in:ex

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

European Commission, 7th Framework Programme

D.2.1. State-of-Art Report on the Current Scholarship on the Law-Security Nexus in Europe

Deliverable submitted November 2008 (M8) in fulfillment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the International 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 D2.1

The Law-Security Nexus in Europe:

State-of the-art report

Gloria González Fuster, Paul de Hert and Serge Gutwirth

TABLE OF CONTENTS

I. Introduction

1. This report reviews the current state of knowledge on the relationship between security and law in Europe. It is the first deliverable of WP2 of the INEX project, whose general objective is to contribute to existing understandings of European security through an analysis of the value-based premises and ethical consequences of the 'internal/external security continuum'. WP2, concerned with the 'Cross-border Legal Dilemmas of the Internal/External Security Continuum', aims at analysing the ethical value assumptions implicit in transnational legal dilemmas of European security practice.[1] Two basic perspectives on legal norms coexist in security-related research: one, essentially descriptive, deals with the ways in which norms are produced and sustained; the other, predominately normative, subjects norms to critical analysis.[2] This paper aims to bring together both, in the belief that a crucial step in considering legal change is to grasp analytically the conditions giving rise to it.[3]

2. The assessment of the current state of knowledge is grounded on extensive literature review, complemented with the screening of primary sources such as policy and legislative documents, as well as relevant recent case law potentially opening new paths for discussion. A series of projects funded by the European Commission (EC) under the 6th Framework Programme for Research and Technological Development, as well as through other funds, have provided pertinent background documentation: notably, the Changing Landscape of European Liberty and Security (CHALLENGE) project;[4] the Reflexive Governance in the Public Interest (REFGOV) project;[5] the Future of Identity in the Information Society (FIDIS) Network of Excellence;[6] the Transnational Terrorism, Security & the Rule of Law (TTSRL) project;[7] HUMSEC;[8] the Privacy Enhancing Shaping of Security Research and Technology (PRISE) project,[9] and the Changing Landscape of Justice and Home Affairs Cooperation in the European Union (EU) and EU-Canada Relations project.[10]

3. The report is split into four main different sections. First, it introduces the general terms of the recent discussions on the law-security nexus in Europe (Section II). Second, it explores the principal different meanings of 'security' in European law, with special focus on the relation between security and the right to privacy, on the one hand, and the right to the protection of personal data, on the other (Section III). Third, a series of key aspects of the relation between EU security policies and the EU legal framework are discussed (Secion IV). Finally, paths for future research are identified and presented (Section V).

---

[1] The research has been circumscribed by parallel work undertaken in the context of INEX. In particular, we have refrained to address in detail issues related to the Common Foreign and Security Policy (CFSP), established as one of the Three Pillars of the EU by the Treaty of Maastricht Treaty in 1992, and the European Security and Defence Policy (ESDP) (part of the CFSP since the 1999 Cologne European Council).

[2] Burgess, J. Peter and David Rodin (2008), *The Role of Law, Ethics and Justice in Security Practices*, Security: Advancing a Framework for Enquiry (SAFE) Conference report, International Peace Research Institute, Oslo (PRIO) Papers, Oslo, p. 5.

[3] Lyon, David (2004), "Globalizing Surveillance: Comparative and Sociological Perspectives", *International Sociology,* 19(2), p. 146.

[4] The project has explored themes such as the development of security through surveillance and control, the changing forms of the 'logics of suspicion' and practices of exception and derogation, especially in relation to established understandings of the rule of law, or the impact of security policies on the rights and freedoms of EU citizens and foreigners (Bigo, Didier, Sergio Carrera, Elspeth Guild and R.B.J. Walker (2007), *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project*, Research Paper No. 4, CEPS, Brussels, February, p. 2). More information: http://www.libertysecurity.org/.

[5] REFGOV is concerned with new forms of governance in the public interest, and gives particular attention to fundamental rights policies in the EU. More information: http://refgov.cpdr.ucl.ac.be.

[6] More information: http://www.fidis.net/.

[7] Dealing with transnational terrorism as one of the most substantial threats to security and the rule of law within the EU. More information: http://www.transnationalterrorism.eu.

[8] On the link between transnational terrorist groups and criminal organisations in the Western Balkans and their role in the peace-building process in the region. More information: http://www.humsec.eu.

[9] The PRISE Supporting Activity, launched in February 2006 with a 28 months duration, defined itself as a participatory approach to develop acceptable and accepted principles for European Security Industries and Policies. It was supported by the Preparatory Action on the enhancement of the European industrial potential in the field of Security Research. More information: http://www.prise.oeaw.ac.at.

[10] Project funded by the Directorate-General for External Relations of the EC, developed from January to December 2008.

II. Main Perspectives On The Law-Security Nexus

4. Recent discussions on the nature of the law-security nexus in Europe have been very wide and have risen in the context of many different debates. The debates have sometimes concerned the law-security nexus in a strict sense, but, possibly more often, the relation between security and human rights. The particular debate on the security-human rights nexus has also many facets, ranging from exploring what is meant by 'security' in this particular relation, and determining the very nature of the relation, to exploring how do governments perceive their right to reformulate existing rules on it.[11]

5. One of the most discussed issues regarding the security-human rights nexus is the so-called 'balance paradigm' or 'balancing approach'.[12] The 'balancing approach' is believed to have been very influential in the recent years,[13] especially as after 11 September 2001[14] different decision-makers have framed much of the debate about security in terms of the supposed need to 'strike a balance' between security and human rights, between security and liberty, or even between security and specific rights, such as the right to privacy.[15] This has been the case e.g. in the particular context of European Union (EU) Justice and Home Affairs (JHA) law, where there has been much discussion on the need to 'balance' human rights and civil liberties, on the one hand, and the Member States' interests in public order and security.[16]

6. The 'balancing approach' has been subject to significant academic criticism. Mistrust on the usefulness of the image coexists with many specific objections to its validity. The image has been considereed not only unhelpful[17] and misleading, but also structurally wrong.[18] Inappropriate assumptions underlying it have been highlighted, such as the existence of a conflict between human rights and the demands of security and public safety,[19] or the notion that the most appropriate way of dealing with such an alleged conflict is to seek a balance between the two sets of interests.[20] A specific objection to the 'balancing paradigm' relates to the supposed inverse relationship between liberty and security, namely that more of one thing means less of another, and vice versa.[21] Many have also insisted on the idea that security and privacy, in particular, are not related in a zero-sum trade-off. On the contrary, they might each be a requirement for the existence of the other.[22] Another counterargument to the 'balancing paradigm' has focused on discussing the assumption that individuals rights can or should be balanced against the interests of the greater community.[23] Some have underlined that the very notion of security being 'balanced' through the 'balancing paradigm' shall be subject to special attention, as it does not refer to traditional conceptions of 'security' but to the

---

[11] Bigo, Didier and Elspeth Guild (2007), "The Worst-case Scenario and the Man on the Clapham Omnibus" in Goold, Benjamin J., and Lazarus, Liora (eds.) (2007), *Security and human rights*, Hart, Oxford, Portland, p. 102.
[12] See, notably: Waldron, Jeremy (2003), "Security and Liberty: The Image of Balance", *The Journal of Political Philosophy*, 11(2), pp. 191-210.
[13] Bronitt, Simon (2008), "Balancing Security and Liberty: Critical Perspectives on Terrorism Law Reform" in Miriam Gani and Penelope Mathex (ed.), *Fresh Perspectives on the 'War on Terror'*, p. 65.
[14] Hereafter, '9/11'.
[15] Cavoukian, Ann (2003), *National Security in a Post-9/11 World: The Rise of Surveillance... the Demise of Privacy?*, Information and Privacy Commissioner of Ontario, p. 45. Arguing in favour of such an approach, see: Golder, Ben and George Williams (2006), "Balancing National Security and Human Rights: Assessing the Legal Response of Common Law Nations to the Threat of Terrorism", *Journal of Comparative Policy Analysis,* 8(1), pp. 43-62.
[16] Peers, Steve (2006), *EU Justice and Home Affairs Law*, Second Edition, Oxford EC Law Library, Oxford University Press, Oxford, p. 1.
[17] Moeckli, Daniel (2008), *Human rights and non-discrimination in the 'War on terror'*, Oxford University Press, Oxford, p. 2.
[18] Michaelsen, Christopher (2006), "Balancing Civil Liberties Against National Security? A Critique of Counterterrorism Rhetoric", *University of NSW Law Journal*, 29(1), p. 3.
[19] Emphasising that a dichotomy between security and human rights and civil liberties is false, see for instance: Muntarbhorn, Vitit, Iris Almeida and Lloyd Lipsett (2002), *Report of the Think Tank on Promoting Human Rights and Democracy in the Context of Terrorism*, International Centre for Human Rights and Democratic Development, Ottawa, May, p. 7. Criticising the opposition between security and freedom, see for instance: Guild, Elspeth and Florian Geyer (2006), Justice and Home Affairs Issues at European Union Level, Written evidence submitted by the Centre for European Policy Studies (CEPS) to the Select Committee on Home Affairs (House of Commons), CEPS, Brussels, November, p. 2.
[20] Ashworth, Andrew (2007), "Security, Terrorism and the Value of Human Rights" in Goold, Benjamin J., and Lazarus, Liora (eds.) (2007), *Security and human rights*, Hart, Oxford, Portland, p. 203.
[21] Bronitt, *op. cit.*, p. 69.
[22] Burgess, Peter J. (2008), *Security After Privacy: The Transformation of Personal Data in the Age of Terror*, Policy Brief, PRIO, 5/2008, p. 1.
[23] Michaelsen, *op. cit.*, pp. 8-9.

potential protection from prospective, unquantifiable risk.[24] The success of the balancing image, it has been argued, has benefited from a weakening of human rights discourse experienced in recent years,[25] and might have been helped by an artificial downgrading of the value of freedom.[26]

7. Coexisting with these debates on the relation between human rights and security, there has also been discussion on the nature of the law-security nexus. This relation had already been much debated before 9/11,[27] but exchanges of views received then a new impetus, especially as in certain circles the idea that security might allow for a redefinition of the nexus and a 'suspension of law' was advanced.[28] If claims relating to a so-called 'age of exception'[29] have found limited support in Europe,[30] they are nevertheless believed to have delineated the background of many considerations in the field.[31] There has been indeed discussion of a so-called climate of 'exceptionalism',[32] as well as different accounts of a 'quasi-permanent state of exception' being deployed in the EU,[33] especially in reference to recurrent Member States decisions to reinstate internal border checks as to maintain public order or national security, or, more generally, to measures taken after 9/11 not only to address a perceived terrorist threat, but also crime in general.[34]

8. It is globally undisputed that normative and institutional instruments developed in the name of security can have implications for human rights and civil liberties. The concerns about how anti-terrorism measures adversely impact civil liberties and human rights are many, and can refer to specific rights and freedoms, such as the right to privacy, or freedom of expression,[35] but can also be more general and far-reaching. Some have claimed that after 9/11 the United States (US) deliberately opted to change the generally applicable rules, displaying a will to reshape international law[36] and, in general, the very boundaries of law.[37] In Europe, some have seen in the modifications imposed on different legal frameworks in the name of counterterrorism changes of a great magnitude, not limited to a suspension or limitation of certain mechanisms of protection, but affecting the entirety of the

[24] Moeckli, Daniel (2008), *Human rights and non-discrimination in the 'War on terror'*, Oxford University Press, Oxford, p. 9.
[25] In particular, in the context of some discussion on the foundation of human rights claims and controversy regarding their judicial and constitutional protection (Lazarus, Liora and Benjamin B. Goold (2007), "Security and Human Rights: The Search for a Language of Reconciliation" in Goold, Benjamin J., and Lazarus, Liora (eds.) (2007), *Security and human rights*, Oxford, Portland, Hart, p. 6).
[26] Tsoukala, Anastassia (2008), *Security, Risk and Human Rights*: *A Vanishing Relationship?*, CEPS Special Report, CEPS, Brussels, September, p. 2.
[27] Current discussions can be placed in the perspective of the traditional debates opposing a 'realist' perspective, according to which human rights norms are only binding on states when they do not collide with other interests such as national security, an a 'pluralist' or 'legalist' approach, maintaining that security should be provided by international rules and norms (Dunne, Tim and Nicholas J. Wheeler (2004), "'We the Peoples': Contending Discourses of Security in Human Rights Theory and Practice", *International Relations*, 18(1), pp. 12 and 13).
[28] Bigo, Didier and Elspeth Guild (2007), "The Worst-case Scenario and the Man on the Clapham Omnibus" in Goold, Benjamin J., and Lazarus, Liora (eds.) (2007), *Security and human rights*, Hart, Oxford, Portland, p. 106. For a discussion on perspectives on the 'state of exception', see: Van Klink, Bart Van and Oliver Lembcke (2007), "Can Terrorism Be Fought within the Boundaries of the Rule of Law? - A Review of Recent Literature in Political Philosophy", *Rechtsfilosofie & Rechtstheorie,* 36(2), pp. 9-26.
[29] See, notably: Agamben, Giorgio (1998), *Homo sacer: sovereign power and bare life*, Stanford University Press, Stanford, and Neal, Andrew (2005), *Review of the literature on the 'state of exception' and the application of this concept to contemporary politics*, CHALLENGE Working Paper.
[30] The EU never declared itself in any 'state of emergency' in response to 9/11 (Douglas-Scott, Sionaidh (2008), "Fundamental rights in EU justice and home affairs", in M. Martin (Ed.), *Crime, rights and the EU: The future of police and judicial cooperation*, JUSTICE, London, p. 15).
[31] Lazarus and Goold, *op. cit.,* pp. 2-4.
[32] As well as of a normalisation of emergency as a technique of government (Bigo, Didier (2006), "Security, exception, ban and surveillance", in Lyon, David (ed.), *Theorizing Surveillance: The panopticon and beyond*, Willian Publishing, Portland, p 63).
[33] Tsoukala, *op. cit.*, p. 1. See also: Lodge, Juliet (2004), "EU homeland security: citizens or suspects?", *Journal of European Integration,* 26(3), pp. 253-279.
[34] Douglas-Scott, Sionaidh (2008), "Fundamental rights in EU justice and home affairs", in M. Martin (Ed.), *Crime, rights and the EU: The future of police and judicial cooperation*, JUSTICE, London, p. 16.
[35] Protected by Art. 10 European Convention on Human Rights (ECHR). See, on this issue: Banisar, David (2008), *Speaking of terror: A survey of the effects of counter-terrorism legislation on freedom of the media in Europe*, Council of Europe, November, p. 3.
[36] Byers, Michael (2008), "Preemptive Self-defense: Hegemony, Equality and Strategies of Legal Change", The Journal of Political Philosophy, 11(2), p. 172.
[37] Leading notably to discussions on the interplay between human rights law and international humanitarian law, especially in situations of non-international armed conflict (Byrnes, *op. cit.*, p. 142).

