in:ex

Converging and conflicting ethical values in the internal/external security continuum in Europe

European Commission, 7th Framework Programme

D.2.2 Analysis of the value dimensions of European law relevant to current and anticipated challenges of the internal/external security continuum

Deliverable submitted September 2009 (M18) in fulfilment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the Internal/External Security Continuum in Europe (INEX)

PRIO	International Peace Research Institute, Oslo	PO Box 9229 Grønland NO-0134 Oslo, Norway	T: +47 22 54 77 00 F: +47 22 54 77 01	www.inexproject.eu

INEX WP2 D.2.2.

Analysis of the value dimensions of European law relevant to current and anticipated challenges of the internal/external security continuum

Gloria González Fuster, Serge Gutwirth and Paul de Hert

Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology & Society (LSTS)

Table of Contents

Introduction

1. This working paper is dedicated to the analysis of the current and upcoming legal challenges in relation with the internal/external security continuum of the European Union (EU), and to the examination of their value dimensions. Being an element of Work Package 2[1] of the INEX project,[2] it ultimately aims at providing a basis for the pondering and elaboration of relevant recommendations with regard to the mentioned legal challenges. It builds on the analysis presented in the previous Work Package 2 report,[3] which critically reviewed the existing literature on the law-security nexus in Europe and identified a series of particularly problematic issues surfacing in such relation.

2. The present report focuses on the legal challenges linked to the discussions concerning the upcoming multi-annual programme for the Area of Freedom, Security and Justice (AFSJ) of the EU. Commonly referred to as the 'post-Hague programme,[4] or the 'Stockholm programme', the new multi-annual programme should set out the priorities for EU action in the fields of citizenship, justice, security, asylum and immigration for the period 2010-2014.[5] The European Commission (EC) published in June 2009 a Communication on such upcoming programme,[6] which has been used as the basic reference point to structure the report and delimit its scope. The main priorities introduced by the EC Communication have been further explored and contextualised below, in order to provide for a deepened understanding of the legal and ethical issues that they entail. These identified priorities include, in particular, the design of a new European information model, the sketching of a new interoperable information system architecture, various developments in relation to the control and surveillance of borders, as well as regarding communications surveillance, the construction of a comprehensive EU scheme for data protection and, finally, the drawing up of new international data protection instruments. As pointed by the EC in another context, considering the types of matters covered by the AFSJ it can be stated that it is 'unsurprising' that this policy area occupies a pre-eminent place in terms of the need to monitor the respect for fundamental rights of related legislative proposals.[7] The same applies to the need to carefully oversee connected policy programmes.

The new European information model

3. The EC Communication on the future AFSJ multi-annual programme places the development of a new European information model at the heart of the coming EU internal security strategy.[8] According to the EC, this new information model should be based on an increased strategic analysis capacity and on the enhanced gathering and processing of information. More concretely, it should be

[1] Work Package 2 is generally concerned with the 'Cross-border Legal Dilemmas of the Internal/External Security Continuum', and is directed towards the analysis of the ethical value assumptions implicit in the transnational legal dilemmas of European security practice.
[2] Converging and conflicting ethical values in the internal/external security in continuum in Europe research project, funded by the EU 7th Framework Programme for Research and Development. More information: http://www.inexproject.eu/.
[3] González Fuster, Gloria, Paul De Hert and Serge Gutwirth (2008a), *State-of-the-art of the Law-Security Nexus in Europe*, INEX Deliverable D.2.1, Brussels.
[4] As it is to represent the follow-up to the Hague Programme. On the Hague Programme, see: Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union, 2005/C 198/01, OJ C198, 12.8.2005, pp. 1-22; European Commission (2006), *Communication from the Commission to the Council and the European Parliament: Implementing the Hague Programme: the way forward*, COM(2006) 331 final, 28.6.2006, Brussels.
[5] And is expected to be adopted by the European Council in December 2009.
[6] European Commission (2009b), *Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen*, COM(2009) 262/4, 10/06/2009, Brussels. The adoption of the programme based on this Communication should be followed by the subsequent presentation of an action plan for implementation.
[7] European Commission (2009e), *Report on the practical operation of the methodology for a systematic and rigorous monitoring of compliance with the Charter of Fundamental Rights*, COM(2009) 205 final, 29.4.2009, Brussels, p. 3.
[8] European Commission (2009b), op. cit., p. 15.

designed by defining: criteria for gathering, sharing and, in general, processing of information obtained for security purposes; new assessment mechanisms; new ways of identifying future informational needs; and a series of guiding principles for a policy on international data transfers for security purposes.[9] According to the EC Communication on the future of the AFSJ, the new European information model shall contribute to more effective European police cooperation by clarifying possible channels for the exchange of information.[10] In this context, Europol, the EU law enforcement organisation,[11] shall be increasingly involved in cross-border operations, and mechanisms should be set up for automatic data transfers to its services. Additionally, the Communication regards information exchanges also as a key element for future developments in the area of criminal justice. Further work on the networking of criminal records and, in particular, on the European Criminal Records Information System (ECRIS), is believed to be able to play in the time to come a significant role in the prevention of offences.[12] Moreover, in order to boost EU capacity for analysing and collating the strategic information at its disposal, synergies between Europol and Frontex, the EU agency for external border security, are identified as requiring improvement, and networks of liaison officers in place are mentioned as needing better coordination.[13] In the opinion of the European Data Protection Supervisor (EDPS), the development of such a new European information model can be seen as the most challenging proposal of the mentioned EC Communication.[14]

4. The EC support for the design of a new European information model appears to echo the notion of a 'EU Justice, Freedom and Security (JLS) Law Enforcement Information Management Strategy' (EU IMS) discussed at Council level during the debates on the preparation of the upcoming AFSJ programme.[15] This notion has been notably tackled in different preparatory documents authored by the Informal High Level Advisory Group on the Future of European Home Affairs Policy (known as 'The Future Group').[16] According to The Future Group, the principal objective of such a EU Information Management Strategy should be to 'master' a so-called 'digital tsunami' of data allegedly threatening effectiveness in the area.[17] The Council is expected to adopt its own conclusions concerning the EU IMS, including the definition of a policy for a coherent approach on the development of information technology to support the collection, storage, processing, analysis and exchange of information, before the end of 2009.[18] Be it under the name of 'new European information model' or 'EU IMS', there is any case no doubt that a new 'EU master plan for information exchange' is on its way,[19] and that such a master plan is primarily concerned with reinforcing and diversifying information exchanges. This master plan shall consist essentially of two structural elements: a legal and strategic framework to support it, and the technical architecture foreseen to deploy it.

---

[9] Idem.
[10] Ibid., p. 16.
[11] Established as a Community agency as from 1 January 2010.
[12] Ibid., p. 17.
[13] Ibid., p. 15.
[14] European Data Protection Supervisor (EDPS) (2009b), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen*, 10 July, Brussels, p. 2.
[15] EDPS (2009b), op. cit., p. 12.
[16] See, notably: Informal High Level Advisory Group on the Future of European Home Affairs Policy ('The Future Group') (2008), *Freedom, Security, Privacy: European Home Affairs in an open world*, p. 45.
[17] Which paradoxically law enforcement authorities seem to promise to fight against, but that they are also keen to exploit for their own interests related to crime control (Hobbing, Peter and Rey Koslowski (2009), *The tools called to support the 'delivery' of Freedom, Security and Justice: A comparison of border security systems in the EU and in the US*, Briefing Paper, PE 410.681, European Parliament, p. 26).
[18] Council of the European Union (2009a), *Note from Presidency to Delegations on the Swedish Presidency: provisional agendas for Council meetings prepared by Coreper (Part 2)*, 30 June, Brussels, p. 26. A preparatory conference is foreseen for September 2009 ("Law Enforcement Information Exchange and Modern Technology" Conference, http://www.se2009.eu/en/meetings_news/2009/9/17/law_enforcement_information_exchange_and_modern_technology_cope_-09).
[19] Council of the European Union (2009b), *Note from the Swedish Delegation to Delegations on: Preparing the Stockholm Programme: Conference in Bruges 4-5 March 2009*, 10576/09, 2 June, Brussels, p. 5.

Availability / Prüm

5. The improvement of information exchanges in the AFSJ and beyond has been a major policy goal for EU institutions for already many years. Pursuing this objective, the Hague Programme had famously introduced the so-called 'principle of availability' as a guiding principle of European security efforts. The principle of availability implied that law enforcement officers from one Member State should obtain information in the course of their duties from any other Member State, and that the law enforcement agency in the other Member State shall make that information available for the stated purpose.[20] The principle of availability eventually failed to receive formal support through the adoption of any legally binding instrument by the Council.[21] Nevertheless, a series of initiatives contributing to the reinforcement of cross-border information exchanges in the AFSJ were eventually construed as contributing to the implementation of that principle. An important step in this direction was seen in the adoption by the Council in 2006 of the so-called 'Swedish initiative' to simplify the exchange of information and intelligence.[22] Eventually, EU institutions came to consider also as a modality of the development of the principle of availability the progress related to data exchanges in the Prüm framework. The so-called Prüm Decision,[23] following the agreement by different Member States on the Prüm Treaty,[24] gave to EU law enforcement authorities access on a 'hit/no-hit' basis[25] to decentralised DNA and fingerprint databases, and full online access to vehicle registration databases.[26] Additionally, and in a parallel manner, the EC carried out preparatory work on the establishment of a EU Criminal Automated Fingerprint Identification System (CAFIS), a centralised alternative for fingerprint data exchanges.[27] According to the EC, as regards the future development of the principle of availability, the focus for time being should be to ensure the effective implementation of the Prüm package and the 'Swedish initiative',[28] together with the establishment of the new overarching strategic approach to law enforcement information exchange.

6. Despite the efforts to portray the Prüm Treaty and its incorporation into the EU legal framework as a manifestation of the principle of availability, they conceptually represent quite different strategic approaches. Indeed, whereas the principle of availability targeted the establishment of a single, EU-wide modus operandi,[29] the Prüm model relies on a more flexible, in a way pragmatic

[20] European Commission (2009a), *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Justice, Freedom and Security in Europe since 2005: An evaluation of the Hague Programme and Action Plan: An extended report on the evaluation of the Hague Programme*, SEC(2009) 766 final, 10.6.2009, Brussels., p. 39.

[21] Even though the EC had adopted a proposal for such purposes: European Commission (2005c), *Proposal for a Council Framework Decision on the exchange of information under the principle of availability*, COM(2005) 490 final, 12.10.2005, Brussels.

[22] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, Official Journal of the European Union, L 386, 29.12.2006, pp. 89-100. The instrument had to be implemented by December 2008.

[23] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal of the European Union L210, 6.8.2008, pp. 1-11, and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal of the European Union L210, 6.8.2008, pp. 12-72.

[24] Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, Prüm, 27 May 2005.

[25] In case of a 'hit', exchange of personal data and case information can take place under existing mutual legal assistance procedures. Although it could seem that the fact that personal data are exchanged only if there is a 'hit', and always under the relevant data protection requirements, could be enough to ensure data protection compliance, it needs to be recalled that the automated search leading to a 'hit' or a 'not hit' is already, by itself, a processing of personal data that needs to comply with data protection requirements.

[26] See: European Commission (2009a),

[27] Ibid., p. 40.

[28] Idem.

[29] Certainly not lacking its particular problematic aspects. On this principle, see, notably: European Data Protection Supervisor (EDPS) (2006a), *Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework*

interconnection of (existing and expected) national databases. From a legislative perspective, the principle of availability was initially supposed to be developed only if backed up by the simultaneous development of a general framework for data protection, providing uniform or at least consistent provisions for all data exchanges undertaken in the AFSJ under the new principle. The Prüm model, on the contrary, has always relied on a flexible regulation by national authorities of both the databases storing the data to be exchanged and the concrete data protection provisions applicable to the exchanges.[30] Although this latter model could seem to interfere less with national realities, thus not imposing any particular data processing practice, in reality it has had the effect of pushing all participating Member States towards the reinforcement of such processing practices, and even towards the creation of new databases,[31] indirectly encouraging all Member States to attain levels of data collection and processing equivalent to those of the Member States more advanced in the field. The EDPS has interpreted the EC proposal for a new European information model as representing a more modest approach than the principle of availability originally endorsed by the Hague Programme.[32] It is nevertheless unclear whether this can be interpreted as meaning that the impetus towards increased data processing is now weaker, or simply that, as happened with the Prüm model, the impetus towards growing data processing is still strong, but the legal framework to sustain it and protect fundamental rights is far less ambitious. For the moment, EU institutions have granted less attention to the discussion and presentation of the legal conditions of the new European information model than to its architectural, technological conditions, and this despite the fact that different problematic issues have already emerged in relation with the deployment of the Prüm model. A particular issue relates to DNA databases and exchanges of DNA data.

DNA databases and data exchanges

7. The constant development of DNA databases in most of EU Member States,[33] which is certainly at least partly tributary to the Prüm Treaty and its incorporation into the EU legal framework,[34] deserves particular attention from a legal and ethical point of view. Generally, can be considered the risks inherent to an excessive multiplication of DNA databases and undue reliance on the results of the searches carried out through them, especially as incorrect or 'adventitious matches' (i.e. matches between a DNA-profile and a person who is not the donor) are always to be expected. But, more specifically, the regulation of these databases can also, *per se*, raise particular problems,

---

Decision on the exchange of information under the principle of availability (COM (2005) 490 final), 28 February, Brussels; Bunyan, Tony (2006), *The "principle of availability"*, Statewatch Analysis, Statewatch, December.

[30] National legal frameworks are notably to provide a level of protection equivalent to the level resulting from the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, European Treaty Series No. 108 ('Convention No. 108') and its Additional Protocol (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, Strasbourg, 8.XI. 2001).

[31] See, for instance: Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN; and Legge 30 giugno 2009, n. 85, "Adesione della Repubblica italiana al Trattato concluso il 27 maggio 2005 tra il Regno del Belgio, la Repubblica federale di Germania, il Regno di Spagna, la Repubblica francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria, relativo all'approfondimento della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale (Trattato di Prum). Istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA. Delega al Governo per l'istituzione dei ruoli tecnici del Corpo di polizia penitenziaria. Modifiche al codice di procedura penale in materia di accertamenti tecnici idonei ad incidere sulla libertà personale".

[32] EDPS (2009b), op. cit., p. 11.

