cooperation in criminal matters and police cooperation have not changed dramatically.[161] Most elements of Article 31 TEU are transposed to Articles 82, 83 and 85 TFEU whereas most elements of Article 30 TEU will be included in Articles 87 and Article 88 TFEU. However, there are some important changes, with potential relevance for data protection:

157. Under Art. 39 TEU: Council.

158. Case 13/83, *European Parliament* v. *Council*, [1985] ECR 1513.

159. Or, exceptionally, an individual that would fulfil the criteria of Art. 265 TFEU.

160. See para 5.3.

161. See on Lisbon and the area of freedom, security and justice, more in detail, Dougan, "The Treaty of Lisbon 2007, Winning minds, not hearts", 45 CML Rev. (2008), 617–703, para 9.

- Article 75 TFEU gives a legal basis for rules with regard to capital movements and payments, such as the freezing of funds, financial assets or economic gains, for instance for presumed terrorists or terrorist groups (but not limited to terrorism).
- Article 77(2)(d) foresees an integrated management system for external borders. This could include the introduction of an entry/exit system, allowing the electronic recording of the dates of entry and exit of third country nationals into and out of the Schengen area.[162]
- Article 77(3) contains a specific legal basis "concerning passports, identity cards, residence permits and other such documents". This legal basis could for instance be used for legislation on the use of biometrics (fingerprints, iris scan) for these documents.[163]
- Article 87(2)(a) deals with "the storage of, processing, analysis and exchange of relevant information." It replaces Article 30(1)(b), however without a link to "appropriate provisions on the protection of personal data". The absence of this link is a logical consequence of the new Article 16 TFEU which – as mentioned above – also applies to police cooperation. However, it probably does not prevent the EU legislature from including specific provisions on data processing in legislation for specific exchanges, for example the exchange of DNA-data, now the subject of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.[164]
- In the longer term, the establishment of a European Public Prosecutor from Eurojust (Art. 86 TFEU).

All in all, these are mainly specifications of already existing competences of the EU, apart from the last bullet point which will be an issue in the longer term. However, this legal framework confirms that processing of personal data, including biometric data, will continue to play an increasingly important role in police and judicial cooperation after the entry into force of the Lisbon Treaty.

5.5.2. *Changes in the institutional field*

More fundamental are the changes in the institutional field, with as most important change the introduction of the ordinary legislative procedure (qual-

162. The Commission already thinks in this direction. See COM(2008)69 final, cited *supra* note 79..

163. This is already a subject of EU intervention. See Council Regulation (EC) No. 2252/2004 of 13 Dec. 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, O.J. 2004, L 385/1, and several subsequent documents.

164. Cited *supra* note 50.

ified majority voting and co-decision) in this area. As Dougan[165] states, the Lisbon Treaty is to be applauded for this extension of this legislative procedure.

Furthermore, with regard to international agreements, Article 218 TFEU establishes the need for consent of the European Parliament in all fields where the ordinary legislative procedure applies. This will cover all the current Third Pillar area and can influence the negotiations of future PNR-like agreements, which would not be adopted without agreement of the European Parliament. Equally, those agreements will fall within the competence of the Court of Justice, including the possibility to obtain an opinion of the Court on the compatibility of an envisaged agreement with the Treaties.[166] These changes are in particular important for a possible agreement applicable to all exchanges between the European Union and the United States in the police and judicial sector.[167] Such an agreement would fully profit from the institutional arrangements under the Lisbon Treaty.

However, imperfections remain. Some of those have already been mentioned as remaining elements of the pillar structure. A new imperfection introduced is the so-called emergency brake, allowing Member States who consider that a proposal would affect fundamental aspects of its criminal justice system to refer the matter to the European Council. Another particularity is that the right of initiative of the Member States is maintained, albeit with a threshold of one quarter of the Member States[168]

All in all, the Lisbon Treaty sets an important step towards the recognition of judicial cooperation in criminal matters and police cooperation as a normal area of EU intervention, but is still far from the full recognition as such. The reluctance of Member States to hand over competences to the EU level is still felt.

An institutional change of a more specific nature is the inclusion of the agencies that have been established in the Second and Third Pillars over recent years within the "normal" legal framework of EC bodies, which means that the normal budgetary provisions and the Staff Regulations apply, and also the general framework for data protection.[169] Presently, these agencies operate outside of the scope of Community law and, as a consequence, outside this "normal" legal framework. It is also important that their acts are not subject to supervision of the Court of Justice.[170] In the Second Pillar these agencies are: the European Defence Agency (EDA), the European Union Institute for Security

165. Dougan, op. cit. *supra* note 161, p. 640.
166. Art. 218(11) TFEU replacing Art. 300(6) EC.
167. See section 3.4 *supra*.
168. Art. 76 TFEU.
169. In particular, Regulation (EC) No. 45/2001.
170. As confirmed by the Court in Case C-160/03, *Spain* v. *Eurojust*, [2005] ECR I-2077.

Studies (ISS) and the European Union Satellite Centre (EUSC). The Third Pillar includes the European Police College (CEPOL) and, of course, Europol and Eurojust.[171]

With regard to Europol and Eurojust, the processing of personal data is a core activity.[172] It also extends to the exchange of personal data with certain third countries such as the United States of America. It is therefore of the utmost importance that Europol and Eurojust are brought within the normal legal framework of the EU, despite the fact that a specific system for the protection of personal data with external independent supervision[173] has been set up for Europol as well as for Eurojust.