population and, as a matter of fact, the very relation between the individual and the State.[38] A series of scholars have underscored that recent security have specific implications for the integrity of criminal law and for the extent to which adherence to established criminal law principles and procedures should restrain responses to terrorism and other serious threats,[39] while others have nuanced the direct impact on law on counter-terrorist strategies.[40]

9. Law is one of the privileged instruments of security policies. Especially since 9/11, law making at international and national level in the name of security has been extensive.[41] For some, such measures have tended to demonstrate the actual limitations of law, and, more particularly, of the rule of law as such as a tool to combat injustice or constrain power. Others have insisted on the fact that, despite their limitations, law and, more concretely, the rule of law do provide the means to restrain at least the worst excesses of security decision-making.[42] Discussions on counterterrorism and the rule of law, as well as on the impact of recent security measures on human rights, echo discussions previously developed in the context of criminal law. For criminal justice scholars, recent debates on the 'balancing approach' opposing security vs. human rights resonate with critiques of balancing models applied to guide criminal justice reform, framed as 'striking a balance' between crime control and due process.[43]

III. Security in European Law

10. The scholarship on the law-security nexus illustrates the existence of many different understandings of the notion of 'security'. Today's more widely used conceptions might be those inherited from the field of international relations,[44] in which conventional definitions have been especially challenged, notably through the notion of 'securitisation'.[45] But how does European law envisage 'security', and the relation between security and law?

Security as in the EU Area of Freedom, Security and Justice

11. An especially important notion of security for our concerns is to be found in Article 2 of the Treaty on the European Union (TEU). According to Article 2 TEU, and since the Treaty of Amsterdam, "*the Union shall set itself the following objectives*: (…) *to maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime*".[46] The aim of the provision is not to create a European

[38] Paye, Jean-Claude (2004), *La fin de l'état de droit: La lutte antiterroriste de l'état d'exception à la dictature*, La Dispute, Paris, p. 15 and p. 201.
[39] Lazarus and Goold, *op. cit.,* p. 18.
[40] For instance: Hufnagel, Saskia (2008), *German perspectives on the right to life and human dignity in the 'war on terror'*, Social Science Research Network, Legal Scholarship Network, ANU College of Law Research Paper No. 08-18, The Australian National University College of Law.
[41] Byrnes, Andrew (2008), "More Law or Less Law? The Resilience of Human Rights Law and Institutions " in Miriam Gani and Penelope Mathew (ed.), *Fresh Perspectives on the 'War on Terror'*, p. 127.
[42] Balkin, Jack M. (2008), "Critical Legal Theory Today", available at SSRN: http://ssrn.com/abstract=1083846. Echoing this divergent interpretations, two schools of thought have been identified: one insisting on the idea that human rights violations must be addressed through a reinforcement of the rule of law and turning to judicial mechanisms, and a second one calling instead for a so-called 'political response' (Moeckli, Daniel (2008), *Human Rights Strategies in an Age of Counter-Terrorism,* SSRN, retrieved from http://ssrn.com/abstract=1189722, p. 2).
[43] Bronitt, *op. cit.*, p. 66.
[44] Burgess, Peter J. (2008), *Security as Ethics*, Policy Brief, PRIO, 6/2008, p. 2. See also: c.a.s.e. Collective (2006), "Critical Approaches to Security in Europe: A Networked Manifesto", *Security Dialogue,* 37(4), pp. 443-487.
[45] According to the method of securitisation analysis, something is constituted as a 'security' issue ('securitised') when somebody argues that the issue poses an existential threat to something that has to survive, giving the issue special politic priority (Wæver, Ole (2005), "The Constellation of Securities in Europe", in Aydinli, Ersel and James N. Rosenau), *Globalization, Security, and the Nation State: Paradigms in transition*, State University of New York Press, Albany, p. 153. See also: COT Institute for Safety, Security and Crisis Management (ed.) (2007), *Notions of Security: Shifting Concepts and Perspectives*, Transnational Terrorism, Security and the Rule of Law (TTSRL), Deliverable 1, Work Package 2, February, pp. 20-21.
[46] Consolidated Version of the Treaty on European Union, *Official Journal* C 325, 24 December 2002. It shall be noted that the same Art. 2 includes a reference to 'security' as in the Common Foreign and Security Policy (CFSP) ("*to assert its identity on the international scene, in particular through the implementation of a common foreign and security policy*

security area in the sense of a common territory with uniform detection and investigation procedures applicable to all law enforcement agencies, and it should not affect the exercise of Member States' responsibilities to maintain law and order and safeguard internal security.[47] On the contrary, it "*rather provides an institutional framework to develop common action among the Member States*".[48] Article 29 TEU complements Article 2 by stipulating that the EU objective shall be "*to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia*", and that such an objective "*shall be achieved by preventing and combating crime, organised or otherwise, in particular terrorism* (…)". Counter-terrorism is therefore considered as a constitutive element of the EU area of Freedom, Security and Justice.[49] Article 11 TEU establishes the goals of EU's Common Foreign and Security Policy, which include *"to develop and consolidate democracy and the rule of law, and respect for human rights and fundamental freedoms"*. This Article is particularly significant for EU cooperation with third countries in Justice and Home Affairs matters, and recalls that the Treaty clearly foresees that security needs to be promoted while respecting human rights.

Security and the European Convention on Human Rights

12. The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[50] provides for strong protection of human rights while allowing states to protect national security.

Security as a Right

13. One of the ideas sometimes emerging, more or less implicitly, in the discussion of the law-security nexus (especially in the context of counterterrorism) is that there is a human right to security, which is an individual right, and, therefore, can be legitimately 'balanced' with any other individual right. This idea is somehow misleading. Even if major international legal instruments do protect the right to security of the person, they do so in conjunction with the right to liberty, as a 'right to liberty and security' confining the power of states to coerce individuals through arbitrary arrest and detention.[51] The right to security, therefore, does clearly not refer to the duty of the state to ensure personal protection from an attack by others.[52] The ECHR[53] is concerned with this right to security, in the sense of protection against arbitrary interference with the liberty of the person, in its Article 5 on the 'right to liberty and security'.[54] Trying to still find an individual 'right to security' to use for balancing purposes, some have tried to configure the duty that the state has to protect the citizenry as

---

including the progressive framing of a common defence policy, which might lead to a common defence, in accordance with the provisions of Article 17").

[47] Justice and Home Affairs Council (1999), *Action plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an Area of Freedom, Security and Justice,* adopted on 3 December 1998, OJ C 19, 23.1.1999, p. 3.

[48] Idem.

[49] Payé, Jean-Claude (2004), *La fin de l'état de droit: La lutte antiterroriste de l'état d'exception à la dictature*, La Dispute, Paris, p. 95.

[50] Art. 6(1) TEU states: *"The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States".* Article 6(2) TEU adds: "*The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950[50] and as they result from the constitutional traditions common to the Member States, as general principles of Community law*".

[51] Michaelsen, *op. cit.*, p. 11.

[52] Macovei, Monica (2005), *The right to liberty and security of the person: A guide to the implementation of Article 5 of the European Convention on Human Rights*, Human rights handbooks No. 5, Council of Europe, p. 6.

[53] European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 November) as amended by Protocol No. 11 and its Protocol of 1952.

[54] Art. 5(1) establishes that *"(e)veryone has the right to liberty and security of person*". Strasbourg case law on Art. 5 has been qualified as supporting the idea that the term 'security' has hardly any specific meaning in its context (Trechsel, Stefan (2001), "The Relevance of the ECHR and the Charter of Fundamental Rights of the EU for the Area of Freedom, Security and Justice", in Collegium (2001), Special Edition — *Proceedings of the Conference: 'Integrated Security in Europe, a Democratic Perspective'*, No. 22, XII.2001, Bruges, p. 90). Art. 6 of the European Charter of Fundamental Rights echoes Art. 5 ECHR, establishing that "[*e*]*veryone has the right to liberty and security of person*" (Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000).

creating a positive individual right to security,[55] while others have invoked the 'right to life' of victims of terrorism, relying on questionable argumentations.[56]

On The Right To Derogate

14. One of the reasons for the limited success of 'exceptionalism' in Europe is possibly that the ECHR is very clear about the strict conditions allowing for the suspension of (certain) rights, known as the possibility of the state 'to derogate'. Article 15 enables the suspension of all but the absolute rights of the ECHR in "*time of war or other public emergency threatening the life of the nation*", provided this is "*strictly required by the exigencies of the situation*". In this sense, the only 'exception' that a state can claim to its international legal responsibility in human rights law is that specified by human rights law itself.[57] If 'exceptional' times allow for the temporal sacrifice of certain individual rights in the name of collective security and freedoms,[58] they can never justify any redefinition of the boundaries of law,[59] or of the very relation between rights and security. Moreover, the legality of any derogation by a state to rights under the ECHR is not a purely internal decision, but is always subject to eventual supranational scrutiny by the European Court of Human Rights (ECtHR).[60]

Security as a Legitimate Aim of Interference

15. The interests of national security, public safety or the economic well being of the country, as well as the prevention of crime or disorder and the protection of the rights and freedoms of others, can be invoked by states in order to justify some, restricted interferences with a series of rights guaranteed by the ECHR. It is in this particular context that takes place an analysis considered by some to be similar to a kind of 'balancing'. However, such an examination is a multifaceted process[61] and cannot be accurately described through the notion of 'balancing', at least not in the sense of a simple weighing of the relative importance of security, on the one hand, and the right guaranteed, on the other hand. The examination of the invocation of one of the mentioned interests in order to justify an interference with a right needs imperatively to follow a series of well-established basic principles. Concretely, interferences with fundamental rights under the ECHR can only be justified if they are in accordance with the law, necessary in a democratic society for one of the objectives mentioned (the interests of national security, public safety or the economic well being of the country, the prevention of crime and disorder, or the protection of the right and freedom of others), proportionate, and non-discriminatory.[62] Where it is determined that a measure can limit the enjoyment of a right or freedom, and that the right in question is capable of limitation, it is still necessary to determine whether the measure is compatible with the procedural requirements of due process.[63]

16. Over the years, the Strasbourg organs have developed the so-called 'margin of appreciation' doctrine, which refers to the measure of discretion states are permitted in their observance of rights.[64] Based on the inherent political nature of the decisions to be taken,[65] the ECtHR recognises to states a substantial 'margin of appreciation', but nonetheless always claims the right to interpret the correct application of the ECHR. The width of margin which is generally conferred upon states in evaluating

---

[55] Michaelsen, *op. cit.,* p. 12.
[56] *Ibidem*, p. 14.
[57] Guild, Elspeth (2007), *Security and European Human Rights: protecting individual rights in times of exception and military action*, Wolf Legal Publishers, Nijmegen, p. 2.
[58] Bigo, Didier and Elspeth Guild (2007), "The Worst-case Scenario and the Man on the Clapham Omnibus" in Goold, Benjamin J., and Lazarus, Liora (eds.) (2007), *Security and human rights*, Hart, Oxford, Portland, p. 110.
[59] *Ibidem*, p. 111.
[60] Guild, Elspeth (2007), *Security and European Human Rights: protecting individual rights in times of exception and military action*, Wolf Legal Publishers, Nijmegen, p. 31.
p. 2 "I will seek to examine human rights and armed conflict from the perspective
[61] Moeckli, Daniel (2008), *Human rights and non-discrimination in the 'War on terror'*, Oxford University Press, Oxford, p. 10.
[62] Extensive case law of the ECtHR provides further details on what is to be understood by these different conditions.
[63] Conte, Alex (2008), *Handbook on Human Rights Compliance While Countering Terrorism*, Center on Global Counterterrorism Cooperation, January, p. 17.
[64] Greer, Steven (1997), *The exceptions to Articles 8 to 11 of the European Convention on Human Rights,* Council of Europe, Strasbourg, p. 15.
[65] Rigaux, François (1992), *La vie privée: une liberté parmi les autres ?*, Larcier, Bruxelles, p. 47.

considerations of national security and protection against organised crime[66] can shrink as a result of thorough examination of two requirements: national authorities must prescribe in law 'adequate and effective guarantees against abuse', and they should provide a sufficient degree of democratic control over the exercise of the administration's discretion.[67]

17. The interests of national security and the prevention of crime can justify, under certain circumstances, infringements of the right to respect for private and family life, home and correspondence,[68] the right to freedom of expression[69] and the right to freedom of peaceful assembly and association.[70] The main cases in which the defence of these interests has been raised indicate that 'national security' concerns, in this context, the security of the state and the democratic constitutional order from threats posed by enemies both within and without.[71]

Security as a Legitimate Aim of Interference with Privacy

18. Many security measures are believed to be at least potentially impinging on the right to privacy, as recognised by Article 8 ECHR.[72] Unsurprisingly, several important cases in which the 'national security' argument has been pleaded have involved interferences with such right.[73]