[33] On the general proliferation of law enforcement databases in France, see: Batho, Delphine and Jacques Alain Bénisti (2009), *Rapport d'information sur les fichiers de police*, Assemblée nationale, N° 1548, 24 mars, Paris. For the UK, see: Anderson, Ross, Ian Brown, Terri Dowty, Philip Inglesant, William Heath and Angela Sasse (2009), *Database State*, The Joseph Rowntree Reform Trust Ltd., York.

[34] Even though there are certainly other factors contributing to this proliferation, and the creation of databases with biometric data is spreading for many different reasons. For instance, the Human Rights Council of the United Nations (UN) adopted a draft resolution on 20 March 2009 inviting its Member States to create national genetic databanks for the identification through forensic genetics of victims of armed conflicts or of violations of human rights and international humanitarian law.

even regardless of any eventual weaknesses related to the technical aspects of the processing of biometric data.

8. The *Marper* judgment[35] of the European Court of Human Rights illustrated certain aspects of this issue. The case, it will be recalled, concerned two complaints in which the applicants contested the retention by United Kingdom (UK) authorities of fingerprints and cellular samples and DNA profiles after criminal proceedings against them had ended with an acquittal or had been discontinued.[36] In its judgement, the Court noted that the UK was the only Member State of the Council of Europe expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued.[37] The Court concluded that the blanket and indiscriminate nature of the powers granted to UK authorities constituted a disproportionate interference with the applicants' right to respect for private life, and could not be considered necessary in a democratic society,[38] amounting therefore to a violation of Article 8 ECHR. The *Marper* judgement can be celebrated for importantly clarifying the criteria to be taken into account to limit the retention of DNA data of innocent individuals.[39] The judgement, however, also left many questions unanswered. Crucially, the Court did not examine with any particular detail *why* shall it be considered legitimate, in a democratic society, to process personal data (including sensitive data) of innocent individuals for the sake of preventing the commission of future, yet uncommitted and perhaps never to be committed crimes, even when there is no particular indication that such future possible crimes will be committed and there is no relation whatsoever between the individuals whose data is processed and the yet uncommitted crimes. Endorsing the assertion of the UK government according to which the retention of fingerprint and DNA data pursued the legitimate purpose of the *detection* of crime, the Court simply added that, because such storing pursued the *detection* of crime, it also pursued the *prevention* of crime.[40] The Court did acknowledge that two separate logics operate in this kind of systems: the original collection of information aims at linking a particular person to a particular crime of which he or she is suspected, whereas the retention of such data aims at another, different, purpose, i.e. assisting in the identification of offenders of future crimes.[41] What the Court failed to explain is why should it be considered legitimate to use for the second purpose the data collected (possibly legitimately) for the first purpose; by failing to do so, the Court seems to interpret the notion of 'prevention of disorder or crime', foreseen in Article 8(2) of the European Convention of Human Rights (ECHR)[42] in a very wide sense, which would include the prevention of any uncommitted, even unsuspected or improbable crimes. This is legally problematic because the 'prevention of disorder or crime' is mentioned in Article 8(2) of the ECHR as a possible ground to justify interferences with the right to respect for private and family life, and any restrictions of fundamental rights shall be interpreted restrictively, and never in broad terms.

9. This general consideration is directly linked to a more practical, but also fundamental, question related to the regulation of the use of DNA databases for the sake of crime detection and

---

[35] *S. and Marper v. The United Kingdom*, European Court of Human Rights, Applications nos. 30562/04 and 30566/04, Judgement of 4 December 2008. See also: González Fuster, De Hert and Gutwirth (2008a), op. cit., p. 21.
[36] Ibid., § 3.
[37] Ibid., § 47.
[38] Ibid., § 125.
[39] In particular, the *Marper* judgement can be regarded as especially relevant in the perspective of the protection both of innocents, as well as of minors (ibid, § 124).
[40] "*The Court agrees with the Government that the retention of fingerprint and DNA information pursues the legitimate purpose of the detection, and therefore, prevention of crime*", ibid., § 100.
[41] "*While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of future offenders*", idem.
[42] Council of Europe (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11*, Rome, 4 November. Art. 8 of the ECHR states: "*(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

prevention. The provisions dealing with such regulation generally establish two basic categories of criteria: first, the criteria justifying the use of the database (normally in terms of who has access, and in which conditions and for which purposes can be carried out searches), and, second, the criteria for determining which data is going to be stored in the database, and for how long. When the overall purpose of the database is the prevention of crime in its widest possible meaning, thus covering the prevention or prosecution of not yet committed crimes, in order to determine which data are to be stored, and for how long, the regulator inevitably will have to rely on criteria which are completely unrelated to the crimes that are to be prevented or prosecuted, as these are yet to happen, and therefore unknown. This inevitably leads the regulator to fix *other* criteria to determine which data is to be stored, based on grounds constitutively different from the overall purpose of the use of the database. These criteria are in most of the cases linked to the presumed commission of other crimes and offences, although it is not for the prevention and prosecution of these committed crimes and offences that the whole system is put in place.[43] Hence, two divergent standards are applied,[44] and the result is that a determined category of individuals (those which fulfil the conditions set for the collection and storage of data) tends to be artificially considered as corresponding to another category, i.e. the category of possible future offenders whose identification will be allowed via the database. In general, this shift of suspicion, from a concrete offense or crime towards the general possible commission of crimes, perverts the validity of the system from an ethical perspective.

10. The mismatch between the purpose of the processing of the data available in the databases and the criteria applied to determine which data are to be collected and stored, and under which conditions, is additionally exacerbated when access to existing databases is later widened. When this happens, the inconsistence between the criteria set for data to be originally included and stored in the database, on the one hand, and the purposes of the further processing being undertaken, on the other, is yet reinforced. This is one of the key reasons why developments such as those triggered by the Prüm model are challenging from a legal and ethical perspective: they contribute to the discussed problem by assuming that new exchanges between databases can be implemented and multiplied without fundamentally affecting the whole legitimacy of the data storage.

An interoperable information system architecture

11. The EC Communication on the upcoming ASFJ multi-annual programme asserts that, in developing the future European information model, the EU needs to give thought to the creation of a new information system architecture.[45] This new information system architecture should ensure that technical solutions adopted at national level are interoperable with existing, as well as future, European information systems.[46] Research and development in the security field is expected to be in step with these priorities and focus on improving interoperability. Moreover, according to the EC Communication, other measures should be undertaken in order to boost the EU capacity for analysing and collating the strategic information at its disposal, for instance by improving synergies between Europol and Frontex.[47] As deplored lamented by the EDPS, however, the EC Communication discusses the architecture for information exchange under the new European information model mainly in relation to the notion of 'interoperability'.[48]

[43] López Barja de Quiroga, Jacobo (2008), "El registro único de las huellas de ADN, la protección de datos y la investigación criminal" in A. Emaldi Cirión, E. Domínguez Peco, F. Aranda Guerrero, J. López Barja de Quiroga, J. Bayo Delgado, J. A. Martín Pallín, V. Moreno Catena, J. Salom Clotet, M. Pérez Sánchez, M. García-Herraiz Rooabert, R. Martínez Martínez and R. De Cospedal García (eds.), *La protección de datos en la cooperación policial y judicial*, Thomson Aranzadi, Cizur Menor, p. 291.
[44] Ibid., p. 305.
[45] European Commission (2009b), op. cit., p. 15.
[46] Idem.
[47] Moreover, networks of liaison officers in place shall be better coordinated (ibid., p. 15).
[48] EDPS (2009b), op. cit., p. 13.

Interoperability as a challenge

12. The idea of interoperability has already its own history in EU policy discussions, and was notably supported by the EC in a 2005 ad-hoc Communication on the subject.[49] At the time, the notion was criticised for its ambiguity, as it appeared to refer sometimes to the common, shared use of large scale Information Technology (IT) systems, and sometimes simply to the possibility of accessing or exchanging data stored in databases, or even to the merging of databases.[50] More critically, the term interoperability was also denounced as hiding behind the appearance of a merely technical debate much more important issues,[51] issues with significant consequences for the effective protection of the rights of individuals.[52]

13. In its Communication on the future programme for the AFSJ, the EC persists in supporting interoperability without clearly defining it. If understood as the encouragement of synergies between existing databases, interoperability inevitably implies a series of concrete legal challenges. Synergies between border-related information systems were actually already one of the central elements of the series of Communications on integrated border management, known as the 'border package',[53] presented by the EC in February 2008, and were in this context strongly criticised by the EDPS.[54] Noting that the EC envisaged in such border package the development of synergies between the Visa Information System (VIS) and two still to be created electronic systems, one for recording the entry and exit from EU territory ('entry/exit system') and a programme for 'registered travellers', and that it even considered the possible merging of the VIS and the entry/exit system, the EDPS stated that this approach was inappropriate, among other reasons, because of the risk of subverting the initial purposes for which data had been collected and stored in each respective case. The establishment of synergies between databases can indeed go against one of the basic principles of data protection law, according to which personal data can be collected only for a specific, predetermined purpose, and shall not be re-used for further purposes incompatible with the initial one. The applicable legislation can foresee exceptions to this basic principle, but only exceptionally. Moreover, when databases are interlinked, or merged, special care needs to be taken to respect the different safeguards in place for each different database, in accordance with their respective purpose, and the question of access limitations needs to be considered with special care.

---

[49] European Commission (2005a), *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*, COM(2005) 597 final, 24.11.2005, Brussels.

[50] European Data Protection Supervisor (EDPS) (2006b), *Comments on the Communication of the Commission on interoperability of European databases*, 10 March, Brussels.

[51] See, in this sense: De Hert, Paul and Serge Gutwirth (2006b), "Interoperability of Police Databases within the EU: An Accountable Political Choice?", *International Review of Law, Computers & Technology*, 20(1&2), pp. 21-35.

[52] EDPS (2009b), op. cit., p. 13.

[53] European Commission (2008c), *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*, European Commission, COM(2008) 69 final, 13.2.2008, Brussels; European Commission (2008b), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European border surveillance system (EUROSUR)*, COM(2008) 68 final, Brussels; and European Commission (2008d), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the evaluation and future development of the FRONTEX Agency*, COM(2008) 67 final, Brussels.

[54] European Data Protection Supervisor (EDPS) (2008), *Preliminary Comments on 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" COM(2008) 69 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final*, 3 March, Brussels, p. 5.

14. In its 2005 Communication on enhanced interoperability of databases,[55] the EC had relied on a questionable argumentation to support the access, in the name of prevention of crime or the fight against terrorism, to databases whose creation was unrelated to such purposes. Acknowledging that the VIS and Eurodac had not been created to store data to be processed in order to identify criminals or terrorists, the EC nevertheless claimed that, depending on the seriousness of the act committed by a criminal or terrorist under investigation, querying these databases might be justified.[56] The *Heinz Huber v. Germany* judgement[57] pronounced on 16 December 2008 by the European Court of Justice (ECJ) brilliantly illuminated the problems linked to this kind of argumentation. The *Huber* ruling allowed for the examination of, among other issues, the use for the purposes of crime fighting of databases containing personal information not collected or initially stored for such purposes. More concretely, the question was whether the use of a central register to store personal data of non-German EU citizens was compatible with the prohibition of discrimination against non-national EU citizens, with the prohibition of restrictions on the freedom of establishment of nationals of a Member State in another Member State and with the requirement of necessity under Article 7(e) of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[58] The use of the central register was actually dual: it was connected, on the one hand, to the application of the legislation relating to the right of residence and for statistical purposes, and, on the other, to the fight against crime. In relation to the latter, the Court stated that the systematic processing of personal data of non-national EU citizens for the purposes of crime fighting, when no equivalent processing is in place for nationals, constitutes a discrimination prohibited by Community law.[59] To get to such a conclusion, the Court firstly observed that the German government claimed that the protection of public order justified the use of the central register storing data of non-German EU citizens for the fight against crime, even though no similar processing was ever applied to the data related to German nationals; secondly, the Court acknowledged that the objective was as such a legitimate one, but it went on to add that it could not be relied on in order to justify the systematic processing of personal data when that processing is restricted to non-German EU citizens.[60] The Court took the view that, as the fight against crime necessarily involves the prosecution of crimes and offences committed irrespective of the nationality of their perpetrators, it follows that, as regards a Member State, the situation of its nationals cannot be different in relation to this objective from that of non-national EU citizens who are resident in its territory.[61] The ECJ, it needs to be emphasised, reached this conclusion without the need to take into account the seriousness of the crime investigated, and that seriousness would not have affected its judgement. *Mutatis mutandis*, it can be argued that the use for security purposes of databases storing data of any particular category of persons not to be considered a priori as posing a particular security risk shall be considered as discriminatory and illegitimate, and that the seriousness of the crimes investigated does not affect this assessment. Equality is ultimately one of the key values endangered by these developments.

[55] European Commission (2005a), op. cit..
[56] Ibid., p. 10.
[57] *Heinz Huber v. Germany*, European Court of Justice, Case C-524/06, Judgement of 16 December 2008, following areference for a preliminary ruling made by the Higher Administrative Court of the federal state of North-Rhine Westphalia, in proceedings between an Austrian national resident in Germany (Mr. Huber) and the Federal Republic of Germany. See, on this judgement: Lucioni, Carlo (2009), "Tutela dei dati personali del cittadino dell'Unione e giudizio di non discriminazione in base alla nazionalità", *Diritto pubblico comparato ed europeo*, 2, pp. 575-582.
[58] Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, 23.11.1995, pp. 31-50. On this directive, see: Poullet, Yves (2006), "The Directive 95/46/EC: Ten years after", *Computer Law & Security Report*, 22, pp. 206-217.
[59] See § 80 of the *Huber* judgement.
[60] Ibid., § 77.
[61] Ibid., §§ 78-79.

A new agency for de facto *interoperability?*

15. Although not formally linked to the stimulation of EU-wide interoperability of information systems, a very concrete step towards it can be found in the currently discussed establishment of a new agency for the long-term operational management of some EU information systems. As specified by the EC Communication on the future of AFSJ, the new agency should take up the management of the new Schengen Information System (SIS II)[62] and the VIS as soon as they become fully operational. Eventually, it could also be entrusted with the development of the 'entry/exit system' and the 'registered travellers' programme.[63] In June 2009, the EC already adopted an ad-hoc legislative package proposing the setting up of such agency, suggesting it could become operational as of 2012 and giving a wider view of its core mission, to include also the management of Eurodac and, in general terms, of other (at the moment non-specified) large-scale information technology systems in the AFSJ.[64] The agency, to be positioned as a centre of excellence, could also be entrusted with the development of future systems.