5.5.3. *Last but not least: Better judicial protection*

The Lisbon Treaty improves the judicial protection of the citizen in the Third and Second Pillars. This is a conclusion that can be drawn without any reservations, in any event after the expiry of transitional period of 5 years included in Protocol No. 36 and despite Protocol No. 30, which limits the application of the Charter of the European Union in Poland and the United Kingdom.[174] The individual has a right to data protection that can be invoked before a Court. This right will be specified in the rules laid down under Article 16(2) TFEU. Moreover, the European Court of Justice will be fully competent in all areas of the law of the European Union, except for the provisions and acts relating to the common foreign and security policy. However, Article 275 TFEU clarifies that the Court will be competent also in the latter area for reviewing the legality of decisions providing for restrictive measures against natural or legal persons, like – for example – blacklisting measures adopted within the framework of the common foreign and security policy.

Finally, under Article 6 TEU and Protocol No. 8, the Union shall accede to the ECHR. Accession can not be expected to lead to a fundamental change on substance of the case law of the Court of Justice. Already now, the ECHR and the case law of the Court in Strasbourg are incorporated in community law, as illustrated by *Österreichischer Rundfunk*.[175]

171. See europa.eu/agencies/index_en.htm.

172. This is best illustrated in the legal framework establishing Europol. In Art. 5 of the Council Decision establishing the European Police Office (cited *supra* footnote 45), the principal tasks of Europol are listed, to begin with: "(a) to collect, store, process, analyse and exchange information and intelligence; (Europol)".

173. By an independent joint supervisory body, see *supra* para 3.1.1

174. The limitation of the application of the Charter in those two Member States has been extensively commented by Dougan, op. cit. *supra* note 161, 665–671.

175. Cited *supra* note 17.

Vice versa, the Strasbourg Court has on several occasions scrutinized the case law of the Court of Justice and judged *on a case by case basis* that "the protection of fundamental rights by Community law can be considered to be, and to have been at the relevant time, 'equivalent' ... to that of the Convention system."[176] However, it could not directly assess the case law of the Court of Justice, but had to do so in an indirect way, assessing the implementation by a Member State. It will make a difference if an individual can directly challenge the acts of EU institutions before the European Court of Human Rights, which also includes judicial decisions of the Court of Justice. It will also make a difference if the European Union can defend its position as party before the Strasbourg Court.

6. Conclusion

Personal information has become an increasingly important tool for the State to ensure the physical security of its citizens, using the possibilities technology offers. Personal data are stored, exchanged and accessed for this purpose on a wide scale. This does not only involve police and judicial authorities of the Member States (and bodies and databases on EU level), but also private parties like airlines, telecommunications operators and financial institutions and in a globalized world also authorities of third countries. The exchange of data with the United States is a recurring issue on the political agenda. Instruments facilitating storage, exchange and access to personal information are even more predominant at the level of the EU. These instruments can be seen as the major contribution of the EU to security.

Under the rule of law, these developments require an effective system of data protection, a fundamental right of each individual. While data protection was introduced in the legal framework of the European Union as a First Pillar issue relating to the internal market, it has become a more general concern of the EU. However, this article shows that the system has important shortcomings when data are processed for Third or Second Pillar purposes.

These shortcomings are primarily caused by the state of the legislation on data protection in those pillars. In the Third Pillar, Framework Decision 2008/977 is not more than a first step towards a general framework for data protection, in combination with a number of different legislative instruments applying to different situations, which leads to much uncertainty as to applicable law. In some situations two or more conflicting instruments can apply, in other situations there is no applicable instrument of EU law. In the Second

176. Appl. 45036/98, *Bosphorus* v. *Ireland*, judgment of 30 June 2005, ECHR 2005-VI, para 165.

Pillar, the situation is simpler – no general legal framework and no specific rules – but that is not satisfactory either. Moreover, the shortcomings in the state of legislation also affect the legal framework applicable to the exchange of data with third countries.

Furthermore, the pillar structure itself leads to unsatisfactory outcomes which the case law of the Court of Justice does not fully compensate. While in *Österreichischer Rundfunk* and in *Lindqvist,* the Court gave a wide interpretation of Directive 95/46/EC, the judgments in the PNR and data retention cases did not offer a solution ensuring that consistent data protection rules would apply to all cases where data collected for commercial purposes are made available for law enforcement. In the case law on terrorists' lists, the Court offered protection in the absence of a legal framework for data protection. It used elements of data protection to ensure the protection of other fundamental rights, but that does not compensate the lack of a satisfactory system of data protection in the Second Pillar.

The Lisbon Treaty offers the necessary means to ensure an effective system of data protection applicable to all areas of EU activity, allowing the legislature to remove the shortcomings of the present legal framework for data protection in the Third Pillar – which this article earlier described as a patchwork – as well as to establish for the first time data protection rules for Second Pillar activities. Of course, much will depend on the content and on the timing[177] of the legislation that will eventually be adopted on the basis of the new Treaty, in particular by the European Parliament and Council under Article 16 TFEU.

In the meantime, much will stay the same. However, it has also been emphasized that Article 16(1) TFEU and Article 8 of the Charter may have direct effect. Moreover, the European Parliament and the Council exercise their power under the supervision of the Court of Justice, with two specific consequences: firstly, the former two institutions are obliged to act and this obligation is enforceable before the Court; secondly, the margin of appreciation of the institutions is limited by the principle of proportionality which has a specific meaning in this context in the light of the constitutional dimension of data protection.

177. Taking into account the transitional period of 5 years included in Protocol No. 36 and its interaction with the activity of the EU legislator.