19. The Strasbourg organs have notably dealt with secret surveillance, accepting that it constitutes by itself an interference with Article 8 ECHR, while also acknowledging that it can, under certain circumstances, be justified on national security grounds. Secrecy by its very nature is considered to increase the risk of abuses, making the availability of effective supervision all the more crucial. Thus, it is notably accepted that any individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied.[74] The possible violation of Article 8 ECHR rights triggers off the application of Article 13 ECHR, on the right to an effective remedy before a national authority, even if the limited effectiveness of such a remedy in situations where the interference is absolutely secret can be discussed.[75] For covert measures of surveillance to be compliant with the ECHR, they must be based on a particularly precise law, giving citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to such measures.[76] This becomes increasingly important as the technology available for surveillance purposes

---

[66] Arai-Takahashi, Yutaka (2002), *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR,* Intersentia, Antwerpen-Oxford-New York, p. 83.
[67] *Ibidem*, p. 74.
[68] Art. 8(2) ECHR.
[69] Art. 10(2) ECHR.
[70] Art. 11(2) ECHR.
[71] Greer, *op. cit.*, p. 19.
[72] On this right, see notably: Sudre, Frédéric (ed.) (2005), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, Bruxelles.
[73] Art. 8 ECHR: "*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*". On the relevant case law, see: De Hert, Paul (2005), "Balancing security and liberty within the European human rights framework: A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review*, 1(1), pp. 68-96.
[74] ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev,* Application no. 62540/00, Judgement of 28 June 2007, § 58. However, when the gist of the applicant's compliant is not that his Art. 8 ECHR rights have been threatened by the very existence of laws permitting secret surveillance, but that measures of surveillance have actually been applied to him, the ECtHR must be satisfied that there is a reasonable likelihood that some such measures have been applied (see, for instance: ECtHR, *Case of Iliya Stefanov v. Bulgaria*, Application no. 65755/01, Judgement of 22 May 2008, § 49).
[75] Trechsel, op. cit., p. 96. Some scholars are very critical towards case law on secret surveillance practices, and, in general, towards the assumption according to which democratic theory contains resources adequate to solving the problem that state secrecy creates (Sagar, Rahul (2007), "On Combating the Abuse of State Secrecy", *The Journal of Political Philosophy,* Volume 15, Number 4, p. 405).
[76] The following minimum safeguards should be set out in statue law to avoid abuses: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their communications monitored; a limit on the duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which data obtained may or must be erased or the records destroyed (ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev,* Application no. 62540/00, Judgement, 28 June 2007, § 75).

becomes more sophisticated.[77] In the landmark judgement *Klass v. Germany*,[78] it was established that, as a matter of principle, the person affected by the measures must be informed at least retrospectively, although the information could, in certain cases, be withheld indefinitely. As withholding indefinitely the information makes the recourse to remedies practically inoperative, other effective means of control must be instituted by the relevant legislation. This approach has been criticised for focusing on the mere availability of domestic institutional controls, disregarding the assessment of the effectiveness of the supervision provided.[79]

20. The ECtHR clarified recently, in its *Liberty* judgement,[80] that the principles of accessibility and clarity that need to be complied with by the rules governing the interception of individual communications are also applicable to more general programmes of surveillance.[81] The *Liberty* case originated in an application[82] against the United Kingdom and Northern Ireland lodged with the Court by Liberty, British Irish Rights Watch and the Irish Council for Civil Liberties, a British and two Irish civil liberties' organisations, on 9 September 1999, concerning the implementation of the Interception of Communications Act of 1985.[83] The ECtHR concluded in its judgement that the law examined did not indicate with sufficient clarity the scope or manner of exercise of the very wide discretion conferred on the state to intercept and examine communications. In particular, 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.[84]

Security and Data Protection

21. The right to privacy has been flanked in Europe with another, distinct right: the right to the protection of personal data.[85] The right to privacy and the right to the protection of personal data (or 'data protection') overlap partially, but not completely, as data protection law serves a multiplicity of interests extending well beyond traditional conceptualisations of privacy.[86] The different nature of both rights has been linked to the elaboration of two complementary sorts of legal tools aiming at the control and limitation of power in the context of the development of the democratic constitutional state: firstly, tools that tend to guarantee non-interference in individual matters, or the opacity of the individual, and, secondly, tools that tend to guarantee the transparency and accountability of the powerful. 'Opacity tools' can be described as measures protecting individuals against external inferences, working as shields,[87] while 'transparency tools' tend to regulate the exercise of power,[88] and both types of tools are in principle to be combined in order to cope effectively with power relations.[89] The right to privacy has been related conceptually to the first type of tools, as by default it protects the opacity of individuals.

---

[77] *Ekimdzhiev*, § 75.
[78] *Klass v. Germany,* judgement of September 1978, Series A N° 28.
[79] Greer, *op. cit.*, p. 22.
[80] ECtHR, *Case of Liberty and Others v. The United Kingdom*, Application no. 58243/00, Judgement of 1 July 2008.
[81] *Liberty,* § 63. The judgement creates notably an important argument against the introduction of secret data mining programs in Europe (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 for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), October, p. 26.
[82] No. 58243/00.
[83] Later repealed by repealed by the Regulation of Investigatory Powers Act 2000.
[84] *Liberty,* § 69.
[85] On the relation between the right to privacy as recognised by international law and the EU right to data protection, see: Bygrave, Lee A. (1998), "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology,* 6, pp. 247-284. See also: Bygrave, Lee A. (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague, London, New York; Del Castillo Vázquez, Isabel-Cecilia (2007), *Protección de datos: cuestiones constitucionales y administrativas (El derecho a saber y la obligación de callar)*, Aranzadi, Thomson Civitas, Cizur Menor; Docquir, Benjamin (2008), *Le droit à la vie privée*, De Boeck, Larcier, Bruxelles; Flaherty, David H. (1989), *Protecting Privacy In Surveillance Societies*, University of North Carolina Press, Chapel Hill; Gutwirth, Serge (2002), *Privacy and the information age*, Rowman & Littlefield Publishers, Lanham.
[86] Bygrave, Lee A. (2001), "The Place of Privacy In Data Protection Law", *University of NSW Law Journal,* 6, p. 4.
[87] Gutwirth, Serge (2007), "Biometrics between opacity and transparency", *Annali dell'Istituto Superiore di Sanità,* 43(1), p. 61.
[88] *Ibidem*, p. 62.
[89] De Hert, Paul and Serge Gutwirth (2003), "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location based services and the virtual residence", in Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)*, European Commission, July, p. 162.

The right to data protection has been connected to the second type, as, also by default, it calls for the transparency of the processing of personal data, giving individuals subjective rights and enforcing the accountability of the processors of data.[90]

22. The ECHR does not have any provision explicitly referring to the protection of personal data, but the ECtHR has been giving increased support to data protection principles developed through other instruments.[91] The ECtHR case law has notably referred to the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention 108).[92] In the EU framework, the right to data protection was recognised at the highest level in 2000 in the EU Charter of Fundamental Rights, which establishes it as an autonomous fundamental right,[93] different from the right to privacy.[94] This recognition of the right to data protection as a separate right was celebrated as being more respectful of the different European constitutional traditions.[95]

23. Despite the increasing formal support granted in Europe to the right to data protection, over the recent years a series of developments have highlighted serious lacunae in the legal framework developing it.[96] Two are the main difficulties encountered: first, the effective implementation of data protection law across jurisdictions with different levels of protection; second, the apparently inherent 'relativity' of data protection law, which comes to the surface when the right to data protection is to be set against other interests, such as security.[97] Concerning the former difficulty, it shall be noted that, since the very origins of European data protection, legal instruments have been primarily concerned with the promotion of the cross-border free-flow of data. In this sense, the mentioned Convention 108 already fully acknowledged, in 1981, the significance of the increasing flow of personal data that was undergoing across borders at the time. Similarly, the Guidelines on the Protection of Privacy and Transborder Flows of Personal data, adopted a year before in the context of the Organisation for Economic Co-operation and Development (OECD),[98] also translated a will to contribute to the free

[90] De Hert, Paul and Serge Gutwirth (2006) "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power" in Claes, E., A. Duff and Serge Gutwirth (eds.), *Privacy and the criminal law*, Intersentia, Antwerp-Oxford-New York, p. 65.

[91] In *Z v. Finland* (Judgment of 25 February 1997, Reports of judgments and Decisions 1997-I), the ECtHR noted that the protection of personal data was of fundamental importance to a person's enjoyment of his or her right to respect for private life. See also, notably: *Rotaru v. Romania*, Application no. 28341/95, Judgement of 4 May 2000, §§ 43-44 and *Amann v. Switzerland*, Application no. 27798/95, Judgement of 16 February 2000, §§ 65-67. Although the Strasbourg organs have acknowledged that the protection of personal data is an issue that can fall within the scope of Article 8 ECHR, they have never held that all aspects of the processing of personal data are worthy of protection under the right to privacy (De Hert and Gutwirth, (2006), *op. cit.*, p. 77). On the ECtHR assessment of the relation between the right to privacy as established by Article 8 of the ECHR and the protection of personal data, see also: *I v. Finland*, Application no. 20511/00, Judgement of 17 July 2008 (in particular, §§ 35, 38 and 40).

[92] ETS 108, Council of Europe, Strasbourg, 28 January 1980; see also the Additional Protocol to the Convention regarding supervisory authorities and transborder data flows (ETS 181, Council of Europe, Strasbourg, 8 November 2001). All EU Member States are parties to this Convention, which should be implemented in conformity notably with other relevant sources, such as the Recommendation regulating the use of personal data in the police sector that the Council of Europe's Committee of Ministers addressed to the Member States of the Council of Europe in 1987 (which has also become the basic standard in the field and is referred to by different EU instruments).

[93] On the right to the protection of personal data in the EU, see: Arenas Ramiro, Mónica (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant Lo Blanch; Di Martino, Alessandra (2004), *Datenschutz im Europäischen Recht*, WHI Paper 15/04, Walter Hallstein-Institut für Europäisches Verfassungsrecht für Europäisches Verfassungsrecht, Humboldt-Universität zu Berlin.

[94] Article 286 of the Treaty of the European Community (TEC) also refers to the protection of personal data (Treaty establishing the European Community, OJ C 325 of 24 December 2002).

[95] De Hert and Gutwirth (2006), *op. cit.*, p. 78.

[96] See, notably: 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; González Fuster, Gloria and Pieter Paepe (2008), "Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects", in Guild, Elspeth and Florian Geyer (eds.), (2008), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, pp. 129-150. For a general description of the legal framework, see: Andenas, Mads and Stefan Zleptnig (2003), "Surveillance and Data Protection: Regulatory Approaches in the EU and Member States", *European Business Law Review,* 14(6), pp. 765-813.

[97] Burkert, Herbert (1999), *Privacy-Data Protection: A German/European Perspective*, 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Massachusetts, June, p. 67).

[98] Organisation for Economic Co-operation and Development (OECD) (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted in the form of a *Recommendation of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data* on 23rd September, Paris.

flow of data.[99] Nevertheless, when cross-border implementation is considered, the question remains open of how to reconcile the rights granted by data protection and the fact that the information provided to individuals is in many cases insufficient, especially taking into account that the limited information available to individuals can impede their enjoyment of the rights granted.[100]

24. The ways in which security limits or channels the applicability of EU data protection law can be described as dual.[101] The EU has established a harmonized regime for the protection of personal data regarding data processing undertaken in the context of First Pillar activities, from which Third Pillar activities are excluded, thus delineating an external limit to a determined framework of protection. Additionally, inside the First Pillar data protection framework different exceptions and restrictions also apply, notably in relation with security, configuring its internal limits.

Security as an External Limit for EC Data Protection

25. The key legal reference for Community data protection is Directive 95/46/EC,[102] generally referred to as the Data Protection Directive, which provides a harmonized regime for processing of data in the course of activities falling under Community law, and related provisions on the transfer of personal data from the EU to third countries. Article 3 of the Data Protection Directive excludes from its scope of application the processing of data "*in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law*".[103] Even if the possible entry into force of the Lisbon Treaty would represent the abolition of the pillar structure of the EU, the limited scope of application of the Data Protection Directive would remain unaltered by virtue of said Article 3.

26. There is no equivalent general EU legal instrument for data protection in the Third Pillar, even if the constitutive texts of different Third Pillar institutions and information systems foresee a number of provisions corresponding to basic data protection principles.[104] In 2005, the EC adopted a proposal

---

[99] The rationale behind the OECD Guidelines was indeed already based on the fact that automated data processing enables vast quantities of data to be transmitted, within seconds, across national frontiers, and that disparities in national legislations could hamper the free flow of data, considered crucial to business (Critchell-Ward, Ann and Kara Landsborough-Mcdonald (2007), "Data Protection Law in the European Union and the United Kingdom", *Comparative Law Yearbook of International Business,* Vo. 29, p. 520). For an overview of legal instruments related to trans-border data protection, see: Gunasekara, Gehan (2006), "The 'final' privacy frontier? Regulating trans-border data flows", *International Journal and Information Technology,* 15(3), pp. 362-393.

[100] De Schutter, Bart (2001), "Data Protection in the Area of Freedom, Security and Justice", in Collegium (2001), *Special Edition — Proceedings of the Conference: 'Integrated Security in Europe, a Democratic Perspective'*, No. 22, XII.2001, Bruges, p. 54.

[101] EC (2007), *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, Brussels, 7.3.2007, p. 7.

[102] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50. On this Directive, see: Poullet, Yves (2006), "The Directive 95/46/EC: Ten years after", *Computer Law & Security Report,* 22, pp. 206-217.

[103] The ECJ clarified the meaning of this provision in the judgement of 6 November 2003 in Case C-101/01, *Bodil Lindqvist Bodil Lindqvist* ([2003] ECR I-12971).