16. To better assess the significance of these developments, some consideration must be given to the nature and characteristics of the mentioned information systems. Despite all the technical and managerial trends towards integration and synergies among databases, the legal frameworks of SIS II, VIS and Eurodac are far from being coincidental. SIS II is established under the third pillar, whereas Eurodac is established under the first pillar, like the VIS, although a third pillar instrument was adopted to allow law enforcement authorities to have access to it. Additionally, the Member States participating in the different systems are not the same.[65] The VIS is a database that will be storing biometric identifiers[66] collected in the Member State's consular offices. Since the beginning, it will use a Biometric Matching System (BMS) built using commonly available standards already foreseen to enable seamless integration with other automated fingerprint identification systems, such as Eurodac.[67] The integration of information systems is thus progressively inscribed in their very design, and this despite their different legal characteristics and rationales.[68]

[62] The unsuccessful work towards SIS II carried out until now appears to be the main reason for EU institutions to consider the need for a new agency.

[63] The EC proposed these two measures in 2008 and would like to see them coming into operation by 2015 (European Commission (2009b), p. 19). For another measure proposed at the time, i.e. the European system of prior travel authorisation, only exchanges of views are expected for the moment.

[64] European Commission (2009c), *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, COM(2009) 293 final, 24.6.2009, Brussels; and European Commission (2009d), *Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty*, COM(2009) 294 final, 24.6.2009, Brussels. The agency should take the form of a regulatory agency, governed by a management board composed of representatives of the EC and participating countries.

[65] Ireland and the United Kingdom do not participate in VIS, are partly involved in SIS II and do participate in Eurodac. Denmark is involved in the three systems on a different legal basis. Non-EU countries such as Iceland, Norway, Switzerland and Liechtenstein are or will be associated with SIS II and VIS.

[66] The date in which operations will start is still unclear, and will depend on the eventual readiness of the Member States [European Commission (2009a), op. cit., p. 26].

[67] Ibid., p. 26.

[68] Proving that there is a certain degree of confusion, or at least ambiguity, in relation with the primary concern for certain measures promoting the access to EU large information systems, it can be noted that on 10 November 2008 the UK brought an action against the Council seeking the partial annulment of Council Decision 2008/633/JHA regarding access for consultation of the VIS by designated authorities of Member States and Europol for the purpose of prevention, detection, and investigation of terrorist offences and other serious criminal offences (Case C-482/08), and in particular of those provisions that have the effect of excluding the UK from benefiting from such access. The access was refused because the UK does not participate in the common visa policy of the Schengen *acquis*, but UK authorities argue that the measure in question is not related to the common visa policy.

Technology as the answer

17. In its presentation of the new European information model for the future ASFJ, the EC examines the technological dimension with greater detail than the legal, or ethical, dimensions of upcoming developments. Moreover, technology appears regularly as the solution to many different challenges, and is even occasionally presented as the way forward without clear identification of the ultimate aim it is to support, as if technological development and increased reliance on technology could be legitimate purposes by themselves. Like during the previous years, the EC continues to rely on the perception of a strong link between the EU security agenda and new technologies, in the understanding, for instance, that police cooperation based on new technologies is the cornerstone for successful cooperation among Member States, and that, in general, the use of technologies in all areas of justice, freedom and security policies should be at the heart of the European approach to security.[69] In this perspective, the EC has asserted that the security research and innovation agenda must continue to be taken forward, in particular in cooperation with the European Security Research and Innovation Forum (ESRIF), a public-private partnership established in 2007.[70] Additionally, working documents from the Council envisaged the possibility of establishing a European pool of security tools. Such 'tool pool' would be an innovative concept allowing Member States and EU institutions to make available and secure tools of proven or merely potential use in the security field for appraisal or testing by authorities of other Member States and, where useful, support its mutual deployment.[71] In this case, the endorsement of technology 'solutions' appears to clearly precede the evaluation of any particular need for technological 'solutions', and the promotion of security-related technologies is envisaged as a good by itself. This is certainly fully consistent with prior practices by EU institutions, as over the years EU security practices have been increasingly mediated through technological devices.[72] A major focus for the development of security technologies in the EU has been represented by borders.[73]

Control and surveillance of borders

18. The EC Communication on the future programme for the ASFJ proposes a series of priorities for the development of EU integrated border management, axed on the sustained updating of the Schengen *acquis* and increased cooperation to control flows at external borders.[74] The EC notably advocates for the different treatment at borders for private and commercial traffic, to be deployed by extending the use of new technologies and, in particular, biometrics. In its Communication, the EC also presents as a priority for integrated border management the taking into account of the situation of vulnerable people and groups, especially in reference to the need of international protection. In this area, the EC considers essential to coordinate the activities of Frontex and of the European Asylum Support Office to receive people intercepted while crossing external borders. Moreover, it states that the EU should consider a clarification of the rules applicable in the light of maritime control and surveillance, while preserving the fundamental obligation of rescue at sea.[75] Development of the European Border Surveillance System (Eurosur) is to be sustained,[76] and by 2013 cooperation

[69] Ibid., p. 59.
[70] Ibid., p. 119.
[71] Portuguese Presidency (2007), *Public security, privacy and technology in Europe: Moving forward: Concept paper on the European strategy to transform Public security organizations in a Connected World*, October, p. 4.
[72] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX D.1.1, Paris, p. 4.
[73] Ibid., p. 4.
[74] European Commission (2009b), op. cit., p. 18. It is worthwhile noting that despite all the described developments, the actual handling of border falls under the responsibility of Member States.
[75] Idem.
[76] In its final phase, Eurosur is expected to constitute a common information sharing environment in the area of border surveillance (European Commission (2008b), op. cit., p. 9) (for a critical perspective on this proposal, see: EDPS (2008), op. cit., pp. 6-7; and Jeandesboz, Julien (2008), *Reinforcing the Surveillance of EU Borders: The Future Development of FRONTEX and EUROSUR*, Research Paper No. 11, CHALLENGE).

between Eurosur, Member States and the EU agency for external border security (Frontex) should be established for the sharing of surveillance data.

Spatial surveillance

19. The management of EU's borders has developed mainly following two sometimes convergent, but in principle divergent dynamics: one tends to the reinforcement of surveillance of access to the territorial, physical borders of the EU, while the other focuses on control and surveillance operated through the new virtual, digital borders of the EU constituted by information systems.[77] The emphasis on control and surveillance has been a constant trend in the formulation of the EU's integrated border management model,[78] which has been a core element of the AFSJ since the Tampere Programme, upon which the Hague Programme was built. In 2005, the European Council launched a 'global approach to migration', which introduced as a key element the management of the southern maritime external borders. The management of the southern maritime borders is now considered an essential part of the European model for integrated border management, and has received in the latest years much more attention that expected at the time of the preparation of the Hague Programme,[79] generating principally a progressive reinforcement of the role of Frontex, the EU agency tasked to coordinate the operational cooperation between Member States in the field of border security. In this context, additionally, was conceived Eurosur, with the objective of creating a fund for improving border security and in order to launch a computerised network to exchange data and coordinate activities. EU institutions have also endorsed the concept of virtual maritime border to reinforce the legal borders of Member States by means of joint operations.

20. In this particular context of the protection of maritime borders have been deployed technical systems focusing primarily on the geographical dimension of border control and surveillance,[80] profoundly transforming such borders and the practices related to border access.[81] Maritime surveillance systems have been designed and deployed in order to detect not only movements occurring within the coastal waters of Member States, but also those in their direction.[82] This has translated into a reinforcement of the preventive dimension of these approaches, in the sense that measures to control access to the EU territory increasingly takes place before third country nationals reach the EU territory itself.[83] In this sense, it has been stated that the joint operations coordinated by Frontex involve both an extra-territorialisation of control and an over-prevention of mobility by third country nationals outside the common European territory.[84] One of the central normative questions associated to border control can be said the one concerning the determination of which actions can be taken in defence of borders, and where can they be taken,[85] especially if the location is envisaged in terms of its timing in relation with human rights obligations.

---

[77] For a discussion of the relation between EU digital borders and internal exclusion policies, see: Broeders, Dennis (2009), *Breaking down anonymity: Digital surveillance on irregular migrants in Germany and the Netherlands*, PhD Thesis, Erasmus University Rotterdam, Rotterdam.

[78] Jeandesboz (2008), op. cit., p. 3.

[79] European Commission (2009a), op. cit..

[80] Amicelle, Anthony, Didier Bigo, Julien Jeandesboz and Francesco Ragazzi (2009), *Catalogue of Security and Border Technologies at Use in Europe Today*, INEX D.1.2., Paris., p. 31.

[81] For instance, in Spain, a sophisticated technological system, Sistema Integrado de Vigilancia Exterior (SIVE), was introduced in the late 90s. Official figures confirmed that, while SIVE had drastically reduced the arrival of boats at the coasts under control, it had also diverted the immigration flows to alternative, more dangerous routes (Ceriani, Pablo, Cristina Fernández, Alejandra Manavella, Luis Rodeiro and Valeria Picco (2009), *Report on the situation of the Euro-Mediterranean borders (from the point of view of the respect of Human Rights)*, Observatori del Sistema Penal i els Drets Humans (OSPDH), Barcelona).

[82] Amicelle, Bigo, Jeandesboz and Ragazzi (2009), op. cit., p. 25.

[83] European Union Agency for Fundamental Rights (FRA) (2009), *The Stockholm Programme: A chance to put fundamental rights protection in the centre of the European Agenda*, 14 July, Vienna, p. 7.

[84] Carrera, Sergio (2007), *The EU Border Management Strategy: FRONTEX and tha Challenges of Irregular Immigration in the Canary Islands*, Centre for European Policy Studies (CEPS), CEPS Working Document No. 261, March, Brussels.

[85] Pickering, Sharon and Leanne Weber (2006), "Borders, Mobility and Technologies and Control", in Sharon Pickering and Leanne Weber (Eds.), *Borders, Mobility and Technologies and Control*, Springer, Dordrecht, p. 10.

21. Surveillance deployed at maritime borders involves various human rights issues.[86] One, often discussed, is the question of access to refugee protection and, in particular, the respect of the principle of non-refoulement of asylum seekers. The principle of non-refoulement prohibits the expulsion, deportation, rejection or extradition of persons to countries in which they would face threats or elementary human rights violations. Its relevance in the protection of EU's external borders derives from international customary law, different international treaties and European law,[87] and European border officials are bound by international human rights and refugee law also when they act extraterritorially, as actions such as turning back, escorting back, or preventing the continuation of a journey relate to sovereign territory.[88] Another human rights issue related to the protection of maritime borders is the issue of rescue at sea. This concerns the exact determination of the cases in which duties exist to rescue shipwrecked persons discovered in the course of sea observation, beyond that of rescue at sea under the law of the sea. This question has become increasingly relevant in light of the development of radar and satellite sea observation.[89] The logic of migration control has traditionally represented the key justification for the deployment of border control and surveillance, even though other rationales, such as, precisely, the prevention of lives at sea, have been progressively been mixed with this logic.[90] Most of the time, however, the respect of the rights of individuals trying to access EU borders tends to appear as a limit for control and surveillance practices, rather than a priority of the system.[91] The European Union Agency for Fundamental Rights (FRA) has argued that, considering that the situation regarding border control and surveillance at sea is particularly acute, best use should be made of the live-saving potential of the Eurosur system, and that the upcoming Stockholm programme should explicitly commit to this.[92] Additionally, current developments can invite to question the consistence of the general EU approach in relation with spatial surveillance, and whether this approach is respectful of the effective the realities of asylum seekers' pressure; in this sense, it could be argued that the significance granted to technological 'solutions' in this area might hide a resistance to discuss more profoundly political approaches.

Digital borders

22. Technology can also be integrated differently in border control strategies. Whereas at physical borders can be found fundamentally detection technologies such as radars, infrared cameras, or sensors, digital borders are commonly configured around information and communication technologies and the processing of personal data. Both types of borders are also dissimilar in terms of accessibility: while control and surveillance systems generally aim at preventing the access to, and the crossing of, physical borders, the access to digital borders is much more open, the tendency being to allow or even encourage access to them even before the individual reaches the actual physical border of the EU (through pre-entry screening measures). The difficulty for those confronted with digital borders is actually not to access them, but to leave them. In this context, it can certainly be argued that the use of technology for border control, and, in particular, the reliance on biometrics, tends to

[86] The EC has already been analysing the international law instruments in relation to illegal immigration by sea, subject on which it issued a study (European Commission (2007f), *Study on the international law instruments in relation to illegal immigration by sea, Commission Staff Working Document*, SEC(2007) 691, 15.5.2007, Brussels). The study examines the legal framework for the exercise of control and surveillance at the maritime external border and suggests further action possibly involving the adoption of instruments amending or complementing the existing legal framework. For a reflection on the impact of the multiplication of systems of border control and surveillance on the right of innocent passage, see: Amicelle, Bigo, Jeandesboz and Ragazzi (2009), op. cit., p. 34.

[87] Weinzierl, Ruth (2007), *The Demands of Human and EU Fundamental Rights for the Protection of the European Union's External Borders*, German Institute for Human Rights, July, Berlin. p. 5.

[88] Fischer-Lescano, Andreas and Tillmann Löhr (2007), *Border Controls at Sea: Requirements under International Human Rights and Refugee Law*, European Center for Constitutional and Human Rights, September, Berlin, p. 2.

[89] Weinzierl (2007), op. cit., p. 7.

[90] Amicelle, Bigo, Jeandesboz and Ragazzi (2009), op. cit., p. 25.

[91] Mirroring *inter alia* the funds allocated to control and surveillance initiatives compared with other types of measures related to migration and asylum policies.

[92] European Union Agency for Fundamental Rights (FRA) (2009), p. 8.

inscribe the border into the body of the individual on the move,[93] but it can also be supported that, perhaps more crucially, individuals on the move become themselves inscriptions in the virtual EU borders, generally for potentially undetermined periods of time.

23. Most of EU large-scale existing and possibly forthcoming border related databases have already been mentioned: they include the SIS and SIS II, the VIS, Eurodac, the Customs Information System (CIS), the 'entry/exit system' and the programme for 'registered travellers'. The list could also be extended to an electronic system of prior travel authorisation, although the preparation of this system has received lately only a relatively unenthusiastic support from EU institutions.[94] EU borders can be interpreted not as devices aimed at stopping mobility, but as devices through which 'unwanted', 'non normalised' collectives are placed under control.[95] Borders can in this light be considered as bordering processes, or 'ordering processes', i.e. processes ordering human collectives.[96] This description is especially suitable when applied to systems integrating the classification of individuals as a key, structural element: this is, for instance, the case with the foreseen programme for 'registered travellers', based on the idea of identifying a privileged group of 'good faith' travellers, which automatically classifies all other individuals as 'bad faith' travellers, to be generally distrusted. Overall distrust,[97] nevertheless, is also latent in other initiatives; in this sense, for instance, the 'entry/exit system' relies on the presumption that those entering the EU might not comply with the rules applicable to their departure.

24. The rights guaranteed through data protection law are in principle the best available tool for individuals to deal with digital borders,[98] in particular by giving them the right to access[99] the data held on them in information systems and to eventually request the rectification or deletion of such data. The fundamental right to the protection of personal data is applicable to 'everyone', and is thus not limited to EU citizens.[100] There are, however, various obstacles impeding the effective implementation of data protection in this area. A major obstacle is represented by the recurrent relativity to which is submitted the deployment of data protection rights, which are recurrently restricted by security-related exceptions and exemptions. As control border is more and more often envisaged from the wide perspective of the internal/external security continuum, the right to personal data protection of individuals on the move tends to be regularly interfered with in the name of

[93] Bigo, Bonditti, Jeandesboz and Ragazzi (2008), op. cit., p. 16.

[94] The lack of enthusiasm might be linked to the still ongoing assessment of the implications of the deployment of the Electronic System for Travel Authorization (ESTA) by the US; on this subject, see: Article 29 Data Protection Working Party (2008b), *Preliminary analysis of the US ESTA by the Art. 29 WP's PNR subgroup at the request of the EU Commission of 10 July 2008*, 24 July, Brussels; European Commission (2008a), *Commission Staff Working Document: The U.S. Electronic System for Travel Authorization (ESTA)*, SEC(2008) 2991 final, 2.12.2008, Brussels.

[95] Bigo, Bonditti, Jeandesboz and Ragazzi (2008), op. cit., p. 19.

[96] Bigo, Bonditti, Jeandesboz and Ragazzi (2008), op. cit., p. 14. See also: Amicelle, Bigo, Jeandesboz and Ragazzi (2009), op. cit., p. 16.

[97] In his comments on the EC 'border package', the EDPS precisely criticised the Communication's underlying assumption according to which all travellers can be considered a priori as potential lawbreakers and should thus be put under surveillance (European Data Protection Supervisor (EDPS) (2008), *Preliminary Comments on 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" COM(2008) 69 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final*, 3 March, Brussels, p. 5).

[98] On this topic, see: Brouwer, Evelien (2008), *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*, Leiden, Martinus Nijhoff Publishers.

[99] On the importance of the right of access, see: *Rijkeboer*, Case C-553/07, Judgement of the ECJ of 7 May 2009; and Ruiz-Jarabo Colomer (2008), *Conclusiones del Abogado General Sr. Dámaso Ruiz-Jarabo Colomer, presentadas el 22 de diciembre de 2008 (Asunto C-553/07, College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*).

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

security. This amalgamation of logics can raise important legal questions, especially in those Member States in which the right to data protection is clearly and strongly recognised as a fundamental right on its own.[101]

25. A specific area in which have been recently highlighted the weaknesses of the effective respect of the rights of the data subject, in particular the right to information and access, is Eurodac. The rights of the data subject should be foreseen in the national legal frameworks implementing notably Article 18 of the Eurodac Regulation, as well as Directive 95/46/EC, which can be considered applicable as *lex generalis*. National legal frameworks should foresee concrete provisions enabling the effective exercise of such rights. The first inspection report on the functioning of Eurodac, however, was very critical in this regard: it decried the very limited exercise of the right of access by data subjects in Eurodac and suggested that the main cause for such limited exercise is probably their lack of awareness about their rights.[102] The second inspection report reviewed national practices related to the right of information. It revealed that, in general, the information on data protection tends to be incomplete,[103] and that only one third of Member States had distinctly indicated that asylum authorities try to make sure that data subjects understand the information they are given.[104] Asylum seekers and illegal aliens usually received different information, the latter sometimes not receiving any information about their data protection rights at all.[105] The second report also indicated that there appeared to be a correlation between the information practices and the number of requests introduced by data subjects,[106] as suggested by the first report. If the legal challenge in this area is to ensure the effectiveness of a series of rights that have been formally been granted, from an ethical perspective the attention should also be directed towards the fact that this specific area of data protection (concerning non-EU citizens) does not appear to be recognised as a political priority.

26. Another issue deserving particular attention in the area of EU digital borders is the collection, storage and use for profiling practices of Passenger Name Record (PNR) data, i.e. data required by airlines to complete the booking of flights.[107] In 2007, the EC presented a proposal for a Council Framework Decision on the use of PNR for law enforcement purposes.[108] In 2008, the Council started redrafting the EC proposal to make its content reach much further than originally envisaged by the EC. Also in 2008, the FRA issued a very critical opinion on the initiative,[109] and the European

[101] In those cases, it needs to be taken into account that an eventual migration-related administrative sanction, or resolution of an administrative file, as they do not per se affect security or public order, or any other rights constitutionally protected, might not justify by themselves the sacrifice or the even the restriction of the fundamental right to data protection of individuals (Solanes Corella, Ángeles and María Belén Cardona Rubert (2005), *Protección de datos personales y derechos de los extranjeros inmigrantes*, Valencia, Tirant Lo Blanch, p. 114).
[102] Eurodac Supervision Coordination Group (2009), *Second Inspection Report*, 24 June, Brussels, p. 7.
[103] Ibid., p. 15.
[104] Ibid., p. 11.
[105] Ibid., p. 14.
[106] Ibid., p. 15. The EDPS insisted on the need to clarify the provisions regarding the rights of the data subjects, in particular underlining that the national data controllers are primarily responsible to ensure the application of these rights, in his Opinion on the new Eurodac Regulation (European Data Protection Supervisor (EDPS) (2009), *Opinion the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...][establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (COM(2008)825)*, 18 February, Brussels).
[107] Which is different from Advance Passenger Information (API), which can be described as the data contained within the machine-readable zone of a travel document (document type, issuing country, full name, travel document number, nationality, date of birth, gender, expiry date of travel document).
[108] European Commission (2007c), *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, 6.11.2007, Brussels.
[109] European Union Agency for Fundamental Rights (FRA) (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 28 October. See also: Brouwer, Evelien (2009), *Towards a European PNR system? Questions on the added value and the protection of fundamental rights*, Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 410.649, European Parliament.

Parliament adopted a similarly critical resolution.[110] Discussions at the Council are currently still ongoing. What is striking about such discussions is that they appear to touch upon decisive aspects of the proposal, such as the very purpose of the whole system, and this despite the fact that its alleged purpose might have a direct impact on the safeguards that accompany its development. Although the instrument is officially to support the making available of PNR data of passengers for the purpose of preventing, detecting, investigating and prosecuting of terrorist offences and serious crime, the explicit mention of 'border control' as an official purpose of the measure has been suggested during Council-level discussions.[111] The recognition of the fact that the processing of PNR data is envisaged for the purpose of border control would be consistent with the origins of the planned EU system, as EU reflections on this system initially took as a source of inspiration the work already carried out in the UK in the field of integrated border management, and, in particular, in relation with the e-Borders programme.[112] Besides, the discussed EU PNR system presents also other features with important legal and ethical consequences,[113] and most notably the reliance on predictive data mining. This is one of the situations in which profiling through predictive data mining[114] is particularly problematic, as statistical data are to be used to establish a classification of individuals in which those disadvantageously classified will be submitted to extra-surveillance, and thus, in this case, the notion of profiling can be judged as being closer than ever to discrimination, and be ethically be condemned by highlighting its analogy with racism.[115] It can certainly be affirmed, as already expressed by the European data protection supervisory authorities, that one of the main risks of developing a European system for PNR is that the new regime might lead to the general surveillance of all travellers.[116] It should be added, nevertheless, that another major risk is legitimising discrimination by embedding it into border control.[117]

27. Not all of EU border-related practices can be easily associated with a particular type of border control and surveillance practices, as the dynamics of physical and digital borders often interact and sometimes converge. In this light, it will be noted that Frontex currently does not process any data that could be legally qualified as personal data, as it is not legally entitled to do so. Nevertheless, it has already been suggested that new solutions could be found for Frontex to indirectly benefit from the processing of personal data, concretely by asking Member States to provide Frontex, Europol and Interpol with personal data and requesting the two latter organisations to process the data and, afterwards, make their conclusions available for Member States and for Frontex.[118] As another example of a converging practice can be cited the EC intention to allow for the use of body scanners

[110] European Parliament (2008), *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, P6_TA(2008)0561, Strasbourg.

[111] Council of the European Union (2009), *Note from the Presidency to the Multidisciplinary group on organized crime on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, 5618/2/09 REV 2, 29 June, Brussels, p. 12.

[112] The roll out of the e-Borders programme was preceded by Project Semaphore, developed from November 2004 to March 2008. The full roll out of e-Borders should take ten years, and its objective is to create an integrated and secure border using new technologies. One of its strategic aims is to enhance the security of the UK by identifying individuals who 'present a risk': using both API and PNR data, border agencies identify patterns and trends of behaviour, determine which ones appear to indicate 'risk activity', and check the data of all travellers against such 'risky activity' patterns.

[113] Another important issue, which, as the reliance on data mining, is shared with measures of monitoring of financial activities, is the participation of private parties in the implementation of a security-related measures. Private parties have been called upon to play a role for the control of migratory flows already for a long time. The Schengen Agreements of 1990 gave Member States to authority to oblige all conveyors to collaborate in the control of migratory flows.

[114] On profiling, see: Hildebrandt, Mireille and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, 2008.

[115] As profiles are to be used to attribute to individuals some behavioural facts supposed to be shared with the members of the group of which they are supposed to pertain to, distinguishing the members of such group from the rest of the population (Rigaux, François (1990), *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, p. 497).

[116] Article 29 Data Protection Working Party and Working Party on Police and Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, WP 145, WPPJ 01:07, December, p. 3.

[117] See, in this sense: González Fuster, Gloria (2009), "Law, justice and ethics for preemptive security practices" in Čas, Johann (ed.), *D 7.3 PRISE Conference Proceedings: "Towards privacy enhancing security technologies – the next steps" Vienna, April 28th and 29th 2008*, pp. 79 – 89.

[118] COWI (2009), *External evaluation of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union: Final Report*, Kongens Lyngby, p. 77.

for the screening of persons at airports.[119] In this case, detection technologies are foreseen not for the purpose of spatial, territorial surveillance, but directly for the screening of bodies crossing borders.[120]

Financial monitoring

28. In its Communication on the up-coming multi-annual programme for the AFSJ, the EC asserts that there is a need to better coordinate the work of financial information cells in the field of money laundering,[121] and puts forward that in the context of the new European information model the analysis of the different financial information cells could feed a database on suspicious transactions, to be managed possibly by Europol. Additionally, the EC calls for more integration of efforts of all available sources to identify suspicious cash transit transactions.

Monitoring and risk-based approaches

29. The Hague Programme had already emphasised the importance of establishing measures to combat the financing of terrorism, including among them the monitoring of suspicious financial flows. In this field, a key step was undertaken with the adoption of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing,[122] directed towards the improvement of the detection of suspicious financial flows notably by extending the obligation to report on suspicious transactions beyond financial institutions. Directive 2005/60/EC, generally referred to as the Third Money Laundering Directive, brought about the application of a risk based approach to customer due diligence, consisting of both the identification and verification of customer identity and the ongoing monitoring of transactions activities for suspicious of money laundering or terrorist financing. The Directive is applicable to the financial sector, as well as to lawyers, notaries, accountant, real estate agents, casinos, trusts, and company service providers. Designated bodies can carry out the assessment in the way they choose, but should in principle identify criteria to assess potential money laundering and financial risks through risk assessment techniques. They are also obliged to report any suspicion of money laundering or terrorist financing to their respective national authorities. Institutions and individuals falling under EU legislation on anti-money laundering and terrorism financing are thus bound to operate risk-based approaches to evaluate their business relations.[123]

30. From a legal perspective, the most relevant aspect of financial monitoring is its reliance on risk-based approaches and predictive data mining practices. Preparatory documents on the future multiannual programme for the AFSJ discussed predictive data mining in the field of financial monitoring in very positive terms, and suggested that it should spread from financial monitoring to

[119] On 11 March 2008 Regulation (EC) No 300/2008 of the European Parliament and of the Council on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/20021 was adopted. The aim of this Regulation is to protect persons and goods within the European Union by preventing acts of unlawful interference with civil aircraft (e.g. hijack, sabotage of aircraft). One of the means for ensuring this is to screen persons before they enter security restricted areas at airports and board an aircraft. The Commission is required by Article 4(2) of this Regulation to adopt general measures on aviation security, which must include the 'methods of screening allowed'.

[120] The European Parliament adopted a resolution stating that the measure could not be considered a mere technical measure related to security, but had a serious impact on the fundamental rights of individuals (European Parliament (2008), *Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection*, B6_TA(2008)0521, Strasbourg). To contribute to the assessment of such impact, the EC opened a public consultation in which it expressed doubts on whether the data obtained through the body scanners could be considered to be personal data or not (European Commission (2008e), *Questionnaire for the consultation on the impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection*, Brussels, p. 8).

[121] European Commission (2009b), op. cit., p. 21.

[122] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, Official Journal of the European Union L 309, 25.11.2005, pp. 15–36.