[104] Over the years, different instruments have set out the protection of personal data in the context of Title VI TEU. They include the Convention implementing the Schengen Agreement of 1990 (Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, p. 19–62), the Europol Convention (Council Act of 26 July 1995 drawing up the Convention based on Article K.3d of the Treaty on European Union on the establishment of a European Police Office (Europol Convention), OJ C 316 of 27.11.1995), the Decision setting up Eurojust (Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 06.03.2002, pp. 1-13) and the Rules of procedure on the processing of personal data at Eurojust (Rules of procedure of the processing and protection of personal data at Eurojust, adopted by the college of Eurojust on 21 October 2004 and approved by the Council on 24 February 2005, OJ C 68, 19.3.2005. pp. 1-10), the Convention on the use of information technology for customs purposes, including data protection provisions applicable to the Customs Information System (CIS) (Council Act 95/C316/02 of 26 July 1996 drawing up the Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the use of information technology for customs purposes, OJ C 316, 27.11.1995, pp. 33-42) and the Convention on mutual assistance in criminal matters between the Member States (Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, pp. 1-15 (in particular, Art. 23).

for a Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters,[105] aimed at ensuring the protection of personal data processed in the framework of police and judicial cooperation in criminal matters between the Member States. The Council Framework Decision on the protection of personal data in the field of police and judicial cooperation in criminal matters was finally adopted on 27 November 2008,[106] but its limited scope of application does not allow for it to be compared with the Data Protection Directive.

27. Determining whether certain types of processing should be considered to take place in the context of First Pillar or Third Pillar activities is not always a straightforward operation. The issue was particularly discussed in reference to the first EU-US agreement on the transfer of Passenger Name Records (PNR) information, examined by the European Court of Justice (ECJ) in 2006. The original EU-US PNR agreement had been negotiated following the passing of US legislation requiring air carriers operating flights to, from, or through the US to provide the US Department of Homeland Security Bureau of Customs and Border Protection with access to data contained in their automated reservation and departure control systems. As the US law appeared to conflict with EU data protection law, talks between the US government and the EU were launched. They resulted in a Council Decision concerning the conclusion of an Agreement between the European Community and the US on the processing and transfer of Passenger Name Records (PNR),[107] and in a European Commission decision on the adequate protection of those personal data, in the understanding that, taking into account the purposes for which the collection of data originally took place, the processing fell under the scope of the First Pillar. The European Parliament did not share this view, and took the case to the ECJ. In its assessment, the ECJ focused its attention on the fact that obligation to transfer the data to US authorities was based on provisions regarding the reinforcement of security, and that the data was going to be used for such purposes.[108] Thus, it concluded that the agreement did not fall under the First Pillar, and on 30 May 2006 annulled both the Council Decision and the Commission Decision[109] for having been adopted on an inappropriate legal basis.

---

[105] EC (2005), *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, COM(2005) 475 final, 4.10.2005, Brussels. This proposal generated many different expectations and concerns, notably regarding the convenience of developing clear rules for data transfers to third countries for the Third Pillar responsibilities (De Hert, Paul and Bart De Schutter (2008), "International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift", in Martenczuk, Bernd and Servaas Van Thiel (eds.) (2008), *Justice, Liberty, Security: New challenges for EU external relations,* VUB Press, Brussels, p. 338). See also, on the proposed Draft Framework Decision: De Hert, Paul, Vagelis Papakonstantinou and Cornelia Riehle (2008), "Data protection in the third pillar: cautious pessimism", in M. Martin (Ed.), *Crime, rights and the EU: The future of police and judicial cooperation*, JUSTICE, London; McGinley, Marie and Roderick Parkes (2007), *Data Protection in the EU's Internal Security Cooperation: Fundamental Rights vs. Effective Cooperation?*, Stiftung Wissenschaft und Politik (SWP) Research Paper 5, German Institute for International and Security Affairs, Berlin, May.

[106] The need for special data protection in the area of police and judicial cooperation would also be recognised in the Lisbon Treaty, if adopted (Kranenborg, Herke (2008), "Access to documents and data protection in the European Union: on the public nature of personal data", Common Market Law Review, 45, p. 1.089).

[107] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States Department of Homeland Security, Bureau of Customs and Border Protection, *Official Journal of the European Union,* L 183, 20/05/2004, p. 83, and Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *Official Journal of the European Union,* L 183, 20/05/2004, pp. 84-85. On this agreement, see also: González Fuster, Gloria and Paul De Hert (2007), "PNR and compensation", in Lodge, Juliet (ed.), *Are You Who You Say You Are? The EU and Biometric Borders*, Wolf Legal Publishers, Nijmegen, pp. 101-109.
Privacy International (PI) (2004), *Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection*, First Report on 'Towards an International Infrastructure for Surveillance of Movement', February.

[108] Terrasi, Alfredo (2008), "Trasmissione dei dati personali e tutela della riservatezza: l'accordo tra Unione Europea e Stati Uniti del 2007", *Rivista di diritto internazionale,* 91(2), p. 382.

[109] Joined Cases C-317 and C-318/04, *European Parliament v. Council and Commission*, Judgment of the Grand Chamber of 30 May 2006 [2006] ECR I-4721. On this judgement, see also: Gilmore, Gráinne and Jorrit Rijpma (2007), "Case law: Joined Cases C-317 and C-318/04, European Parliament v. Council and Commission, Judgment of the Grand Chamber of 30 May 2006 [2006] ECR I-4721", *Common Market Law Review,* 44, pp. 1081-1099; González Vaqué, Luis (2006), "El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EE.UU. para la transmisión de datos sobre los pasajeros de las compañías aéreas", *Revista Española de Derecho Europeo,* 20, octubre - diciembre, pp. 557-576; Guild, Elspeth and Evelien Brouwer (2006), *The Political Life of Data: the ECJ Decision on the PNR Agreement between the EU and the US*, Policy Brief No. 109, CEPS, Brussels, July; Mendez, Mario (2007), "Passenger Name Record Agreement: European Court of Justice", *European Constitutional Law Review,* 3(1), pp. 127-147; Michel, Valérie (2006), "La dimension externe de la protection des données à caractère personnel: acquiescement, perplexité et frustration", *Revue trimestrielle de droit européen,* 42(3), pp. 549-559; Pedilarco, Emanuele (2006), "Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione Europea - Stati Uniti sul trasferimento dei dati dei passeggeri aeri", *Diritto pubblico comparato ed europeo,* 2006, pp. 1225-1231.

Security as an Internal Limit of Data Protection

28. Certain provisions allow for security-related exceptions and restrictions to applicable data protection provisions, under certain circumstances. The Data Protection Directive foresees in its Article 13(1) that Member States may restrict data protection rights granted by its provisions "*when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;* (…) *(g) the protection of the data subject or of the rights and freedoms of others*".[110] Convention 108 also foresees a series of exceptions and restrictions for the application of its main provisions.[111] Similarly, even if since 2001 a protocol to Convention 108 requires the parties to allow data transfers to third states only if such states provide an 'adequate level of protection',[112] the parties are allowed to derogate from such an adequacy requirement for a number reasons, including the existence of a "*legitimate prevailing interest, especially important public interests*".[113]

29. Such security-related restrictions to general data protection principles are harmonized at EU level only in a limited number of cases, the most prominent example being the harmonization imposed by Directive 2006/24/EC[114], known as the Data Retention Directive, which requires telecommunications providers to automatically collect and retain all information on users' activities. The origins of establishing at EU level such an approach can be traced back to 2002,[115] when a scheduled review of the Directive on privacy and data protection in the field of telecommunications lead to adoption of Directive 2002/58/EC[116], generally referred to as the e-Privacy Directive, and the introduction of a special provision to allow Member States to adopt measures requiring that logs of telecommunication activities be kept for certain periods of time even in the absence of a belief that the users are engaged in any criminal activity,[117] and even if the provisions previously in vigour required that the data in question had to be deleted as soon as possible.

---

[110] It has been argued that despite the content of Art. 13 of Directive 95/46/EC, Art. 14 of the same Directive potentially allows data subjects to object to their information being processed by a particular body even when issues of national security arise; on this hypothesis, see: Moiny, Yves (2005), *Protection of Personal Data and Citizens' Rights of Privacy in the Fight Against the Financing of Terrorism*, CEPS Policy Brief, CEPS, Brussels, March, p. 5.

[111] Derogations must be provided by the law and constitute a necessary measure in a democratic society in the interests of "*protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences*" or "*protecting the data subject or the rights and freedoms of others*" (Art. 9(2) of Convention 108).

[112] Additional Protocol to the Convention regarding supervisory authorities and transborder data flows, ETS 181, Council of Europe, Strasbourg, 8 November 2001.

[113] See Art. 2(2)(a) of the Additional Protocol to Convention 108. See also: Bignami, Francesca (2007), *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining*, Duke Law School Working Paper Series, Paper 75, p. 39.

[114] 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. The Data Retention Directive is currently being challenged by Ireland at the ECJ. On this Directive, 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; Vilasau, Mónica (2006), "La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad", *Revista d'Internet, Dret i Política,* No. 3.

[115] Bunyan, Tony (2002), « Surveillance des télécommunications : fin de partie », *Culture et Conflits*, 46, pp. 65-71. See also: Pérez Asinari, María Verónica (2004), "La regulación de los datos de tráfico en la Unión Europea: ¿Entre la seguridad y los derechos fundamentales?", *Lexis Nexis,* II(4), pp. 49-59.

[116] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002, pp. 37-47.

[117] The provision chronologically followed Art. 15(2) of the 'e-Commerce Directive', according to which Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, pp. 1–16). See, on this subject: Ballesteros Moffa, Luis Ángel (2008), "Hacia un difícil equilibrio entre privacidad y seguridad: la conservación de datos en las comunidades electrónicas y la transferencia de datos de pasajeros por las compañías aéreas", *Revista Española de Derecho Administrativo,* 137(2008), p. 43.

IV. Security Policies and the European Legal Framework

30. The literature provides many accounts of the progressive transformation of the EU into a security actor. European security has notably been said to be the result of a process of externalisation of (national) 'internal security' issues towards a European 'internal security regime',[118] thus allowing for the identification of two parallel processes: one of 'Europeanisation' and another of 'externalisation' of security concerns.[119] These processes are believed to have benefited from the global success of broad perceptions of security in which counter-terrorism plays a key role,[120] a notion of security sometimes described in terms of a wide 'security policy continuum'.[121] The EU has dealt with traditionally (national) 'internal security' issues in the area of Justice and Home Affairs. Additionally, over the years, EU institutions have increasingly emphasised the importance of what has come to be known as the 'external dimension' of EU Justice and Home Affairs, in a process described as the 'externalisation' of such an area.[122] In the course of this process, EU Justice and Home Affairs tends to become a strategic policy in the context of EU's external relations, which, in their turn, are also becoming ever more important for the EU in general. Two different 'externalising' processes are therefore identified: one driving national 'internal' security issues towards their Europeanisation, and the other pushing these (Europeanised) 'internal' security issues towards the filed of EU external relations. In their assessment of the implications for the EU legal framework of these developments, some scholars are especially worried with respect to aspects of accountability of policy choices.[123] In addition, many concerns have been expressed as regards the monitoring of the protection and promotion of human rights in the context of European security. The EU Agency for Fundamental Rights,[124] recently established, enjoys only a limited mandate, not covering Third Pillar issues. Other bodies with monitoring duties, such as the European Data Protection Supervisor (EDPS),[125] have also limited powers.[126]

An Overview

[118] Anderson, Malcolm (2007), "Internal and External Security in the EU: Is There Any Longer a Distinction?", in Gänzle, Stefan and Allen G. Sens (eds.), *The Changing Politics of European Security: Europe alone?*, Palgrave, Hampshire, p. 38.
[119] Anderson, Malcolm and Joanna Apap (2002), *Changing Conceptions of Security and their Implications for EU Justice and Home Affairs Cooperation*, CEPS Policy Brief No. 26, CEPS, October, p. 3.
[120] Den Boer, Monica (2003), *9/11 and the Europeanisation of Anti-terrorism Policy: a Critical Assessment*, Notre Europe Policy Papers, N° 6, September, p. 3 and p. 6.
[121] Den Boer, *op. cit.*, p. 16. For a description of the EU Area of Freedom, Security and Justice as a 'security continuum' harbouring an inter-connection between security, crime and immigration in which migration tends to be regarded as a meta-propeller for different problems: Den Boer, Monica (2008), *Immigration and Its Effects on the Security Discourse in Europe: Time for Demystification*, Amsterdam Law Forum, 1(1). The success of such a perception is to be put in the context of a redefinition of the traditional distinctions between 'internal security' and 'external security' notions believed to be operating in Europe since the collapse of the bi-polar system in 1989 (Anderson, Malcolm et al. (1995), *Policing the European Union*, Oxford University Press, Oxford, p. 179). While some authors have described the redefinition in terms of a blurring of notions (Anderson and Apap, *op. cit.*, p. 1; also in this sense: Rees, Wyn (2006), *Transatlantic-Counter Terrorism Cooperation: The New Imperative*, Routdlege, New York, p. 7., others prefer to speak in terms of a 'de-differentiation' of the questions of internal and external security, portray the field of security as a generative space of struggle crossing the internal and external fields of security (Bigo, Didier (2005), "Globalized-in-security: the Field and the Ban-opticon" in Solomon, John and Naoki Sakai, *Traces: Translation, Philosophy and Colonial Difference*, Volume 4, p. 5).
[122] Balzacq, Thierry (2008), *The External Dimension of EU Justice and Home Affairs: Tools, Processes, Outcomes,* CEPS Working Document No. 303, CEPS, September, Brussels, p. 2.
[123] In this sense: Mathiesen, Thomas (2005), *Lex Vigilatoria: Towards a control system without a state?*, Essays for civil liberties and democracy in Europe, European Civil Liberties Network, p. 2; Puntscher Riekmann, Sonja (2008), "Security, Freedom and Accountability: Europol and Frontex", in Guild, Elspeth and Florian Geyer (eds.), (2008), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, pp. 19-34.
[124] Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, OJ L 53, 22.02.2007, pp. 1-14. See also: De Schutter, Olivier (2007), "L'agence des droits fondamentaux", *Journal des tribunaux du droit européen,* Avril(138), pp. 97-102.
[125] On the EDPS, see: Hijmans, Hielke (2006), "The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority", *Common Market Law Review,* 43, pp. 1313-1342.
[126] For a description of monitoring mechanisms and practices in the field of EU data protection, see: González Fuster, Gloria and Serge Gutwirth (2008), *Data Protection in the EU: Towards 'Reflexive Governance'?*, REFGOV Working Paper Series, FR-19, July, Brussels.