[123] Amicelle, Bigo, Jeandesboz and Ragazzi (2009), op. cit., p. 22.

many other security-related areas. In particular, it was announced that, generally, routine data monitoring and analysis should increasingly be handled by machines; the systems will then flag up exceptions (unusual behaviour and anomalies) for human investigation.[124] Emerging technologies are supposed to push this trend forward in three main areas: developing 'intelligent' responses for the monitoring of a single data stream (for instance, through CCTV); developing 'intelligent' responses for monitoring across multiple data streams, including streams of multiple types (for instance, simultaneous monitoring through CCTV and telecommunications monitoring); and progress in the type of interactions between the monitoring and humans (for instance, issuing certain types of alerts instead of simply 'flags').[125]

Data protection issues

31. Various issues related to the right to the protection of personal data have arisen in this context. In the first place, it shall be observed that Directive 2005/60/EC is directed towards the fight against both money launderers and terrorist financers. It is generally acknowledged, however, that terrorist identification via predictive data mining is not a feasible objective, and thus the patterns on which the system relies are to be regarded as merely indicative, simply suggesting in which cases further investigation may be warranted.[126] This implies that those transactions flagged as 'suspicious' are clearly recognised not as being *definitely* related to money laundering or terrorism financing, but only *possibly* related to such activities. The central problem in this regard is that, as Directive 2005/60/EC was adopted in the name of the fight against money laundering and terrorist financing, and national legislations implementing its provisions fall under the same logic and, explicitly or implicitly, tend to extend to the processing leading to (and subsequent to) the flagging of activities security-related restrictions to data protection.[127] As national legal frameworks aim at establishing limitations of data protection rights to make sure that the individuals whose transactions are being examined are not aware of it, the question is how these limitations are balanced with the right to access to data,[128] which is a structural element of the fundamental right to data protection. In principle, the limitation should be granted restrictively, and thus for the minimum period necessary. During this time, moreover, the relevant data protection supervisory authority, or the courts, should be granted powers compensating for the limitation of the right of the data subject.[129] The issue must be regarded as significant, especially if are taken into account the number of false positives that this kind of risk analysis tends to produce, and in particular the fact that, even if one of the general purposes of the measure might be the fight against terrorism or serious crime, most of the transactions flagged as suspicious would have no link at all with them. Any citizen can carry out conducts which are considered as risk conducts, and thus flagged and reported, but they will not be granted the possibility to contest such assessment.[130] The limitation, which could be accorded when there is indeed a concrete link between the conduct and terrorism or serious crime, some concrete suspicion, will in most of the cases be unfounded, and thus contrary to fundamental rights requirements.[131]

---

[124] Portuguese Presidency (2007), *Public security, privacy and technology in Europe: Moving forward: Concept paper on the European strategy to transform Public security organizations in a Connected World*, October, p. 10.
[125] Idem.
[126] National Research Council of the National Academies (2008), *Protecting Individual Privacy in the Struggle Against Terrorist: A Framework for Program Assessment*, National Academy of Sciences, Washington, D.C., p. 78-79.
[127] In some Member States, a special regime will be applicable to the files of law enforcement authorities to be used for law enforcement purposes, for which important exceptions are foreseen, limiting the right to data protection of those affected by the processing (Solanes Corella, Ángeles and María Belén Cardona Rubert (2005), *Protección de datos personales y derechos de los extranjeros inmigrantes*, Valencia, Tirant Lo Blanch, p. 75).
[128] These restrictions are extended, it will be noted, even to the processing carried out by private actors.
[129] Llaneza, Paloma (2007), "El derecho de acceso a los datos de carácter personal contenidos en los ficheros relativos a la prevención del blanqueo de capitales", *Revista Española de Protección de Datos*, 3, p. 276.
[130] In the UK, for instance, individuals wishing to make use of their right to access the data related to them stored in the database storing all 'suspicious activity reports' are unlikely to succeed because of exemptions foreseen in data protection provisions in relation with national security and crime (European Union Committee of the House of Lords (2009), *Money laundering and the financing of terrorism*, House of Lords, HL Paper 132, 22 July, London, p. 49).
[131] Llaneza (2007), op. cit., p. 279.

32. In the second place, it is unclear whether the whole system is in full compliance with fundamental requirements of transparency of data processing. The *Liberty v. the United Kingdom* judgement[132] of the European Court of Human Rights is particularly relevant for this dimension of the issue. The case concerned legislation allowing for the interception of communications between the UK and outside territory. In its judgement, the Court asserted that the law questioned did not indicate with sufficient clarity the scope or manner of exercise of the very wide discretion conferred on the State not only to intercept, but also to examine communications, as it did not set out in a form accessible to the public any indication of the procedure to be followed for the examination, sharing, storing and destroying of intercepted material.[133] The Liberty case has been interpreted as having significant implications for any State operation involving data mining or similar processes: even if information is *originally* gathered under sufficiently clear and public rules, *subsequent* treatment must be similarly precise and accessible. From this perspective, one is entitled to question whether existing national approaches to financial monitoring fully comply with these requirements, and especially how would the proposed new database on suspicious transactions and its management by Europol ensure such compliance. The use of predictive data mining takes us back again to the legal and ethical issues related to profiling: when profiles are being applied, a series of features, or conducts, which by themselves are protected by the law because they fall under the freedom of individuals, are transformed by the system into signs of pertaining to a pre-defined, suspect category. Thus, behaviours that are per se not only innocent, but also constitutionally protected, are transformed into indications of criminal activity.[134]

33. Finally, some consideration needs to be given to the situations in which suspicious transactions are stored in a database and the database itself is not sufficiently protected to ensure that the information stored is only processed for legitimate purposes. This appears to be especially problematic at the moment in the UK, in relation with the ELMER database managed by the Serious Organised Crime Agency (SOCA), which stores very large number of 'suspicious activity reports' provided by private parties.[135] The access to the database of suspicious activity reports has been judged too wide, and the data appear to be retained for unnecessarily long periods of time.[136] ELMER seems to be in practice generally available to police forces and national agencies with prosecution powers, and used for purposes unrelated to serious organised crime such as ensuring compliance with tax obligations. What is particularly worrying in this situation is that the 'suspicious activity reports' notified are not assessed before being entered into the database, and that the SOCA does not take any measure to confirm whether or not the suspicion on which it was based is well founded.[137]

Communications surveillance

34. The EC Communication on the 'Stockholm programme' advocates greater surveillance of the use of the Internet for terrorist purposes, in particular by increasing the operational capacity of the authorities responsible for monitoring, by making available suitable technical resources, and by

[132] *Case of Liberty and Others v. the United Kingdom*, European Court of Human Rights, Application no. 58243/00, Judgement of 1 July 2008. The case originated in an application against the United Kingdom and Northern Ireland lodged by a British and two Irish civil liberties' organisations on 9 September 1999 concerning the implementation of the Interception of Communications Act of 1985
[133] *Liberty*, § 69.
[134] Rigaux (1990), op. cit., p. 431.
[135] European Union Committee of the House of Lords (2009), *Money laundering and the financing of terrorism*, House of Lords, HL Paper 132, 22 July, London, p. 48.
[136] The reports are kept in the database for a default period of ten years, renewable for periods of six additional years if the entry is amended or updated (European Union Committee of the House of Lords (2009), *Money laundering and the financing of terrorism*, House of Lords, HL Paper 132, 22 July, London, p. 6 and p. 49).
[137] Ibid., p. 49.

improving the cooperation between the private and public sectors.[138] The objectives of the surveillance would be to curtail dissemination of terrorist propaganda and practical support for terrorist operations, and to facilitate the identification members of terrorist networks. It shall be recalled that interception and monitoring of communications are part of the range of special investigative techniques that law enforcement or intelligence agencies can use. In principle, their use will require judicial approval, although the exact modalities of protection can vary from Member State to Member State.

Traffic data

35. Up until now, the attention of EU institutions towards communications surveillance has mainly focused on the processing of so-called 'traffic data', i.e. data related not directly to the content of communications, but to their performance. The mandated storage of such traffic data was the core feature of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks,[139] which does not focus on the retention on content-related data.[140] The main objective is thus not to intercept communications to access their content, but, nevertheless, the storage of traffic data is not a neutral measure, as it does affect the right to respect for communications guaranteed under Article 8 of the ECHR. At the time of the adoption of Directive 2006/24/EC, critical discussions centred on how the blanket retention of data fits the requirement of necessity and proportionality.[141] Further developments have thrown the light on at least two other major issues: first, the fact that recent communication developments tend to put under particular stress the distinction between 'traffic data' and 'content data';[142] and, second, the risks inherent to the deployment of the provisions foreseen in Directive 2006/24/EC through the creation of national databases storing all the collected data.[143] Another major legal challenge in this area is to determine the legal implications of the processing of Internet Protocol (IP) addresses,[144] as depending on the particular type of processing taking place they might sometimes be protected as communications-related data or as personal data,[145] or even be left unprotected, and this qualification has a direct impact on the procedure applicable to access and process the data – the value-related discussion emerging in this area being whether the access by law enforcement authorities to this data is always appropriately framed.

---

[138] European Commission (2009b), op. cit., p. 22.

[139] 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, OJ L 105, 13.04.2006, pp. 54-63. Ireland had sought the annulment of Directive 2006/24/EC claiming it had not been adopted on an appropriate legal basis, but the ECJ decided that it relates predominantly to the functioning of the internal market and therefore had been adopted on a valid legal basis (*Ireland v Parliament and Council*, Case C-301/06, Judgement of the ECJ of 10 February 2009).

[140] Which is in principle excluded from retention, although in certain circumstances data which is not supposed to convey information about content can reveal such type of information.

[141] On traffic data retention, see: Bignami, Francesca (2007), "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law*, 8 Chicago Journal of International Law, pp. 233-254; Breyer, Patrick (2005), "Telecommunications Data Retention and Human Rights: the Compatibility of Blanket Traffic Data Retention with the ECHR", *European Law Journal*, 11(3), pp. 365-375; Poullet, Yves (2004), "The Fight against Crime and/or the Protection of Privacy: A Thorny Debate!", *International Review of Law, Computers & Technology*, 18(2), pp. 251-273. Also at stake is the right to anonymity (see, on this subject: De Hert, Paul (2003), "The case of anonymity in Western political philosophy: Benjamin Constant's refutation of republican and utilitarian arguments against anonymity" in Nicoll, Chris, Miriam Van Dellen & Corien Prins (eds.), *Digital Anonymity and the Law: Tensions and Dimensions*, Asser, The Hague, pp. 47-97).

[142] Policy Engagement Network, Information Systems and Innovation Group (2009), *Briefing on the Interception Modernisation Programme*, The London School of Economics and Political Science, London, p. 16.

[143] For progress in this direction in the UK, see: Anderson, Brown, Dowty, Inglesant, Heath and Sasse (2009), op. cit., p. 25.

[144] See, on this subject: Rodríguez Lainz, José Luis (2009), "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas", *Diario La Ley*, N° 7086, Sección Doctrina, 2 Enero 2009, Año XXIX, Ref. D-382; Martínez Martínez, Ricard (2005), "En torno a la consideración jurídica del número IP", *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, 1, pp. 283-304.

[145] See, for instance: Article 29 Data Protection Working Party (2008a), *Eleventh Annual Report of the Article 29 Working Party on Data Protection*, European Commission, Brussels, p. 43.

Deep Packet Inspection (DPI)

36. Recently, techniques directed towards the monitoring of the content of Internet communications have been receiving special attention in different fields. Deep Packet Inspection (DPI) is certainly the technique benefiting from the strongest impetus. The main difference between DPI and other, more traditional filtering technologies is that DPI offers the capability to analyse all layers of the data packets sent across the Internet.[146] DPI actively looks into the content of all communications,[147] generally in order to select a special category of communications leading to further surveillance or to other actions.

37. The EC has been considering the possible need to reinforce the monitoring of Internet not only in the name of security,[148] but also for other purposes such as the fight against child pornography. In 2004, a Council Framework Decision against sexual exploitation and child pornography was adopted;[149] in 2007, an EC report on the implementation of this Framework Decision highlighted the need for more actions in certain areas, in particular in relation with 'grooming' through the Internet, and argued that there is a need for new methods to detect these crimes.[150] Currently, already a series of countries around the world rely on filtering by internet service providers for the purpose of fighting child sexual exploitation.[151] The systematic monitoring of internet user's activities has also been discussed by EU institutions in reference to 'graduated response schemes' or 'three strikes approaches' during the debate on the adoption of a legislative resolution on the review of the Universal Service[152] and e-Privacy[153] Directives.[154] In this context, the purpose of the monitoring is to allow copyright holders to identify alleged copyright infringement. Stressing that there is no objection to the reinforcement of cooperation between authorities, copyright and internet service providers towards the protection of lawful content, the EDPS nevertheless pointed out that there is reason for concern regarding the systematic monitoring of individuals' use of the internet, independently of any suspicion of copyright infringement, on which these mechanisms typically rely.[155] The systematic monitoring of communications, on whichever grounds, ultimately questions the relevance of the notion of 'private' communications, by making the distinction between private and public communications becomes de facto irrelevant.[156]

---

[146] Wagner, Ben (2009), *Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'*, Global Voices Advocacy, p. 4.
[147] Policy Engagement Network (2009), ibid., p. 22.
[148] The EC had considered the possibility to filter out terrorism-related material, but eventually disregarded it taking into account legal obstacles and economical costs (United Nations Counter-Terrorism Implementation Task Force (CTITF) (2009), *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*, February, p. 20).
[149] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, Official Journal of the European Union L13, 20.1.2004, pp. 44–48.
[150] European Commission (2007e), *Report from the Commission based on Article 12 of the Council Framework Decision of 22 December 2003 on combating the sexual exploitation of children and child pornography*, COM(2007) 716 final, Brussels.
[151] United Nations Counter-Terrorism Implementation Task Force (CTITF) (2009), p. 20.
[152] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), Official Journal, L 108, 24.4.2002, pp. 51–77.
[153] 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), Official Journal of the European Communities, L 201, 31.7.2002, pp. 37-47.
[154] For the original proposal by the European Commission, see: European Commission (2007c), *Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation*, COM(2007) 698 final, 13.11.2007, Brussels.
[155] European Data Protection Supervisor (EDPS) (2009), *EDPS comments on some issues in the review of Directive 2002/22/EC (Universal Service)*, 16 February, Brussels, p. 1.
[156] Derrida, Jacques (1994), *Politiques de l'amitié*, Paris, Galilée, p. 166.

Reinforcing EU data protection

38. The EC Communication on the upcoming programme for the AFSJ asserts that, taking into account the challenge posed by the increasing exchange of personal data, on the one hand, and the recognition by the Charter of Fundamental Rights of the rights to privacy and data protection,[157] on the other hand, a comprehensive scheme for EU data protection should be established.[158] The EC adds in its policy document that further initiatives, legislative or non-legislative, may be necessary to maintain the application of basic data protection principles such as, for instance, those related to lawful processing of data, the rights of the individuals or independent supervision.[159] Additionally, the Communication argues in favour of the development of technologies ensuring compliance with privacy and data protection law, and advances that should be examined the introduction of a European certification scheme for privacy-aware technologies, products and services. Hence, the EC foresees possible progress in the EU policy and legal framework for privacy and data protection in three main directions: (a) the establishment of a EU-wide regime for data protection; (b) the adoption of other legislative or non-legislative ad-hoc measures; and (c) the support of privacy-compliant technologies, possibly through a privacy certification scheme. The recognition of the importance of the protection of personal data as one of the key issues of the future of AFSJ is certainly justified by the developments in the area, both current and upcoming (and especially precisely those expected under the Stockholm programme: the preparation of a new European information model, steps towards increased interoperability, reinforcement of the control and surveillance of borders, etc.).

A comprehensive scheme for EU data protection

39. Discussions regarding the convenience of establishing a comprehensive EU data protection scheme have been arising regularly during the past years.[160] The existing legal framework is indeed deeply marked by an asymmetry of protection between the EU 'first pillar',[161] in which Directive 95/46/EC provides for a uniform minimum level of protection, and the EU 'third pillar',[162] which lacks a comparable instrument. This asymmetry can be judged problematic both because of the resulting lower level of protection in the third pillar, and because of the inefficiencies derived from having to deal with divergent standards and procedures depending on the pillar concerned.

40. The move towards a single, comprehensive EU data protection framework is however generally regarded as impracticable as long as the EU maintains its existing pillar structure. Under the current treaties, the adoption of a comprehensive legal framework applying to all processing appears extremely difficult, due to the pillar structure in itself and also to the fact that the protection of personal data processed by EC institutions is linked to a specific legal basis.[163] Nevertheless, the entry into force of the Lisbon Treaty would position Article 16 of the Treaty of the Functioning of the European Union (TFEU) as the new legal basis to be used to establish a comprehensive legal

[157] In Art. 7 and Art. 8 of the Charter (Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 303, 14.12.2007, pp. 1-16). On this topic, see: Arenas Ramiro, Mónica (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant Lo Blanch; Bygrave, Lee A. (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague, London, New York, Kluwer Law International; De Hert, Paul and Serge Gutwirth (2006a), "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power", in E. Claes, A. Duff & S. Gutwirth (Eds.), *Privacy and the Criminal Law*, Antwerp-Oxford, Intersentia, pp. 61-104; Gutwirth, Serge (2002), *Privacy and the information age*, Lanham, Rowman & Littlefield Publishers; Siemen, Birte (2006), *Datenschutz als europäisches Grundrecht*, Berlin, Duncker & Humblot.
[158] European Commission (2009b), op. cit., p. 8.
[159] Idem.
[160] See, on this topic: González Fuster, Gloria and Serge Gutwirth (2008), *Data protection in the EU: Towards 'Reflexive Governance'?* , REFGOV Working Paper Series, FR-19, Brussels.
[161] Concerning Community matters.
[162] Falling under Title VI of the TEU.
[163] Namely, Art. 286 TEC.

framework for data protection.[164] Future action in this field looks thus to be put on hold until the possible adoption of the Lisbon Treaty.[165] Under the current conditions, the EC has already tried to improve the situation, and thus to reduce the gap between the first and the third pillar, by pushing for the adoption of a third pillar legal instrument ensuring a level of protection which could be considered, if not fully equivalent to the one guaranteed by Directive 95/46/EC, at least similar to it. In this perspective was originally presented and discussed, during the period falling under the Hague Programme, the EC proposal[166] that eventually lead to 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.[167] Nevertheless, Council Framework Decision 2008/977/JHA, adopted after three years of exchanges of views in the Council, finally failed to provide any consistent protection for data processing falling under the third pillar.[168] According to the EDPS, the replacement of such Council Framework Decision should a priority under the Stockholm programme.[169]

Other legislative or non-legislative measures

41. Despite the formal support granted to the right to personal data protection as a fundamental right in the EU, different serious lacunae are persistent in the legal framework supposed to develop it.[170] These lacunae concern not only the lack of inter-pillar consistency, but also the quality of the protection ensured both in the first and in the third pillar. It is thus understandable that the EC mentions in its Communication on the future AFSJ programme the possible adoption of more measures in the field.

42. During the period falling under the Hague Programme, the EC has regularly considered the possible need to revise the basic instrument of EC (first pillar) data protection, i.e. Directive 95/46/EC, but systematically concluded that the mentioned Directive did not require any review.[171] Nevertheless, it is generally acknowledged that many efforts are still needed to reinforce the effective implementation of existing safeguards.[172] The EC itself recently took concrete steps towards a deeper examination of the necessity to proceed to such review by opening a public consultation on the EU legal framework for the fundamental right to protection of personal data.[173] Concerning the third

[164] EDPS (2009b), p. 6. Art. 16(1) TFEU states: "*Everyone has the right to the protection of personal data concerning them*". Art. 16(2) establishes: "*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*".

[165] See, on this subject: Bayo Delgado, Joaquín (2008), "La cooperación internacional policial a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos" in A. Emaldi Cirión, E. Domínguez Peco, F. Aranda Guerrero, J. López Barja de Quiroga, J. Bayo Delgado, J. A. Martín Pallín, V. Moreno Catena, J. Salom Clotet, M. Pérez Sánchez, M. García-Herraiz Rooabert, R. Martínez Martínez and R. De Cospedal García (eds.), *La protección de datos en la cooperación policial y judicial*, Thomson Aranzadi, Cizur Menor, p. 35.

[166] European Commission (2005), *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, COM(2005) 475 final, 04.10.2005, Brussels.

[167] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350, 30.12.2008, p. 60–71.

[168] See, on this Council Framework Decision: Bayo Delgado, Joaquín (2008b), "La protección de datos en la investigación policial y en el proceso penal", *Jueces para la Democracia, Información y Debate*, 63, pp. 11-24.

[169] EDPS (2009b), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen*, 10 July, Brussels, p. 8.

[170] González Fuster, De Hert and Gutwirth (2008a), op. cit., p. 11 et seq.

[171] See: European Commission (2003), *First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, 15.5.2003, Brussels; European Commission (2007b), *Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, COM(2007) 87 final, 7.3.2007, Brussels.

[172] See, notably: European Data Protection Supervisor (EDPS) (2007), *Opinion on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, 25 July, Brussels.

[173] Open from July 9, 2009 to December, 31 2009.

pillar, it must be noted that in the persistent absence of a horizontal, harmonising EU instrument on the protection of personal data in police and judicial cooperation in criminal matters, the applicable rules continue to be determined by a variety of legal texts, the scope and nature of the requirements being dependent on the specific objective of the text and on the personal data processed.[174] The EC has asserted that the focus in this area should be directed towards the monitoring of the implementation and application of the relevant legal instruments and the development of a new system of oversight and advice for the protection of personal data, specific for the area of police and judicial cooperation.[175] None of these suggestions is particularly innovative, and the main weakness of the proposed action may lie in the lack of concrete suggestions on how to put forward measures that until now have been vigorously resisted by the Council.

43. The EC points out in its Communication on the future programme for the AFSJ the need to reaffirm and further develop a series of key principles of data protection. A principle that appears as crucial, but is not mentioned by the EC, is the need for transparency of processing practices. Transparency of processing plays indeed an instrumental role in allowing data subjects to exercise their rights, and is particularly problematic in the law enforcement area.[176] Another very important issue not addressed by the EC in the mentioned Communication are the implications for data protection of the involvement of private actors in security-related practices, an involvement that has been encouraged by the EU legislator through different measures, be it the Data Retention Directive, the different instruments related to PNR data, or financial monitoring.[177] The key question in this light is how to ensure in these circumstances effective control on the use of data, be it by the data subject, data protection supervisory authorities or the judiciary.[178]

Putting privacy and data protection into technology

44. The development of technologies ensuring compliance with privacy and data protection provisions has also been explored by the EC for already some years. With the aim of encouraging the use of Privacy Enhancing Technologies (PETs), the EC issued in 2007 an ad-hoc Communication.[179] However, as no other concrete action has been undertaken in this direction, the EC support to PETs has been limited so far to the expression of an intention to continue to promote these technologies and encourage data controllers and consumers to adopt them.[180] The main challenge for future policy decisions regarding notions such as 'privacy by design', PETs or, in general, privacy-aware or privacy enhancing technologies, is the determination of the concrete instruments to be used for their support.[181] The certification scheme mentioned by the EC in its Communication is a possibility, but not the only one. A more vigorous approach would be implemented by imposing legal obligations, as recalled by the EDPS in his Opinion on the EC Communication.[182]

45. The institutional support for PETs was also examined in preparatory documents on the future multi-annual programme for the AFSJ, but from another perspective. Some of these preparatory documents were much more sceptical than the EC Communication: pointing out that although PETs

[174] European Commission (2009a), op. cit., p. 46.
[175] Idem.
[176] EDPS (2009b), op. cit., p. 9.
[177] Idem, p .13. Or, in other terms, the diversion for generic security purposes of personal data collected for commercial purposes.
[178] Idem, p .14.
[179] European Commission (2007a), *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 final, 2.5.2007, Brussels.
[180] González Fuster, De Hert and Gutwirth (2008a), op. cit., p. 19.
[181] In addition to supporting PETs, there is also room for a more decisive taking into account by the legislator of the implications of the increasing importance of information technology for the development of personality; for instance, in the line of the recognition by the German Constitutional Court of the right to 'confidentiality and integrity of information systems' (judgement published on 27 Feb 2008, Online-Durchsuchung, 1 BvR 370/07; 1 BvR 595/07).
[182] EDPS (2009b), op. cit., p. 10.

can have a beneficial impact on privacy and data protection, they can also be used by terrorists and other criminals for undesired purposes, it was explained, for instance, that by automatically rendering data anonymous after a certain lapse of time may be erased the evidence of crimes; that encryption tools may help conceal criminal plans; and that privacy-enhancing cookie-cutters may make ineffective police efforts to gather information on illegal activities.[183] This line of reasoning mirrors what appears to an understanding shared by different law enforcement authorities in Europe, according to which the use of PETs tends to be interpreted as an indication of suspect behaviour, instead of as a legitimate way of ensuring the effectiveness of a fundamental right. As EU institutions get caught between this train of thought and their vehement support for technology in the AFSJ, it is not sure that they will soon decide to finally intercede for PETs in another way than through injecting resources to the research and development.

International data protection instruments

46. When discussing privacy and data protection, the EC Communication on the future AFSJ programme establishes that the EU must position itself as a driving force behind the development and promotion of international standards for personal data protection, as well as for the conclusion of related bilateral or multilateral instruments, in the understanding that already engaged discussions on data protection could be used as a basis for future bilateral or multilateral agreements.[184] During the period the Hague Programme, the EU and its Member States received multiple requests from third countries to use the personal data of EU citizens for law enforcement purposes. These requests concerned notably the use of PNR data for law enforcement purposes (e.g., from the US, Canada, Australia and South Korea) and the access to financial transaction data (US).[185] This lead the EC to consider the advantages of having an overall strategy on the transfer of personal data eventually enabling the EU to play its role in the development of international standards and in the conclusion of international instruments (bilateral or multilateral).[186]

Global standards

47. The necessity for any regulation dealing with data protection to take into account the international dimension of data transfers has been clear over the decades. Conscious of the possible temptation for data controllers to escape from data protection obligations by transferring data outside of the scope of application of national or regional provisions,[187] decision-makers have generally opted to simultaneously foreseeing specific provisions regulating the export of personal data, on the one hand, and encouraging international cooperation to raise the global level of protection, on the other. In Europe, the issue of data exports has generally been approached by requiring from those wishing to export data to a third country to ensure an 'adequate level of protection' for such data. Directive 95/46/EC, in particular, established as the basic principle for data transfers to a third country the requirement that the third country in question ensures an 'adequate level of protection'.[188] Although the notion of 'adequate protection' can sound rather vague, the EU has developed over the years a

[183] Portuguese Presidency (2007), *Public security, privacy and technology in Europe: Moving forward: Concept paper on the European strategy to transform Public security organizations in a Connected World*, October, p. 8.
[184] European Commission (2009b), op. cit., p. 8.
[185] European Commission (2009a), op. cit., p. 116.
[186] Idem.
[187] The scope of application of Directive 95/46/EC depends on two principles: the principle of establishment (which is interpreted differently from Member State to Member State) and the principle of the automated means (generally interpreted in very large terms) (see Art. 4(1) of Directive 95/46/EC).
[188] Art. 25(1) of Directive 95/46/EC. There are however also other mechanisms to allow for data transfers to third countries; see, notably: Article 29 Data Protection Working Party (2008c), *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, WP 155 rev.01, 1 October, Brussels; Article 29 Data Protection Working Party (2009), *Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor*), WP 161, 5 March, Brussels.

special formal procedure and methodology to assess the 'adequacy' of the protection granted and to officially recognise it as such.[189] Up until now, however, only a limited number of third countries have been recognised as having achieved such a status. The system has been criticised for its slowness, but it has also been praised for having helped to ensure that third countries around the world see EU data protection as an inspirational model.

48. While the relevance of the 'adequacy principle' has never been officially questioned, the idea that the EU should, additionally, work in order to raise internationally the level of privacy and data protection has been gaining impetus over time. Different proposals for new international instruments have been discussed in different fora.[190] Currently, a particularly followed initiative is being carried out by the International Conference of Privacy and Data Protection Commissioners, coordinated by the Spanish data protection supervisory authority. The initiative originated in the 2008 International Conference of Privacy and Data Protection Commissioners[191] and it reflects the collective effort of international supervisory authorities.[192] For European supervisory authorities, it has the main advantage of providing an opportunity to try to influence international privacy and data protection discussions; such opportunities tend to be rare, as their positions are often ignored by EU institutions in relation with negotiations in this area.[193] The definitive version of the proposal adopted by International Conference of Privacy and Data Protection Commissioners shall be made public in November 2009.