31. A key step for the development of EU security was the 1985 Schengen Agreement[127] support of the abolition of internal border controls, and, as a side measure, the call for common control of external borders.[128] The approach has been described as an example of the doctrine of 'compensatory measures', according to which in order to 'compensate' for the alleged security deficit created by the abolition of internal frontier controls there is a need to enhance police co-operation among states, *inter alia* to ensure effective control of common external frontiers.[129] As a consequence of the creation of a common external border, the EU[130] was to become progressively involved in issues not only of security, but also of identity and control.[131] Schengen provisions were to be implemented through the establishment of the Schengen Information System (SIS), the oldest European border-related database system, containing alerts about objects and persons considered to be a threat to Member States.[132] In its new, soon-to-come, generation, SIS II,[133] the system will allow to check identities on the basis of biometric information (facial photographs and fingerprints).

32. In 1992, the Treaty of Maastricht[134] marked the creation as an established area of EU activity of EU Justice and Home Affairs, eventually re-baptised as the Area of Freedom, Security and Justice (AFSJ).[135] The recognition of its international dimension was inaugurated with the entry into force of the Treaty of Amsterdam[136] in May 1999.[137] The Treaty of Amsterdam also provided EU Justice and Home Affairs with a hybrid nature, shifting immigration, asylum, and civil law issues from the Third Pillar to the First Pillar,[138] while leaving policing and criminal law issues in the Third Pillar.[139] In October 1999, the Council adopted the Tampere Programme, establishing the priorities for EU Justice and Home Affairs issues for the period 1999-2004. The Tampere Programme explicitly stated that internal and external security policies require coordination,[140] putting the need for external relations in the area of Justice and Home Affairs firmly on the political agenda.[141] The events of 9/11 provided EU Justice and Home Affairs with a new impetus.[142] Even if counterterrorism is still primarily a concern of Member States, the EU has since 9/11 made progress on a large number of issues considered of importance for such purposes, notably including measures in the area of judicial and police cooperation, the prevention of financing of terrorism, border controls and cooperation with the US.[143]

---

[127] Agreement between the governments of the states of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, signed at Schengen, 14 June 1985.
[128] In Article 17 of the Schengen Agreement, external borders are referred to as the place to which checks will be transferred. The article also mentions the need to harmonize laws, regulations and administrative provisions for this purpose, complemented by measures aimed at safeguarding internal security and preventing illegal immigration.
[129] Anderson, (1995), *op. cit.*, p. 135.
[130] The Convention on the Implementation of the Schengen Agreement (CISA) replacing the Schengen Agreement came into force in 1995; Italy, Spain, Portugal, Greece, Austria, Denmark, Finland and Sweden, as well as Iceland and Norway eventually joined the area. With the Treaty of Amsterdam, the body of Schengen rules was incorporated into EU law. The United Kingdom and Ireland opted out of these provisions, and Denmark also adopted a special position.
[131] Peers, *op. cit.*, p. 93.
[132] SIS has been notably described as and has been described as the EU area where there is the closest relationship between migration and criminal matters (Cholewinski, Ryszard (2007), "The Criminalisation of Migration in EU Law and Policy" in Baldaccini, Anneliese, Elspeth Guild and Helen Toner (2007), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, Oxford, p. 303).
[133] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, pp. 4-23. On data protection implications of SIS II, see: Karanja, S. K. (2006), "SIS II Legislative Proposals 2005: Gains and Losses!", *Yulex,* 2005, pp. 81–103.
[134] Treaty on European Union (TEU), signed on 7 February 1992.
[135] Peers, *op. cit.*, p. 8.
[136] Signed on October 2, 1997.
[137] Martenczuk, Bernd and Servaas Van Thiel (2008), "The External Dimension of EU Justice and Home Affairs: Evolution, Challenges and Outlook", in Martenczuk, Bernd and Servaas Van Thiel (eds.) (2008), *Justice, Liberty, Security: New challenges for EU external relations,* VUB Press, Brussels, p. 10.
[138] To a special Title IV of Part Three of the Treaty establishing the European Community (TEC).
[139] In Title VI TEU (Peers, Steve (2008), *Changing the institutional framework for EU Justice and Home Affairs law without the Lisbon Treaty,* Statewatch Analysis, July, p. 1).
[140] Anderson and Apap, *op. cit.*, p. 3.
[141] Alegre, Susie (2008), *The EU's External Cooperation in Criminal Justice and Counter-Terrorism: An Assessment of the Human Rights Implications with a particular focus on Cooperation with Canada*, CEPS Special Report, Centre for European Policy Studies, Brussels, September, p. 3.
[142] Anderson and Apap, *op. cit.*, p. 8.
[143] For instance, the amendment of the Money Laundering Directive, the setting up of a Eurojust cross-border prosecution unit, the framework decision on joint investigative teams and the seizure of assets and evidence by a judicial order issued in any Member State across the whole territory of the EU (Anderson and Apap, *op. cit.*, p. 7). In 2002, the Council adopted the Framework Decision for the creation of the European Arrest Warrant (Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) and Statements made by certain Member States on the adoption of the Framework Decision, OJ L 190, 18.7.2002, pp. 1–20), sometimes

The Tampere Programme was followed by the Hague Programme on strengthening Freedom, Security and Justice in the EU, adopted by the EU Council on November 2004.[144] The Hague Programme included a call for the elaboration of a strategy on the external aspects of EU Justice and Home Affairs. Accordingly, in October 2005, the Council adopted a EU Strategy for the External Dimension of Justice and Home Affairs,[145] on the basis of a communication from the European Commission.[146] In December 2005, the EU adopted a Counter-Terrorism Strategy consisting of different normative and institutional responses, and reinforcing the idea that internal and external aspects of security are intimately linked.[147]

33. A significant response against perceived terrorist threats came in the form of 'targeted', 'smart' sanctions against persons and groups considered to be terrorists, crucially with the aim of transposing United Nations (UN) Security Council Resolution 1373/2001 on the suppression of terrorism.[148] Targeted sanctions have since then triggered many different human rights concerns, mainly related to the rights to a fair trail and an effective remedy.[149] UN resolutions have been implemented at EU level both through common positions adopted under the Common Foreign and Security Policy (CFSP) and Commission and Council regulations.[150] These measures have repeatedly been challenged before the Court of First Instance (CFI). A considerable case law has developed,[151] with important clarifications not only regarding targeted sanctions in particular, but also more generally on the relation between European law and international law. The ECJ *Kadi and Al Barakaat* judgement[152] is especially important in this sense. In this case, the ECJ set aside previous judgements of the CFI[153] and declared that the CFI had erred in law in ruling that the Community courts had, in principle, no jurisdiction to review the validity of the regulation at issue, except in respect of certain overriding rules of international law known as *ius cogens*. Another key judgement was provided by the CFI in the *Organisation des Modjahedines du Peuple d'Iran (OMPI)* case,[154] as the CFI annulled for the first time a Community measure freezing the financial assests of a particular legal person,[155] and made a number of crucial findings relating to the right to a fair hearing in this context.

---

linked to the fight against terrorism. See, on this issue: Sievers, Julia (2008), "Too Different to Trust? First Experiences with the Application of the European Arrest Warrant", in Guild, Elspeth and Florian Geyer (eds.), (2008), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, pp. 109-128).

144 Pineda Polo, Cristina (2005), "The Hague Programme: An Introduction" in Alegre, Susie et al., *The Hague Programme: Strengthening Freedom, Security and Justice in the EU*, European Policy Centre (EPC) Working Paper no. 15, February, pp. 6-15.

145 The Strategy (Council of the European Union (2005*), A Strategy for the External Dimension of JHA: Global Freedom, Security and Justice*, 30 November, Brussels) identifies five thematic priorities for the development of relations with third countries in this field: human rights; strengthening institutions and good governance; migration, asylum and border management; fight against terrorism; and organised crime.

146 EC (2005), *Communication from the Commission: A Strategy on the external dimension of the Area of Freedom, Security and Justice,* COM(2005) 491 final, 12.10.2005.

147 Council of the European Union (2005), *The European Union Counter-Terrorism Strategy*, 30 November, p. 6.

148 This policy began with a package of four acts originally adopted in December 2001, comprising two Common Positions adopted jointly on the basis of Articles 15 and 34 TEU, an EC Regulation implementing the EC law aspects of the foreign policy provisions of the second Common Position, and an EC Decision further implementing that Regulation (Peers, *op. cit.*, p. 518).

149 Biersteker, Thomas J. and Sue E. Eckert (2006), *Strengthening Targeted Sanctions Through Fair and Clear Procedures*, Report commissioned by the governments of Germany, Switzerland and Sweden, Watson Institute for International Studies, p. 13.

150 Cameron, Iain (2003), "European Union Anti-terrorist Blacklisting", *Human Rights Law Review,* 2(2), p. 227.

151 On these developments, see also: Nettesheim, Martin (2007), "U. N. Sanctions Against Individuals – A Challenge To The Architecture of European Governance", *Common Market Law Review,* 44(3), pp. 567-600; Porretto, Gabriele (2008), "The European Union, Counter□Terrorism Sanctions against Individuals and Human Rights Protection" in Miriam Gani and Penelope Mathew (ed.), *Fresh Perspectives on the 'War on Terror'*, pp. 235-268; Bulterman, Mielle (2006), "Fundamental Rights and the United Nations Financial Sanction Regime: The Kadi and Yusuf Judgments of the Court of First Instance of the European Communities", *Leiden Journal of International Law*, 19, pp. 753-772; Tappeiner, Imelda (2005), "The fight against terrorism: The lists and the gaps", *Utrecht Law Review,* 1(1), pp. 97-125.

152 *Yassin Abdullah Kadi, Al Barakaat International Foundation v Council of the European Union, Commission of the European Communities, United Kingdom of Great Britain and Northern Ireland*, Joined Cases C-402/05 P and C-415/05 P, Judgment of the Court (Grand Chamber) of 3 September 2008.

153 Of 21 September 2005.

154 *Organisation des Modjahedines du peuple d'Iran v. Council and UK (OMPI),* Case T-228/02, Judgement of the Court of First Instance (Second Chamber) of 12 December 2006.

155 The judgement was generally welcomed, even if criticism persists on the CFI resistance to provide full judicial review of terrorist lists, irrespective of the pillar they are adopted in (Eckes, Christina (2007), "Case T-228/02, *Organisation des Modjahedines du peuple d'Iran v. Council and UK (OMPI),* Judgement of the Court of First Instance (Second Chamber) of 12 December 2006", *Common Market Law Review,* 44, p. 1129).

34. As the importance of the EU as an international actor in the area of Justice and Home Affairs is progressively confirmed, questions regarding human rights considerations in this dimension become more relevant.[156] A number of ways in which the EU cooperates with third countries raise questions related to the negative responsibility of the EU and its Member States not to engage in activities that violate human rights.[157] This concerns notably the issues of the prohibition of torture[158] and the death penalty.[159] Extradition and deportation to countries outside of the EU is another main element of external JHA cooperation that potentially engages human rights protection. In this context is especially relevant the recent ECtHR judgement of *Saadi v Italy*,[160] where the ECtHR rejected the need to strike a balance between the prohibition on torture and the interests of national security, and clarified parameters of the prohibition on torture in cases of extradition or expulsion, strengthening the absolute prohibition on torture.[161]

35. The EU is currently developing a new five years strategy for its Justice and Home Affairs policy, covering the period 2010-2014. A special group, called 'The Future Group', was constituted to draft some initial considerations on the programme. 'The Future Group' presented in July 2008 its final report, titled *Freedom, Security and Privacy: European Home Affairs in an open world*.[162] In the report, the 'balancing metaphor' of *freedom vs. security* appears to have been replaced by a triangular vision of mobility, security and privacy. This triangle is presented as an already established 'European model' of balancing mobility, security and privacy, which is to be 'preserved'.[163] In this balancing triangle, 'security' would refer to state security, whereas 'privacy' would mean the right to privacy as established by Article 8(1) ECHR duly taking into account Article 8(2) ECHR,[164] but also the right to data protection.[165] At the centre of the triangle, has been placed the notion of data sharing.[166]

Security And Approaches To Technology[167]

36. Technology plays a central role in different fields of European security, from document security[168] to border control.[169] At national level, since 9/11 many Member States have expanded their legal frameworks for the monitoring of communications, taking advantage of new technological possibilities.[170] An important specific trend in this field, actually predating 9/11,[171] is to impose through

---

156 Alegre (2008), *op. cit.*, p. 16.

157 *Ibidem*, p. 32. A special issue has been with absolute lack of action in relation with certain subjects the role of EU Member States in 'secret detentions' and 'extraordinary renditions' (Amnesty International (2008), *State of Denial: Europe's Role in Rendition and Secret Detention*, London, p. 1: see also: Tóth, Judit (2008), "EU Member States' Complicity in Extraordinary Renditions", in Guild, Elspeth and Florian Geyer (eds.), (2008), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, pp. 71-87).

158 Concerning the prohibition of torture, for EU Member States or agencies receiving information or evidence the question of provenance is crucial. To use information provided by third countries that may have been extracted through torture or ill treatment would undermine the *ius cogens* absolute prohibition on torture (Alegre, *op. cit.*, p. 33).

159 Regarding the death penalty, it needs to be taken into account that there is a danger, in providing evidence to third countries, that that evidence may be used in proceedings against a person who is at a risk of the death penalty (Alegre, *op. cit.*, p. 35).

160 *Saadi v Italy*, Application no. 37201/06, Judgment of 28 February 2008.

161 Alegre, *op. cit.*, p. 36.

162 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*, Report, June. The report is complemented by a report focusing on justice: High Level Advisory Group on the Future of European Justice Policy (2008), *Proposed Solutions for the Future EU Justice Programme,* June.

163 'The Future Group', *op. cit.*, p. 3.

164 United Kingdom Delegation (2007), *Mobility, Security and Privacy,* Contribution to the Fourth meeting of the High Level Advisory Group on the future of EU Home Affairs Policies, December, p. 1.

165 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,* Report, June, p. 17.

166 Or "*ensuring the best possible flow of data"* ('The Future Group', *op. cit.*, p. 3); Bunyan, Tony (2008), *The Shape of Things to Come: EU Future report*, Statewatch, September, p. 41.

167 On security technologies in Europe, see also D.1.1. Deliverable of the INEX programme: 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 Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November.

168 Faull, Jonathan and Luigi Soreca (2008), "EU-US Relations in Justice and Home Affairs", in Martenczuk, Bernd and Servaas Van Thiel (eds.) (2008), *Justice, Liberty, Security: New challenges for EU external relations,* VUB Press, Brussels, p. 399.

169 Dalferth, Simon (2004), *Enlarging the Area of Freedom, Security and Justice: Europeanisation, Policy Transfer and the Police*, September, Charles University, Praha, p. 14.

170 Notably by broadening the range of crimes justifying interceptions, relaxing the requirements for surveillance, authorising especially invasive techniques such as 'Trojan horses', or multiplying the cases in which telecommunication

law a design of telecommunications equipment that facilitates the interception of communications.[172] The technology-privacy nexus has been explored widely in the literature.[173] It has significantly been argued that the vision of a zero-sum relation between security and privacy is generally played out precisely along the axis of technology.[174] European institutions have widely tended to encourage the use of technology for security purposes in different domains, even if they have defended with less vigour the use of technology for the promotion of privacy. Despite its formal support to the notion of Privacy Enhancing Technologies (PETs), the European Commission has until now actively promoted their use only through soft-law measures, such an ad-hoc Communication.[175] Background documents used in the preparation of the already mentioned 'The Future Group' report on the future of EU Justice and Home Affairs stress, however, that actually supporting PETs can be problematic, in the understanding that PETs might be used by individuals carrying out illegal activities on the Internet to prevent their identity being discovered.[176]

37. The judiciary has already reacted at national level to some innovative uses of technology for security purposes. An especially worth-noting judgement was provided by the German Constitutional Court in February 2008, examining the constitutionality of secret online searches of computers by government agencies.[177] The case derived from a constitutional complaint against a statute allowing the search of information technology systems, questioning the legitimacy of secret monitoring of personal computers. The German Constitutional Court acknowledged the existence of a gap in the legal protection of the confidentiality and integrity of personal information technology systems,[178] and recognised a 'basic right to the confidentiality and integrity of information systems' as part of the general personality rights constitutionally protected in Germany.[179] In the judgement's reasoning, the Court notably took into account the increasing importance of information technology for the development of personality.

Biometrics (and Databases)

38. The origin of biometric identification in the EU is linked to the 1985 Schengen Agreement of 1985.[180] Another key moment of the history of the European support for biometrics was the adoption of the Biometric Passports Regulation,[181] which, in combination with two follow-up EC decisions, called for the compulsory biometric enrolment of all EU citizens applying for passports by August 2006 (for

providers have to identify users. In Sweden, a law authorises the National Defence Radio Establishment (Försvarets Radioanstalt – FRA) to monitor without a court order all telecommunications that cross the borders of the country (Banisar, *op. cit.*, p. 31).

171 Council Resolution of 17 January 1995 on the lawful interception of telecommunications, OJ C 329, 4.11.1996, pp. 1–6.

172 Banisar, *op. cit.*, p. 33.

173 See, notably: Koops, Bert-Jaap and Ronald Leenes (2005), "'Code' and the Slow Erosion of Privacy", *Michigan Telecommunications and Technology Law Review,* 12, pp. 115-159. Arguing that technology tends to be developed adapting to an American (as opposed to European) notion of privacy: Mattelart, Armand (2008), *La globalisation de la surveillance : Aux origines de l'ordre sécuritaire*, Editions La Découverte, Paris, p. 226. Some have distinguished 'public protective technologies', allegedly enhancing security, from 'liberalizing technologies', apparently expanding individual liberties (Etzioni, Amitai (2004), *The Common Good*, Polity Press, Malden, p. 97).

174 Burgess, Peter J. (2008), *Security After Privacy: The Transformation of Personal Data in the Age of Terror*, Policy Brief, PRIO, 5/2008, p. 1.

175 EC (2007), *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. See also: Bygrave, Lee A. (2002), "Privacy-Enhancing Technologies: Caught between a Rock and a Hard Place", *Privacy Law & Policy Reporter,* 9, pp. 135-137. Through EC funding, researchers have also tried to provide criteria useful for 'security technologies' to comply with, and possibly enhance, privacy and data protection (Raguse, Maren, Martin Meints, Owe Langfeldt and Walter Peissl (2008), *Criteria for privacy enhancing security technologies*, Privacy and Security (PRISE)).

176 United Kingdom Delegation, *op. cit.*, p. 2.

177 Published on 27 Feb 2008 (Online-Durchsuchung, 1 BvR 370/07; 1 BvR 595/07).

178 Thus, considered to be not satisfactorily protected by the existing German provisions ensuring the right to informational self-determination and the protection against the interception of post and telephone calls and recording conversations.

179 The Court limited exceptions to the new right to specific cases where factual indications for a concrete danger exist for the life, body and freedom of persons or for the foundations of the state or the existence of human beings, and declared that measures could only be implemented after approval by a judge.

180 Liberatore, Angela (2005), *Balancing Security and Democracy: The Politics of Biometric Identification in the European Union*, European University Institute Working Papers, RSCAS No. 2005/30, p. 5.

181 Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ, L 385, 29.12.2004, pp. 1-6.

facial images) and June 2009 (for fingerprints).[182] Another crucial element was the deployment of Eurodac,[183] the fingerprint database for identifying asylum seekers, which has developed into a truly pan-European biometric identification regime.[184] Additionally, in 2004 was approved the creation of the Visa Information System (VIS),[185] to hold biometric data (facial photograph and 10-digit fingerprints) to identify persons who have lodged a visa application for a EU Member State.

39. There is no international legal instrument explicitly dealing with the regulation of biometrical data.[186] Protection for the individual is to be found primordially in the general framework for privacy and data protection. From a practical perspective, many questions remain open concerning the implementation of data protection law in the field of biometrics. Different national data protection authorities responsible for ensuring monitoring of compliance with data protection obligations in the EU have taken to contradictory decisions for similar biometric systems,[187] and crucial uncertainties remain regarding the purposes and the criteria that make biometric data processing lawful and legitimate.[188] Conceptually, data protection law appears to confirm in its relation to biometrics its processor-friendly, enabling logic.[189] The legislative development of the right to privacy fundamentally through the protection of personal data has been described as not contributing to an effective protection of individuals in the light of the widespread use of biometrics. This argument is based on the idea that the European regime neglects the importance of the notion of bodily integrity,[190] only taken into consideration during the phase of collection of data, but disregarded during further processing, and thus creating a situation in which two different levels of protection are granted: bodily integrity applies exclusively to protect 'the body itself', whereas 'informational privacy' (or data protection) applies to its digital representations.[191]

40. A recent judgement of the ECtHR could be crucial for future developments in this field. The judgement for the *S. and Marper*[192] case concerns 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.[193] Both had asked for their fingerprints and DNA samples to be destroyed by the police, but the police had refused.[194] The judgement reviews different national approaches in Europe to the taking and retention of DNA information in the context of criminal proceedings, and notes that the UK is the only Council of Europe Member State 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.[195] After establishing that the retention of both cellular samples and DNA profiles discloses an interference with the applicants' right to respect for private lives within the

---

[182] Aus, Jonathan P. (2006), *Decision-making under Pressure: The Negotiation of the Biometric Passports Regulation in the Council*, ARENA Working Paper, No. 11, Centre for European Studies, University of Oslo, September, p. 2.
[183] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316 of 15 December 2000, pp. 1-10; Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 62 of 5 March 2002, pp. 1-5.
[184] Aus, Jonathan P. (2006), *Eurodac: A Solution Looking for a Problem?,* European Integration online Papers (EIoP), Volume 10, N° 6, 21 July, p. 11; see also: AUS, Jonathan P. (2003), *Supranational Governance in an 'Area of Freedom, Security and Justice': Eurodac and the Politics of Biometric Control*, Sussex European Institute Working Paper No. 72.
[185] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.06.2004, pp. 5-7.
[186] Note, however, that general standards of the identification on the basis of biometrical data have been laid down by the International Civil Aviation Organisation (ICAO) (Zeller, Judit, Nóra Chronowski, Tímea Drinóczi and Miklós Kocis (2007), "Biometrics: Identification, Verification or Disintegration of Personal Identity?", *Central European Political Science Review*, 8(30), p. 92. See also: Stanton, Jeffrey M. (2008), "ICAO and the biometric RFID passport", in Bennett, Colin J. and David Lyon (eds.) (2008), *Playing the identity card: surveillance, security and identification in global perspective*, Routledge, New York.
[187] Kindt, Els (2007), "Biometric application and the data protection legislation: The legal overview and the proportionality test", *Datenschutz und Datensicherheit*, 31, p. 169.
[188] *Ibidem*, p. 166.
[189] De Hert, Paul (2005), *Biometrics: legal issues and implications*, Background paper, Institute of Prospective Technological Studies, Sevilla.
[190] Van Der Ploeg, Irma (2003), "Biometrics and the body as information: Normative issues of the socio-technical coding of the body" in Lyon, David (ed.) (2003), Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, Routledge, New York, p. 66.
[191] *Ibidem*, p. 67.
[192] *S. and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgement of 4 December 2008.
[193] *Ibidem*, § 3.
[194] *Ibidem*, § 12.
[195] *Ibidem*, § 47.

meaning of Article 8 ECHR,[196] and that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may also in itself give rise to important private-life concerns,[197] the ECtHR went on to declare that the core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection, and impose as well limited periods of storage.[198] Consequently, the ECtHR 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 as necessary in a democratic society,[199] amounting therefore to a violation of Article 8 ECHR.

Borders (and Databases)[200]

41. As seen, different EU-wide databases have been emerging fundamentally in relation with (external) border-related and mobility issues (i.e., the SIS, the CIS, the VIS, Eurodac),[201] raising many different questions related to the effective protection of individuals.[202] If the external borders of the EU can be imagined to be the borders of EU Member States with non-EU Member States, this is however not always fully accurate legally speaking.[203] The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU (Frontex)[204] is indeed concerned with such borders of EU Member States.[205] Nevertheless, UK, Ireland and Denmark enjoy certain 'opt-outs' in a series of areas of EU law, while Norway and Iceland are very closely associated with certain parts of EU Justice and Home Affairs.[206] Borders, in any case, do not systematically mark the boundaries of legal responsibility for states.[207]

42. Since 2002, the EU has endorsed a concept of 'integrated border management' believed to imply a logic focusing on security and risk, rather than transparency and individual rights.[208] In the context of Schengen, the 'border management' notion is defined as including 'border checks', to be performed at authorised crossing points, and 'border surveillance', which is carried out between such

---

196 *Ibidem*, § 77.
197 *Ibidem*, § 86.
198 *Ibidem*, § 107.
199 *Ibidem*, § 125.
200 On the management of EU borders and security technologies, see also D.1.1. Deliverable of the INEX programme, already mentioned.
201 For different accounts of their evolution, see: Broeders, Dennis (2007), "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants", *International Sociology,* 22(1), pp. 71-92; Busch, Heiner (2006), *The dream of total data collection – status quo and future plans for EU information systems*, Statewatch Bulletin Vol. 16, No. 5/6. On biometrics and security, see also: Skokowski, Paul (2002). *Can Biometrics Defeat Terror?,* paper presented at the National Security Forum, March.
202 See, notably: Brouwer, Evelien (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers, Leiden. See also: Quilleré-Majzoub, Fabienne (2005), "Les individus face aux systèmes d'information de l'Union Européenne: l'impossible équation du contrôle juridictionnel et de la protection des données personnelles au niveau européen?", *Journal du droit International,* 132(3), pp. 609-635. Calling for further developments to take more carefully into account the vulnerable position of non-citizens, both in relation to the application for travel documents and admission at the real/virtual order: Redpath, Jillyanne (2005), *Biometrics and International Migration*, International Migration Law, No. 5, International Organization for Migration (IOM), p. 16.
203 Tekofsky, Aliza (2006), *Security in European Union External Border Law*, CHALLENGE Working Paper, February 27, p. 2.
204 Council Regulation (EC) No 2007//2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25.11.2004, pp. 1-11. See also: Jeandesboz, Julien (2008), *An Analysis of the Commission Communications on Future Development of FRONTEX and the Creation of a European Border Surveillance System (EUROSUR),* Briefing Paper for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, June.
205 European Union Committee, House Of Lords (2008), *FRONTEX: The EU external borders agency,* Report with evidence, 9th Report of Session 2007-08, 5 March, London: The Stationery Office Limited, p. 12.
206 Peers, *op. cit.*, p. 2.
207 The ECtHR has notably developed principles indicating that the borders of the state are not the borders of responsibility for state agents as regards human rights (Guild, Elspeth (2007), *Security and European Human Rights: protecting individual rights in times of exception and military action*, Wolf Legal Publishers, Nijmegen, p. 58). States are in particular obliged to respect and ensure the rights and freedoms of persons within their power or effective control, even if not acting within their territory (Conte, Alex (2008), *Handbook on Human Rights Compliance While Countering Terrorism*, Center on Global Counterterrorism Cooperation, January, p. 7).
208 Garlick, Madeline and Judith Kumin (2008), "Seeking Asylum in the EU: Disentangling Refugee Protection from Migration Control", in Martenczuk, Bernd and Servaas Van Thiel (eds.) (2008), *Justice, Liberty, Security: New challenges for EU external relations,* VUB Press, Brussels, p. 127.