49. The key legal challenge in relation to these developments is to determine the relation between any future international data protection instrument to which the EU might subscribe and the fundamental EU principle of 'adequate level of protection'. Ultimately, the main dilemma concerning the development of any new international data protection instrument, be it a multilateral or a bilateral instrument, relates indeed to its relation with the existing European system and, in particular, with EU provisions on international transfers. From a European perspective, lifting up the adequacy requirement would mean that data could be exported to third countries not ensuring a basic level of protection, a measure that would have a direct impact on the level of protection guaranteed in EU territory. From the point of view of third countries, if adopting and implementing a new international data protection instrument does not allow them to facilitate data exports from the EU, the profit for them of adhering to such an initiative might be unclear. The answer provided to this challenge by the initiative being coordinated by the Spanish supervisory authority is yet unknown. A draft version of the text,[194] however, presented a worrying solution: it established that regions could apply higher levels of protection than the level granted by the new standards[195] but that those higher levels could

[189] At EU level, the recognition has to follow a 'comitology' procedure; by virtue of an EC decision based on Art. 25(6) of Directive 95/46/EC, personal data can flow from the 27 EU member states and three European Economic Area (EEA) member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.

[190] See, for instance: Cavoukian, Ann (2006), *Creation of a Global Privacy Standard*, Information and Privacy Commissioner of Ontario,

[191] In 2008, they approved the mandate for the Working Group preparing such international standards, based on three main ideas: a) the right to data protection and privacy are fundamental rights of individuals; b) the rise of information society has led the right to data protection and privacy to become essential for guaranteeing respect for human rights; c) in a globalized world, the persisting differences in the field of data protection and in the respect for privacy are detrimental to the implementation of an effective and global data protection.

[192] The international community of data protection supervisory authorities has also called for the United Nations (UN) to draw up a binding legal instrument on the right to data protection and privacy. In 2005, the international data protection supervisory authorities also asked the Council of Europe to invite those States that, although they are not members of the Organisation, do have appropriate laws in the field of data protection, to adhere to the Convention for the protection of individuals in respect of the automatic processing of personal data (STE Nº 108) and to the additional Protocol (STE Nº181).

[193] European data protection supervisory authorities have been regularly criticising agreements negotiated between the EU and the US for the exchange of personal data, for instance regarding the processing of PNR data. See, for instance; Article 29 Data Protection Working Party (2007), *Opinion 5/2007 on the follow-up 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 concluded in July 2007*, Adopted on 17 August 2007, Brussels.

[194] Agencia Española de Protección de Datos (AEPD) (2009), *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data*, Version 3.

[195] "*The provisions in this document should be considered as minimum requirements, which may be supplemented by additional measures for the protection of privacy with regard to the processing of personal data*" (ibidem, p. 2).

not be used to block data flows when a protection similar to the one provided by the new standards was ensured.[196] In practice, the content presented in the draft version would replace the 'adequate level of protection' principle, which referred to 'adequate' in comparison with the EU level of protection, with a 'similar protection' principle, establishing that data can be transferred to any country providing for protection similar to the one ensured by the new instrument.[197] Adding to this the fact that, comparatively, international regimes for the protection of personal data[198] tend to diverge precisely on issue of safeguards (or lack of safeguards) they foresee for cross-border data flows,[199] it has to be considered that once data have left EU territory to a country providing only 'similar' protection, they might then be further transferred with no particular protection whatsoever. In the end, the value-related debate that might need to take place in this area concerns the identification of elements of data protection that the EU considers essential and non-negotiable, and those that might be open to discussion.[200]

EU-US data flows

50. The need for new international instruments dealing with data protection can be contextualised in a general will to raise global levels of protection, but it also needs to be linked to the possibility for the EU to open its new European information model to third countries. There is no mention in the EC Communication on the new multi-annual programme for the AFSJ on the degree of openness to the new European information model to third countries. In contrast, preparatory documents did discuss with great emphasis the possible support of a Euro-Atlantic area of cooperation with the United States (US). The key question in this area is how far can the EU go in this kind of discussions without giving up European protection, or how to ensure that any new agreement is fully compatible with European values.[201]

51. Several initiatives have already been taken to back up the transfer of personal data from the EU to the EU.[202] The EU-US High Level Contact Group on information sharing and privacy and personal data protection finalized its report in June 2008,[203] and since then the report has been regarded as a positive step for the future preparation of any other agreements. On 27 July 2009 the EU Ministers of foreign affairs gave a mandate to the EC and the Swedish EU Presidency to negotiate a temporary agreement with the US giving the latter access to European bank data from the Society for Worldwide Interbank Financial Telecommunication (SWIFT) that would last until the Lisbon Treaty is finally ratified. In 2007, a first agreement had been reached between the US and the EU to establish

---

[196] "*The additional measures provided in the preceding paragraph may not be an obstacle to international transfers of personal data, where they are carried out pursuant to section 14 of this Document*" (idem).

[197] "*As a general rule, international transfers of personal data may be carried out when the State or organization recipient of such data afford a substantially similar level of protection to that one provided in this Document*" (ibidem, p. 3).

[198] Among other initiatives needs to be mentioned the Asia-Pacific Economic Cooperation (APEC) privacy initiative, which involves a Framework, with Privacy Principles, adopted by Ministers of the 21 APEC economies in 2004. An implementation part was added to the Framework in 2005, and encourages both domestic implementation of the Principles by individual members and continuing multilateral work, by a Data Privacy Sub-group, primarily in the development of a Cross Border Privacy Rules (CBPR) approach to cross border transfers of personal data.

[199] Other issues in which there are important divergences are, in particular, the determination of the grounds legitimising the processing of data and the question of compliance and monitoring.

[200] This identification might be difficult as, for instance, Art.8(3) of the EU Charter of Fundamental Rights introduces as a key element of the fundamental right to the protection of personal data the existence of a supervisory authority, which is one of the aspects of EU data protection more regularly contested internationally.

[201] Hobbing and Koslowski (2009), op. cit., p. 38.

[202] On this topic, see: Adam, Alexandre (2006), "L'échange de données à caractère personnel entre l'Union européenne et les Etats-Unis: Entre soucis de protection et volonté de coopération", *Revue trimestrielle de droit européen*, 42(3), pp. 411-437 ; and De Hert, Paul and Rocco Bellanova (2008), *Data Protection from a Transatlantic Perspective: the EU and US Move Towards an International Data Protection Agreement?* , Study, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, PE 408.320, October.

[203] Council of the European Union (2008), *Note from the Presidency to COREPER on the EU-US Summit, 12 June 2008: Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 9831/08, 28 May, Brussels. See also: González Fuster, De Hert and Gutwirth (2008a), op. cit., p. 26.

which data can be accessed by US authorities and in which conditions.[204] The EDPS has made it clear that in his view any agreement with the US on data protection and data exchange should be based on Convention N° 108 of the Council of Europe and the relevant case law of the European Court of Justice and the European Court of Human Rights.[205] From his perspective, all general agreements with third countries shall be based on the level of protection guaranteed within the territory of the EU.

Concluding remarks

52. The paper has allowed for the examination of some key priorities identified by the EC for the future of the AFSJ. Suggested developments have been contrasted with legal requirements as derived from existing legal instruments and relevant case law, and special care has been taken in describing the value dimensions linked to the compliance with such legal requirements. The previous report of Work Package 2 had emphasised the importance of various subjects as urgently requiring further attention: the use of new metaphors guiding political choices in the deployment of security policies in Europe, such as the triangle 'mobility, security and privacy'; the double nature of data protection law, which can constitute both a limiting factor for personal data processing, and an enabler for such data processing, data protection law having thus potentially ambiguous effects when deployed as counter-balancing force against increasing security-related interferences with the rights of individuals; the lack of vigorous promotion by European institutions of 'privacy-by-design', coupled with the generalisation of what can be called an 'impossibility of privacy (by law and) by design', as backed up by different policy decisions; the many legal and ethical questions raised by profiling through predictive data mining, singularly in relation with security practices; and the significant recent case law of the European Court of Human Rights and of the European Court of Justice in relation with all these issues. In a way or another, all these subjects have been encountered again in the present review of the current and upcoming challenges for the AFSJ.

53. We have notably portrayed the value dimensions connected to the particular ordering of the priorities discussed, which commonly tends to place the respect for fundamental rights in the second place in any lists of objectives: in this sense, for instance, the elaboration of a new European information model is reckoned as an objective of paramount relevance, while the effective respect of the fundamental right of personal data protection is viewed as an imposed condition to attain such main objective; similarly, maritime surveillance is supported for control and security purposes, and only when its deployment seems to frontally confront fundamental rights of the individuals are these brought back into the picture.

54. The analysis of the currently discussed paths for the future development of the AFSJ has also taken us back to the description of a tendency towards the deployment of a 'pro-activity / profiling / prevention' framework,[206] reaffirming the need to further reflect on the consequences of the move towards increased 'monitoring of the future'.[207] Many of the described practices are indeed inscribed in logics of prevention in the widest of senses, and they (generally implicitly) assume that it is not only possible, but also suitable to interfere massively with the right to respect for private life of individuals in the name of the prevention of crimes, or even of administrative faults, yet to be committed. This approach is not only arguable in terms of its effectiveness, but has two important ethical consequences: first, the fact that all individuals are potentially placed under suspicion, and,

[204] The EC also appointed the French judge Jean-Louis Bruguière to examine compliance by US authority with the agreed use of the data, limited to the fight against terrorism. A first report by the judge was presented to the European Parliament on 17 February 2009. On US access to SWIFT data, see: González Fuster, Gloria, Paul De Hert and Serge Gutwirth (2008b), "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law, Computers & Technology*, 22(1-2), pp. 191-202; and Poullet, Yves and Elise Degrave (2007), ""L'Affaire Swift"", *Revue du droit des technologies et de l'information*, 27, pp. 3-9.
[205] EDPS (2009b), op. cit., p. 10.
[206] Bigo, Bonditti, Jeandesboz and Ragazzi (2008), op. cit., p. 25.
[207] Amicelle, Bigo, Jeandesboz and Ragazzi (2009), op. cit., p. 50.

second, the fact that some categories of individuals are placed under special suspicion. Both issues are ethically problematic, and emphasising one of them should not lead us to forget the other. Regarding the first one, it can be noted that measures such as, for instance, adopting techniques allowing for the systematic monitoring of the content of all communications, or the granting of access to general databases to law enforcement and intelligence agencies, tend to blur the boundary between permissible targeted surveillance and more problematic mass surveillance, which potentially amounts to arbitrary or unlawful interference with the right to respect for private life.[208] The second issue is tied to the foundational principle according to which fundamental rights are to be granted to all individuals, and not only to those who are entirely perceived as being absolutely 'innocent' or presumably 'bona fide'. On the contrary, the idea that fundamental rights are to be ensured for everybody includes in this notion those whose conducts might have been automatically flagged by a determined data mining system as 'suspicious', those whose constructed profile matches a 'risky' pattern and those signalled as a possible manifestation of a potential 'threat'; it is precisely for them, actually, that the respect for fundamental rights becomes outstandingly important. In this sense, it should be deplored that the EC Communication on the future programme for the AFSJ fails to consider the protection of the whole spectrum of rights that are directly affected by supported data processing practices.

55. Regarding privacy and data protection, many particular aspects have been identified as requiring further attention: for instance, the effective insurance of the data protection rights of individuals confronted with digital borders, or the preservation of data protection rights of individuals in the context of financial monitoring. The particular dynamics of EU policing certainly favour the relegation of the concrete modalities of the insurance of data protection to the national legal frameworks, but, in front of persistent problems, more ambitious approaches and more detailed consideration of the repercussions of different measures envisaged might be needed. As far as the right to data protection is concerned, it can be said that in the long run its inconsistent support throughout the EU legal framework ultimately allows for questioning the very development of data protection as a EU fundamental right. In this light, it is also crucial to recall that current restrictions imposed on data transfers to third countries not ensuring an adequate level of protection are to be considered necessary for the respect of the right of data protection not only in such third countries, but also in the very EU territory, and thus should not modified lightly.

56. More generally, the value debate connected to the discussed issues has two main faces: on the one hand, the question of determining whether the action proposed is, by itself, legitimate and ethical, and on the other hand, the question of whether what has been considered ethical and legitimate is to be deployed in practice with sufficient guarantees to ensure that there is no undesired impact on the fundamental rights of individuals. Regarding the first question, the key issue might be described as whether should be regarded as necessary the move towards an increased 'monitoring of the future' based on the processing of information of both innocents and of categories of persons artificially constructed as 'potentially more probably suspect than other', as well as on the assumption that information technology is the most appropriate tool to be relied on for further action in the AFSJ. Only if particular steps in this direction are considered suitable, becomes then relevant the question of whether these moves take place accompanied by the appropriate safeguards. The discussion of such safeguards should not, however, detract the required attention from the prior value discussion.

[208] Scheinin, Martin (2009), *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, February, United Nations, Human Rights Council.

Bibliography

Adam, Alexandre (2006), "L'échange de données à caractère personnel entre l'Union européenne et les Etats-Unis: Entre soucis de protection et volonté de coopération", *Revue trimestrielle de droit européen*, 42(3), pp. 411-437.

Agencia Española de Protección de Datos (AEPD) (2009), *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data*, Version 3.

Amicelle, Anthony, Didier Bigo, Julien Jeandesboz and Francesco Ragazzi (2009), *Catalogue of Security and Border Technologies at Use in Europe Today*, INEX D.1.2., Paris.

Anderson, Ross, Ian Brown, Terri Dowty, Philip Inglesant, William Heath and Angela Sasse (2009), *Database State*, The Joseph Rowntree Reform Trust Ltd., York.

Arenas Ramiro, Mónica (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant Lo Blanch.

Article 29 Data Protection Working Party (2007), *Opinion 5/2007 on the follow-up 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 concluded in July 2007*, Adopted on 17 August 2007, Brussels.

--- (2008a), *Eleventh Annual Report of the Article 29 Working Party on Data Protection, European Commission*, Brussels.

--- (2008b), *Preliminary analysis of the US ESTA by the Art. 29 WP's PNR subgroup at the request of the EU Commission of 10 July 2008*, 24 July, Brussels.

--- (2008c), *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, WP 155 rev.01, 1 October, Brussels.

--- (2009), *Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor*), WP 161, 5 March, Brussels.

Article 29 Data Protection Working Party and Working Party on Police and Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, WP 145, WPPJ 01:07, December.

Batho, Delphine and Jacques Alain Bénisti (2009), *Rapport d'information sur les fichiers de police*, Assemblée nationale, N° 1548, 24 mars, Paris.