authorised crossing points,[209] and is mainly based on risk-analysis.[210] It has been asserted that the efforts to strengthen external border controls in the EU justify a shift in terminology from 'border control' to 'border security',[211] especially since in 2004 the Council expressly linked the monitoring of people's movement with counterterrorism.[212] Border-related security initiatives have been described as an intensification of surveillance in a manner apparently at odds with the concept of the EU as a borderless area, leading to the paradoxical situation of an area without frontiers but with more controls,[213] in which the abolition of (internal) borders seems to prompt the emergence of new forms of control.[214] Some view the displacement of borders from traditional borders to 'sanitarian' and security controls in terms of a new 'ubiquity' of borders,[215] while biometrics are pointed out as allowing the body to becomes the ultimate carrier of borders.[216] In any case, in the EU there is currently only a fragmentary coverage of border movements.[217]

43. Since the 1980s, certain immigration policies appear to have been conceived with the aim of favouring the prevention of the arrival of irregular migrants or asylum seekers to borders,[218] an approach linked to a will to reduce state obligations related to ensuring international protection for those who might need it.[219] Some especially have lamented a EU tendency towards the externalisation of migrant control in third countries.[220] The Hague Programme famously called for the development of partnerships with countries in transit and source areas of migrant and refugees, in an approach described as an attempt to establish a series of concentric circles in which states outside the EU play an ever-increasing role in assisting the application of the EU migration management priorities.[221] In order to describe this trend has been used the notion of 'policing at distance' or 'ban-opticon',[222] which among other things aims at stressing that understanding the 'devices' implemented in the field requires a consideration of both the legal principles which allow for their implementation and the technological instruments used.[223]

---

[209] Hills, Alice (2003), *Towards a rationality of democratic border managemen*t, Geneva Centre for the Democratic Control of Armed Forces (DCAF), March, p. 3.

[210] Council of the European Union, General Secretariat (2002), *EU Schengen Catalogue, External borders control, removal and readmission: Recommendations and best practices*, February, p. 14.

[211] Mitsilegas, Valsamis (2007), "Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance" in Baldaccini, Anneliese, Elspeth Guild and Helen Toner (2007), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, Oxford, p. 359.

[212] Referring notably to the use of biometrics in EU visas and passports and the enhancement of interoperability and synergies between EU databases and information systems (Mitsilegas, *op. cit.,* p. 386).

[213] Mitsilegas, *op. cit.*, p. 393.

[214] Faure Atger, Anaïs (2008), *The Abolition of Internal Border Checks in an Enlarged Schengen Area: Freedom of movement or a web of scattered security checks?* , Research Paper No. 8, CHALLENGE, Brussels, p. 18.

[215] Balibar, Etienne (2007) « Qu'est-ce qu'une « frontière » ?», in Caloz-Tschopp, Marie Claire and Pierre Dasen (2007), *Globalization, migration and human rights: a new paradigm for research and citizenship*, Volume I, Bruylant, Bruxelles, p. 529.

[216] Amoore, Louise (2006), "Biometrics borders: Governing mobilities in the war on terror", *Political Geography,* 25, p. 348. Also in this sense: Epstein, Charlotte (2007), "Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders", *International Political Sociology,* I, pp. 149-164.

[217] Even if large-scale information systems like SIS II and VIS are to share a common technical platform, there is so far no interoperability between any of these systems (Hobbing, Peter (2008), *Tracing Terrorists: The EU-Canada Agreement in PNR matters*, CEPS Special Report, Centre For European Policy Studies (CEPS), Brussels, September, p. 19).

[218] Crepeau, François, Delphine Nakache and Idil Atak (2007), "International Migration: Security Concerns and Human Rights Standards", *Transcultural Psychiatry*, 44, p. 323.

[219] *Ibidem*, p. 325. The importance granted to the external dimension of immigration and asylum policies in the EU efforts in the field of Freedom, Security and Justice has actually been pointed out as the culmination of policies placing emphasis on border control and management at the expense of refugee protection needs (Baldaccini, Anneliese (2007), "The External Dimension of the EU's Asylum and Immigration Policies: Old Concerns and New Approaches" in Baldaccini, Anneliese, Elspeth Guild and Helen Toner (2007), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, Oxford, p. 278).

[220] Glasson-Deschaumes, Ghislaine (2007) « La régularité d'une présence invisible ou le silence culturel et politique des immigrés en situation régulière», in Caloz-Tschopp, Marie Claire and Pierre Dasen (2007), Globalization, migration and human rights: a new paradigm for research and citizenship, Volume I, Bruylant, Bruxelles, pp. 259-284.

[221] Baldaccini, *op. cit.*, p. 297.

[222] In particular in reference to the Schengen visa (Guild, Elspeth and Didier Bigo (2003), « Schengen et la politique des visas », *Culture et Conflits,* n° 49, 1/2003, pp. 5-21), said to allow for a division of the control of the EU external border into two parts: a territorial border and a virtual border (Guild, Elspeth (2007), "Citizens Without a Constitution, Borders Without a State: EU Free Movement of Persons" in Baldaccini, Anneliese, Elspeth Guild and Helen Toner (2007), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing: Oxford, p. 41).

[223] Guild, Elspeth and Didier Bigo (2003), « Le visa Schengen : expression d'une stratégie de « police » à distance », *Culture et Conflits,* n° 49, 1/2003, pp. 22-37.

44. In 2008, the European Commission presented its vision of future border control systems.[224] Under the motto 'the next steps in border management', it proposed an 'integrated' system based on (a) the registration, in an entry-exit database, of all third country nationals entering EU territory; (b) the granting of a registered traveller status to 'low risk travellers' from third countries after appropriate pre-screening, and (c) an Automated Border Control System to manage entry/exit of both third country nationals with registered traveller status and EU citizens.[225] A clear sign in terms of keeping non-approved foreigners at distance has been seen in the Electronic Travel Authorisation (ETA)[226] concept, now also endorsed by the European Commission. The approach has been practised for years in Australia, and is now being considered on both sides of the Atlantic.[227] The most controversial element of the E(S)TA is that even citizens of visa-free countries could be subjected to some advance-control.[228]

Information Sharing

45. 'Information sharing' as a principle was especially praised in the US right after 9/11, when a number of actors emphasised the need for the active promotion of greater information transfers,[229] potentially leading to a shift from a 'need to know' culture in the access to information from a 'need to share' culture.[230] Discussions on integrating the information sharing principle in the EU started also after 9/11, in particular in relation with the fight against terrorism,[231] even if they eventually expanded to the fight against crime in general.[232] Different concrete EU level measures have supported information sharing practices. A 2005 Communication from the European Commission on the interoperability and synergies among European databases in the area of Justice and Home Affairs,[233] which presented among other things a series of ideas on how to use EU-wide databases for combating terrorism and serious crime even if they were originally unrelated to such purposes, met strong opposition. Eventually, the support to any direct interlinking of EU large-scale IT-systems was abandoned, even if other, subtler approaches to information sharing were developed.[234] The Council

---

[224] EC (2008), *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, 13.2.2008, Brussels. On this Communication, see also: Peers, Steve (2008), *Proposed New EU Border Control Systems*, Briefing Paper, Civil Liberties, Justice and Home Affairs Committee of the European Parliament, June; Guild, Elspeth, Sergio Carrera and Florian Geyer (2008), *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?* , CEPS Policy Brief No. 154, CEPS, Brussels, March.

[225] Hobbing (2008), *op. cit.*, p. 20.

[226] In the EU it has been baptised Electronic System Travel Authorisation (ESTA) to avoid confusion with Euskadi Ta Askatasuna (ETA).

[227] Hobbing (2008), *op. cit.*, p. 21.

[228] *Idem*.

[229] Following what has been described as the logic of an 'information sharing paradigm' based on three premises: the existence of a new threat; the idea that such 'new' threat was significant, and the argument according to which progress in information technology offers the most effective response to the significant 'new' threat (Swire, Peter P. (2006), "Privacy and Information Sharing in the War on Terrorism", *Villanova Law Review*, 51, p. 102).

[230] National Commission on Terrorist Attacks upon the United States (2004), *The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States*, New York, Norton, p. 417; see also: Borys, W.J. (2006) *"Need To Know" To "Need To Share": How Terrorism Is Changing The Intelligence Community's Culture,* Canadian Forces College, p. 6.

[231] A series of EU policy documents have linked to counterterrorist efforts to the need to improve information sharing via common approaches (for instance: Council of the European Union (2005), *The European Union Counter-Terrorism Strategy*, 30 November, p. 13).

[232] Bunyan, Tony (2006), *The "principle of availability"*, Statewatch, December, p. 2.

[233] EC (2005), *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. On this Communication, see: De Hert, Paul and Serge Gutwirth (2006), "Interoperability of Police Databases within the EU: An Accountable Political Choice?", *International Review of Law, Computers & Technology,* 20(1&2), pp. 21-35.

[234] As an illustration of subsequent formalised procedures can be mentioned the procedure for access to VIS by designated Member State authorities and Europol, established by: Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.08.2008, pp. 129-136. See, on this issue: Hobbing, Peter (2006), *A comparison of the now agreed VIS package and the US-VISIT system,* Briefing Paper, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament.

Framework Decision of 18 December 2006 widely encourages exchanges of information and intelligence, in particular related to organised crime and terrorism.[235]

46. In the field of EU police and judicial cooperation, a major step was the creation of the 'principle of availability'. The European Commission adopted in 2005 a proposal on the exchange of information under such principle.[236] The adoption of the proposal was eventually left aside by the Council, while a series of Member States agreed on other information sharing commitments under the Prüm Treaty.[237] In 2007 was reached a political agreement on a Decision transposing most of the Third Pillar part of the Prüm Treaty (including provisions on fingerprints, DNA and vehicle registration data) into the EU institutional framework, and the European Commission has stated that once the text is adopted it can be considered as a partial implementation of the 'principle of availability'.[238] 'The Future Group' report on the upcoming programme for EU Justice and Home Affairs discusses a 'convergence principle', which is to follow on, in a sense, from the 'principle of availability' and the 'interoperability' of EU information systems;[239] it also recommends implementing a EU Information Management Strategy (EU IMS) "*promoting a coherent approach to the development of information technology and exchange of information*".[240]

47. The ECJ recently delivered a judgement on the use for crime fighting purposes of databases containing personal information that could be considered of the highest importance for upcoming developments in this field, in relation with the case *Heinz Huber v. Germany*.[241] The case concerned a reference for a preliminary ruling from the Higher Administrative Court of North-Rhine Westphalia (Germany) asking the ECJ whether the general processing of personal data of foreign citizens of the EU in a central register is compatible with the prohibition of discrimination of nationality against EU citizens who exercise their right to move and reside freely within the territory of the Member States, with the prohibition of restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State, and with the requirement of necessity under Article 7(e) of the Data Protection Directive. Advocate General Maduro had already considered in his Opinion for the case that large-scale national databases containing only extensive data on EU citizens (and third country nationals), but not on its own nationals, as discriminatory and in breach of community law,[242] explaining that at the core of the case there was a question of discrimination.[243] Similarly, the ECJ declared that the difference in treatment between those nationals and those EU citizens arising by virtue of the systematic processing of personal data relating to EU citizens who are not nationals of the Member State concerned for the purposes of fighting crime constitutes a discrimination prohibited by

---

[235] 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.

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

[237] On the data protection aspects of the Prüm Treaty, see: Aced Félez, Emilio (2007), "Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm", *Revista de Derecho constitucional europeo,* Enero-Junio, n° 7, pp. 65-96; Cámara Villar, Gregorio (2007), "La garantía de los derechos fundamentales afectados por la Convención de Prüm", *Revista de Derecho constitucional europeo,* Enero-Junio(7), pp. 97-118.. For a critical consideration of its implications for EU decision-making: Balzacq, Thierry, Didier Bigo, Sergio Carrera and Elspeth Guild (2006), *Security and the Two-Level Game: the Treaty of Prüm, the EU and the Management of Threats*, CEPS Working Document, No. 234, CEPS, Brussels, January; Bellanova, Rocco (2008), "The "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange?", in Guild, Elspeth and Florian Geyer (eds.), (2008), *Security versus Justice?: Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, pp. 203-221.

[238] EC (2008), *Communication from the Commission to the Council and the European Parliament: Report on Implementation of the Hague Programme for 2007,* COM(2008) 373 final, 2.7.2008, Brussels, p. 7. Also in this sense: Aced Félez, Emilio (2007), "Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm", *Revista de Derecho constitucional europeo,* Enero-Junio, n° 7, p. 65.

[239] Bunyan, Tony (2008), *The Shape of Things to Come: EU Future report*, Statewatch, September, p. 37.

[240] 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,* Report, June, p. 9.

[241] *Heinz Huber v. Germany,* Case C-524/06, Judgement of 16 December 2008.

[242] Poiares Maduro (2008), *Opinion of Advocate General Poiares Maduro in Case C-524/06 (Heinz Huber v Bundesrepublik Deutschland)*, delivered on 3 April 2008.

[243] *Ibidem*, § 4. Observing that the existence of two separate data processing systems casts an 'unpleasant shadow' over EU citizens, whom the German Government monitors much more strictly and systematically than German citizens (*ibidem,* § 5), the Advocate General recalled that the combating of crime and threats to security could not justify the difference in treatment between Germans and citizens of other Member States. Indeed, even if law-enforcement and the combating of crime could, in principle, be a legitimate public policy reason qualifying rights granted by Community law, Member States cannot invoke it selectively (*ibidem*, § 21). Additionally, Maduro considered that granting access to a system as the one at issue in the proceedings to public authorities other than immigration authorities is incompatible with Article 8 ECHR and, therefore also with the requirements of necessity under Article 7(e) of the Data Protection Directive (*ibidem*, § 27, § 32).