Bayo Delgado, Joaquín (2008), "La cooperación internacional policial a la luz de la Propuesta revisada de Decisión Marco relativa a la protección de datos" in A. Emaldi Cirión, E. Domínguez Peco, F. Aranda Guerrero, J. López Barja de Quiroga, J. Bayo Delgado, J. A. Martín Pallín, V. Moreno Catena, J. Salom Clotet, M. Pérez Sánchez, M. García-Herraiz Rooabert, R. Martínez Martínez and R. De Cospedal García (eds.), *La protección de datos en la cooperación policial y judicial*, Thomson Aranzadi, Cizur Menor, pp. 21-36.

--- (2008b), "La protección de datos en la investigación policial y en el proceso penal", Jueces para la Democracia, Información y Debate, 63, pp. 11-24.

Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve, INEX D.1.1, Paris.

Bignami, Francesca (2007), "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law*, 8, pp. 233-254.

Broeders, Dennis (2009), *Breaking down anonymity: Digital surveillance on irregular migrants in Germany and the Netherlands*, PhD Thesis, Erasmus University Rotterdam, Rotterdam.

Brouwer, Evelien (2008), *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*, Leiden, Martinus Nijhoff Publishers.

--- (2009), *Towards a European PNR system? Questions on the added value and the protection of fundamental rights*, Committee on Civil Liberties, Justice and Home Affairs (LIBE), PE 410.649, European Parliament.

Bunyan, Tony (2006), *The "principle of availability"*, Statewatch Analysis, Statewatch, December.

Bygrave, Lee A. (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague, London, New York, Kluwer Law International.

Cavoukian, Ann (2006), *Creation of a Global Privacy Standard*, Information and Privacy Commissioner of Ontario.

Ceriani, Pablo, Cristina Fernández, Alejandra Manavella, Luis Rodeiro and Valeria Picco (2009), *Report on the situation of the Euro-Mediterranean borders (from the point of view of the respect of Human Rights)*, Observatori del Sistema Penal i els Drets Humans (OSPDH), Barcelona.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, European Treaty Series No. 108 ('Convention No. 108') and Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, Strasbourg, 8.XI. 2001.

Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union, 2005/C 198/01, OJ C198, 12.8.2005, pp. 1-22.

Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, Official Journal of the European Union L13, 20.1.2004, pp. 44–48.

Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal of the European Union L210, 6.8.2008, pp. 1-11.

Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal of the European Union L210, 6.8.2008, pp. 12-72.

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, Official Journal of the European Union, L 386, 29.12.2006, pp. 89-100.

Council of Europe (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11*, Rome, 4 November.

Council of the European Union (2008), *Note from the Presidency to COREPER on the EU-US Summit, 12 June 2008: Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 9831/08, 28 May, Brussels.

--- (2009a), *Note from Presidency to Delegations on the Swedish Presidency: provisional agendas for Council meetings prepared by Coreper (Part 2)*, 30 June, Brussels.

--- (2009b), *Note from the Swedish Delegation to Delegations on: Preparing the Stockholm Programme: Conference in Bruges 4-5 March 2009*, 10576/09, 2 June, Brussels.

COWI (2009), *External evaluation of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union: Final Report*, Kongens Lyngby.

De Hert, Paul (2003), "The case of anonymity in Western political philosophy: Benjamin Constant's refutation of republican and utilitarian arguments against anonymity" in Nicoll, Chris, Miriam Van Dellen & Corien Prins (eds.), *Digital Anonymity and the Law: Tensions and Dimensions*, Asser, The Hague, pp. 47-97.

De Hert, Paul and Rocco Bellanova (2008), *Data Protection from a Transatlantic Perspective: the EU and US Move Towards an International Data Protection Agreement?* , Study, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, PE 408.320, October.

De Hert, Paul and Serge Gutwirth (2006a), "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power", in E. Claes, A. Duff & S. Gutwirth (Eds.), *Privacy and the Criminal Law*, Antwerp-Oxford, Intersentia, pp. 61-104.

--- (2006b), "Interoperability of Police Databases within the EU: An Accountable Political Choice?", *International Review of Law, Computers & Technology*, 20(1&2), pp. 21-35.

Derrida, Jacques (1994), *Politiques de l'amitié*, Paris, Galilée.

Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, 23.11.1995, pp. 31-50.

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), Official Journal, L 108, 24.4.2002, pp. 51–77.

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), Official Journal of the European Communities, L 201, 31.7.2002, pp. 37-47.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, Official Journal of the European Union L 309, 25.11.2005, pp. 15–36.

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, OJ L 105, 13.04.2006, pp. 54-63.

Eurodac Supervision Coordination Group (2009), *Second Inspection Report*, 24 June, Brussels.

European Commission (2003), *First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, 15.5.2003, Brussels.

--- (2005a), *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*, COM(2005) 597 final, 24.11.2005, Brussels.

--- (2005b), *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, COM(2005) 475 final, 04.10.2005, Brussels.

--- (2005c), *Proposal for a Council Framework Decision on the exchange of information under the principle of availability*, COM(2005) 490 final, 12.10.2005, Brussels.

--- (2006), *Communication from the Commission to the Council and the European Parliament: Implementing the Hague Programme: the way forward*, COM(2006) 331 final, 28.6.2006, Brussels.

--- (2007a), *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 final, 2.5.2007, Brussels.

--- (2007b), *Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, COM(2007) 87 final, 7.3.2007, Brussels.

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

--- (2007d), *Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation*, COM(2007) 698 final, 13.11.2007, Brussels.

---(2007e), *Report from the Commission based on Article 12 of the Council Framework Decision of 22 December 2003 on combating the sexual exploitation of children and child pornography*, COM(2007) 716 final, Brussels.

--- (2007f), *Study on the international law instruments in relation to illegal immigration by sea, Commission Staff Working Document*, SEC(2007) 691, 15.5.2007, Brussels.

--- (2008a), *Commission Staff Working Document: The U.S. Electronic System for Travel Authorization (ESTA)*, SEC(2008) 2991 final, 2.12.2008, Brussels.

--- (2008b), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European border surveillance system (EUROSUR)*, COM(2008) 68 final, Brussels.

--- (2008c), *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*, European Commission, COM(2008) 69 final, 13.2.2008, Brussels.

--- (2008d), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the evaluation and future development of the FRONTEX Agency*, COM(2008) 67 final, Brussels.

--- (2008e), *Questionnaire for the consultation on the impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection*, Brussels.

--- (2009a), *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Justice, Freedom and Security in Europe since 2005: An evaluation of the Hague Programme and Action Plan: An extended report on the evaluation of the Hague Programme*, SEC(2009) 766 final, 10.6.2009, Brussels.

--- (2009b), *Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen*, COM(2009) 262/4, 10/06/2009, Brussels.

--- (2009c), *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, COM(2009) 293 final, 24.6.2009, Brussels.

--- (2009d), *Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty*, COM(2009) 294 final, 24.6.2009, Brussels.

--- (2009e), *Report on the practical operation of the methodology for a systematic and rigorous monitoring of compliance with the Charter of Fundamental Rights*, COM(2009) 205 final, 29.4.2009, Brussels.

European Court of Human Rights, *Case of Liberty and Others v. the United Kingdom*, Application no. 58243/00, Judgement of 1 July 2008.

S. and Marper v. The United Kingdom, Applications nos. 30562/04 and 30566/04, Judgement of 4 December 2008.

European Court of Justice, *Heinz Huber v. Germany*, , Case C-524/06, Judgement of 16 December 2008.

European Data Protection Supervisor (EDPS) (2006a), *Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final)*, 28 February, Brussels.

(2006b), *Comments on the Communication of the Commission on interoperability of European databases*, 10 March, Brussels.

(2007), *Opinion on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, 25 July, Brussels.

--- (2008), *Preliminary Comments on 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" COM(2008) 69 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final*, 3 March, Brussels.

--- (2009), *EDPS comments on some issues in the review of Directive 2002/22/EC (Universal Service)*, 16 February, Brussels.

--- (2009b), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen*, 10 July, Brussels.

--- (2009c), *Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...][establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (COM(2008)825)*, 18 February, Brussels.

European Parliament (2008), *Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection*, B6_TA(2008)0521, Strasbourg.

--- (2008b), *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, P6_TA(2008)0561, Strasbourg.

European Union Agency for Fundamental Rights (FRA) (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 28 October.

--- (2009), *The Stockholm Programme: A chance to put fundamental rights protection in the centre of the European Agenda*, 14 July, Vienna.

European Union Committee of the House of Lords (2009), *Money laundering and the financing of terrorism*, House of Lords, HL Paper 132, 22 July, London.

Fischer-Lescano, Andreas and Tillmann Löhr (2007), *Border Controls at Sea: Requirements under International Human Rights and Refugee Law*, European Center for Constitutional and Human Rights, September, Berlin.

González Fuster, Gloria (2009), "Law, justice and ethics for preemptive security practices" in Čas, Johann (ed.), *D 7.3 PRISE Conference Proceedings: "Towards privacy enhancing security technologies – the next steps" Vienna, April 28th and 29th 2008*, pp. 79 – 89.

González Fuster, Gloria, Paul De Hert and Serge Gutwirth (2008a), *State-of-the-art of the Law-Security Nexus in Europe*, INEX Deliverable D.2.1, Brussels.

--- (2008b), "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law, Computers & Technology*, 22(1-2), pp. 191-202.

González Fuster, Gloria and Serge Gutwirth (2008), *Data protection in the EU: Towards 'Reflexive Governance'?* , REFGOV Working Paper Series, FR-19, Brussels.

Gutwirth, Serge (2002), *Privacy and the information age*, Lanham, Rowman & Littlefield Publishers.

Hildebrandt, Mireille and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, 2008.

Hobbing, Peter and Rey Koslowski (2009), *The tools called to support the 'delivery' of Freedom, Security and Justice: A comparison of border security systems in the EU and in the US*, Briefing Paper, PE 410.681, European Parliament.

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

Jeandesboz, Julien (2008), Reinforcing the Surveillance of EU Borders: The Future Development of FRONTEX and EUROSUR, Research Paper No. 11, CHALLENGE Project.

Llaneza, Paloma (2007), "El derecho de acceso a los datos de carácter personal contenidos en los ficheros relativos a la prevención del blanqueo de capitales", *Revista Española de Protección de Datos*, 3, pp. 263-279.

López Barja de Quiroga, Jacobo (2008), "El registro único de las huellas de ADN, la protección de datos y la investigación criminal" in A. Emaldi Cirión, E. Domínguez Peco, F. Aranda Guerrero, J. López Barja de Quiroga, J. Bayo Delgado, J. A. Martín Pallín, V. Moreno Catena, J. Salom Clotet, M. Pérez Sánchez, M. García-Herraiz Rooabert, R. Martínez Martínez and R. De Cospedal García (eds.), *La protección de datos en la cooperación policial y judicial*, Thomson Aranzadi, Cizur Menor, pp. 285-331.

Lucioni, Carlo (2009), "Tutela dei dati personali del cittadino dell'Unione e giudizio di non discriminazione in base alla nazionalità", *Diritto pubblico comparato ed europeo*, 2, pp. 575-582.

Martínez Martínez, Ricard (2005), "En torno a la consideración jurídica del número IP", *Nuevas Politicas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, 1, pp. 283-304.

National Research Council of the National Academies (2008), *Protecting Individual Privacy in the Struggle Against Terrorist: A Framework for Program Assessment*, National Academy of Sciences, Washington, D.C.

Pickering, Sharon and Leanne Weber (2006), "Borders, Mobility and Technologies and Control", in Sharon Pickering and Leanne Weber (Eds.), *Borders, Mobility and Technologies and Control*, Springer, Dordrecht, pp. 1-19.

Policy Engagement Network, Information Systems and Innovation Group (2009), *Briefing on the Interception Modernisation Programme*, The London School of Economics and Political Science, London.

Portuguese Presidency (2007), *Public security, privacy and technology in Europe: Moving forward: Concept paper on the European strategy to transform Public security organizations in a Connected World*, October.

Poullet, Yves (2004), "The Fight against Crime and/or the Protection of Privacy: A Thorny Debate!", *International Review of Law, Computers & Technology*, 18(2), pp. 251-273.

--- (2006), "The Directive 95/46/EC: Ten years after", *Computer Law & Security Report*, 22, pp. 206-217.

Poullet, Yves and Elise Degrave (2007), ""L'Affaire Swift"", *Revue du droit des technologies et de l'information*, 27, pp. 3-9.

Rigaux, François (1990), *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant.

Rodríguez Lainz, José Luis (2009), "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas", *Diario La Ley*, N° 7086, Sección Doctrina, 2 Enero 2009, Año XXIX, Ref. D-382.

Ruiz-Jarabo Colomer (2008), *Conclusiones del Abogado General Sr. Dámaso Ruiz-Jarabo Colomer, presentadas el 22 de diciembre de 2008 (Asunto C-553/07, College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*).

Scheinin, Martin (2009), *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, February, United Nations, Human Rights Council.

Siemen, Birte (2006), *Datenschutz als europäisches Grundrecht*, Berlin, Duncker & Humblot.

Solanes Corella, Ángeles and María Belén Cardona Rubert (2005), *Protección de datos personales y derechos de los extranjeros inmigrantes*, Valencia, Tirant Lo Blanch.

United Nations Counter-Terrorism Implementation Task Force (CTITF) (2009), *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*, February.

Wagner, Ben (2009), *Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'*, Global Voices Advocacy,

Weinzierl, Ruth (2007), *The Demands of Human and EU Fundamental Rights for the Protection of the European Union's External Borders*, German Institute for Human Rights, July, Berlin.

List of Acronyms

AFSJ	Area of Freedom, Security and Justice
AEPD	Agencia Española de Protección de Datos
APEC	Asia-Pacific Economic Cooperation
API	Advanced Passenger Information
BMS	Biometric Matching System
CAFIS	Criminal Automated Fingerprint Identification System
CBPR	Cross Border Privacy Rules
CIS	Customs Information System
CTITF	Counter-Terrorism Implementation Task Force
DNA	Deoxyribonucleic acid
EC	European Commission
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
ESRIF	European Security Research and Innovation Forum
EU	European Union
FRA	Fundamental Rights Agency
IMS	Information Management Strategu
IP	Internet Protocol
IT	Information Technology
JLS	Justice, Freedom and Security
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs
PETs	Privacy Enhancing Technologies
PNR	Passenger Name Records
SIS	Schengen Information System
SOCA	Serious Organised Crime Agency
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
US	United States
VIS	Visa Information System