Community law, which must be interpreted as meaning that it precludes the putting in place by a Member State, for the purposes of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State.[244]

48. The Hague Programme stressed the idea that strengthening the Area of Freedom, Security and Justice 'requires' innovative approaches not only to internal EU information sharing, but also to the cross-border exchange of law-enforcement information.[245] Currently, different EU-level mechanisms allow for the sharing of information with third countries.[246] Agreements between Europol and Eurojust and third countries are an example of such mechanisms. Europol[247] currently has agreements with Canada, Croatia, Iceland, Norway, Switzerland and the US.[248] Similarly, the Eurojust decision allows Eurojust to exchange information with international organisations and bodies and third states, and to conclude cooperation agreements with third states and international organisations and bodies, which may contain provisions concerning the exchange of personal data.[249] In 2006, Eurojust and the US Department of Justice signed an agreement aiming to facilitate co-operation, co-ordination and the exchange of information between EU and US prosecutors on terrorism and cross-border criminal cases. The Frontex Regulation allows Frontex to cooperate with Europol and other international organisations.[250]

EU-US Cooperation

49. Already in a Joint EU-US Statement of 20 September 2001 on combating terrorism it was announced that agreement had been reached for the EU and US to work together to reinforce their cooperation in the fields of aviation and other transport security; police and judicial cooperation,[251] including extradition;[252] denial of financing terrorism, including financial sanctions; export control and non-proliferation; border controls, including visa and document security issues; and law enforcement access to information and exchange of data. International security cooperation can however encounter different problems when the different parties involved do not share the same fundamental rights standards.[253] Transferring personal data to the US for law enforcement purposes is currently one of the most problematic issues in the EU-US relationship,[254] as the US is not considered by the EU to provide

---

[244] See § 80 and § 81 of the *Huber* judgement, already mentioned.

[245] EC (2008), *Communication from the Commission to the Council and the European Parliament: Report on Implementation of the Hague Programme for 2007,* COM(2008) 373 final, 2.7.2008, Brussels, p. 7.

[246] Contributing towards a perception of data as constantly *"fly*(ing) *around"* (Grammatikas, Vassilios (2006). *EU Counter-terrorist Policies: Security vs. Human Rights?,* HUMSEC Working Paper, p. 15).

[247] See: Council Act of 12 March 1999 on the rules governing the transmission of personal data by Europol to third states and third bodies, OJ C 88, 30.03.1999; Council Act of 28 February 2002 amending the Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third states and third bodies, OJ C 76, 27.03.2002, pp. 1-2. Concerning Europol, as a general principle there can be no transmission of personal data without previous negotiation of an agreement, except in the cases in which the transmission of data is absolutely necessary to safeguard the essential interests of the Member States, or to prevent an imminent danger associated with crime. The Director of Europol is obliged to inform both the Management Board and the Joint Supervisory Body of Europol when he has decided to use his authorities to transmit data without an agreement, a possibility used at least once (Heimans, Dick (2008), "The External Relations of Europol – Political, Legal, and Operational Considerations", in Martenczuk, Bernd and Servaas Van Thiel (eds.) (2008), *Justice, Liberty, Security: New challenges for EU external relations,* VUB Press, Brussels, p. 378).

[248] Alegre, *op. cit.*, p. 23. Two arrangements have actually been signed between Europol and the US: one, in December 2001, aims at enhance cooperation between EU Member States and the US in preventing, detecting and investigating terrorism and organised crime; the second, in December 2002, allows for the sharing of personal data.

[249] In that case, the Eurojust Joint Supervisory Body shall be consulted. The transmission of data to third states and bodies not subject to Convention 108 may be effected only when an 'adequate' level of data protection is acquired, except in certain 'emergency' cases (Mitsilegas, Valsamis, Jörg Monar and Wyn Rees (2003), *The European Union and Internal Security: Guardian of the People?*, Palgrave: Hampshire, p. 124).

[250] See Art. 13.

[251] See, in particular: Agreement on mutual legal assistance between the European Union and the United States of America, 25 June 2003. The agreement contains provisions on data protection. The negotiations leading to this agreement, as well as to the agreement on extradition, and mutual legal assistance, caused controversy notably relating to the legal personality of the EU under current treaties (Alegre, *op. cit.*, p. 5).

[252] Agreement on extradition between the European Union and the United States of America (OJ L 181, 19.7.2003, p. 27).

[253] EU Network of Independent Experts in Fundamental Rights (2003), *The balance between freedom and security in the response by the European Union and its Member States to the terrorist threats*, Thematic Comment, p. 8.

[254] Faull and Soreca, *op. cit.*, p. 415. On this issue, see also: Heisenberg, Dorothee (2005), *Negotiating Privacy: the European Union, the United States and Personal Data Protection*, Lynne Rienner Publishers, London. Another field in which the different standards of fundamental rights protection tend to create problems in the context of the reinforcement of US-EU cooperation is judicial cooperation (EU Network of Independent Experts in Fundamental Rights, *op. cit.,* p. 19).

an 'adequate level' of protection for personal data, which would allow for 'normal' transfers of data.[255] Cases such as the 'SWIFT affair'[256], on the access by US authorities to the records of the Belgium-based global financial cooperative, have illustrated these frictions.

50. To find 'solutions' in the context of data protection for transatlantic data transfers, in 2006 was established a EU-US High Level Contact Group on information sharing and privacy and personal data protection, discussing data sharing and data protection for law enforcement purposes,[257] and charged with working towards a joint text laying down common data protection principles. The research for common approaches has been particularly supported by those considering of main relevance for transatlantic cooperation the identification of "*an appropriate fulcrum that allows us to continue to balance security and liberty*".[258] In June 2008, the EU-US High Level Contact Group presented its final report,[259] which tends to identify common principles for privacy and data protection as a step towards exchange of information with the US to fight terrorism and serious transnational crime. The search for data protection bilateral solutions is to be put in the context of tensions between bilateral and multilateral approaches to transatlantic relations.[260]

Counterterrorism And Pro-Activity

51. Many international and European counterterrorism initiatives have been analysed in the literature as marking a shift towards forward-looking strategies. Sometimes described in terms of 'prevention', 'pro-activity'[261], 'anticipation',[262] 'radical prevention' or 'pre-emption',[263] the initiatives in question can actually consist of very different realities.

---

[255] The reasons for which personal data in US territory are not considered to enjoy adequate protection are many, and include for instance the USA Patriot Act provisions allowing American authorities to order organisations to turn over records and 'other tangible things' in their possession, while prohibiting the organisation from communicating that it has been asked to release the data (Stefanick, Lorna (2007), "Outsourcing and transborder data flows: the challenge of protecting personal information under the shadow of the USA Patriot Act", *International Review of Administrative Sciences,* 73, p. 538). On this Act, see also: Petrosino, Anthony (2005), *The United States and Counterterrorism: History, Measures, and Lessons*, Report to the Research and Documentation Centre, Netherlands Ministry of Justice, 17 November, p. 22. Additionally, US strong support of internal information sharing transforms any transfer of data to the US into an opening of unclear possibilities; in this sense, since the 'interim Agreement' signed by the Council and DHS on 6 October 2006, the EU explicitly committed to ensuring that PNR data are processed as required by DHS "*in reliance upon DHS's continued implementation of the Undertakings as interpreted in the light of subsequent events*", an interpretation clarified in an explanatory letter of DHS to the Commission and the Council referring to the enhancement of the amount and use of PNR data transferred in the framework of the US Information Strategy Environment data sharing strategy, meaning that DHS is to disseminate the data to other governmental agencies (Ntouvas, Ioannis (2007), "Air Passenger Data Transfer to the USA: the Decision of the ECJ and the latest developments", *International Journal of Law and Information Technology,* 16(1), p. 86

[256] The revelations on the subject eventually led to an exchange of letters between EU and US officials to establish a series of data protection guarantees. On the SWIFT affair, see: González Fuster, Gloria, Paul De Hert and Serge Gutwirth (2008), "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.

[257] Faull and Soreca, *op. cit.*, p. 416.

[258] Aldrich, Richard J. (2004), "Transatlantic intelligence and security cooperation", *International Affairs*, 80(3), p. 736.

[259] Council of the European Union (2008), Note from the Presidency to COREPER on EU US Summit, 12 June 2008 – Final Report by EU-US High Level Contact on information sharing and privacy and personal data protection, 28 May, Brussels. See also: EDPS (2008), *Opinion of the EDPS on the Final Repory by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, Brussels, 11 November.

[260] In 2008, US authorities reinforced the pressure on EU Member States not yet part of the visa-free arrangements with the US for providing them with concessions not covered by the EU-US PNR agreement, in exchange of prospects of becoming part of the Visa Waiver Program (VWP). This involved allowing armed sky marshals on board of US-bound flights, provision of PNR data beyond the 2007 requirements and accepting the ETA system (Hobbing, *op. cit.*, p. 46). Although this conflicted with EU policy interests in both visa and PNR matters, the Czech Republic eventually signed a Memorandum of Understanding on 26 February, and others followed rapidly (Estonia, Latvia, Lithuania, Hungary, Malta, Slovakia) (*idem).* The European Commission decided to allow agreements on 'minor issues' while remaining in charge of discussion on the ETA system (*ibidem,* p. 47).

[261] See, notably: Levi, Michael and David S. Wall (2004), "Technologies, Security and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Volume 31, Number 2, June, pp. 194-220.

[262] Bigo, Didier, Sergio Carrera, Elspeth Guild and R.B.J. Walker (2007), *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project,* Research Paper No. 4, CEPS, Brussels, February, p. 9.

[263] Zedner, Lucia (2007), "Seeking Security By Eroding Rights: The Side-stepping of Due Process" in Goold, Benjamin J., and Lazarus, Liora (eds.) (2007), *Security and human rights*, Oxford, Portland, Hart, p. 260. The shift of counterterrorism towards forward-looking strategies is certainly not completely unrelated to the so-called 'Bush Doctrine' for fighting terrorism, based on a will to act pre-emptively before attacks occur, inspired in the doctrine of military pre-emption;

52. Some have considered useful to refer to the 'precautionary principle' for the analysis of EU security initiatives,[264] even if whether this principle can or should be applied at all to security practices is highly contentious.[265] The 'precautionary principle' as a legal principle was first developed in the field of environmental law, and the EU law recognises it only in reference to environmental Community policy.[266] The principle posits that where the risk of harm is unpredictable and uncertain, and where the damage that would be brought about that (eventual) harm would be irreversible, any lack of scientific certainty in relation to the nature of the harm or its consequences should not justify inaction.[267] In the literature on data protection, the 'precautionary principle' is sometimes invoked in order to support the idea that technical equipment shall respect certain requirements favouring the implementation of privacy and data protection requirements.[268] No public authority has ever claimed to have embraced the precautionary principle for counterterrorism policy.[269] Nonetheless, some perceive a trend in new counterterrorism laws towards a more 'precautionary' model,[270] in the sense that decision-makers are authorising and taking action where the level of danger is unknown or uncertain.[271]

53. One of the ways in which forward-looking counterterrorism strategies have had an impact in law is through adaptations of the criminal law, notably through the use of 'preventive'[272] definitions of terrorist offences. The 2002 Framework Decision on Combating Terrorism foresaw a broad definition of terrorism,[273] and included measures designed to prevent terrorist acts notably by incriminating 'acts relating to a terrorist group'.[274] The trend to take into account the organised nature that terrorist offences imply by making the membership of terrorist organisations an offence, indicting individuals for their relations with certain groups, regardless of the possible participation by these individuals in the commission of other offences and possibly regardless of any breach having been already committed,[275] can be seen as a manifestation of forward-looking approaches,[276] but there are more. The Council of Europe opened for signature its Convention on the Prevention of Terrorism[277] in May 2005, banning not just incitement but also 'public provocation' when it "*causes a danger*" that a terrorist incident "*may be committed*".[278] If incitement[279] has been long banned in many countries by criminal

---

Indicative of this shift was for instance the 2002 report of the US Department of Justice *Shifting From Prosecution to Prevention, Redesigning the Justice Department to Prevent Future Acts of Terrorism* (Swire, *op. cit.*, p. 104).

[264] Stern, Jessica and Jonathan B. Wiener (2006), "Precaution Against Terrorism", *Journal of Risk Research,* 9(4), pp. 393-447; Preuss-Laussinotte, Sylvia (2006), « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *Cultures & Conflits,* 64, pp. 77-95.

[265] Bronitt, *op. cit.*, p. 79.

[266] Article 174(2) TEC.

[267] Bronitt, *op. cit.*, p. 78.

[268] Poullet, Yves (2002), « Pour une troisième génération de réglementations de protection des données », *Jusletter,* 3, October, p. 12. Others envisage the application of the 'precautionary principle' as a general cautious attitude towards the deployment of certain information and communication technologies (European Group on Ethics in Science and New Technologies (2005), *Ethical aspects of ICT implants in the human body,* 16 March, p. 24).

[269] Bronitt, *op. cit.*, p. 79.

[270] It has also been argued that the term 'precaution' can describe the current way of responding to the terrorist threat within the insurance business (Aradau, Claudia and Rens Van Munster (2007), "Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future", *European Journal of International Relations,* 13, pp. 89-115) and that the current political focus on possible catastrophes has redefined the meaning of business responsibility in terms of precaution (Petersen, Karen Lund (2008), "Risk, responsibility and roles redefined: is counterterrorism a corporate responsibility?", *Cambridge Review of International Affairs,* 21(3), p. 410).

[271] Bronitt, *op. cit.*, p. 80.

[272] For some, 'preemptive' (Human Rights Watch (2008), *Preempting Justice: Counterterrorism Laws and Procedures in France,* July, p. 1).

[273] Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, pp. 3–7.

[274] De Goede, Marieke (2008), "The Politics of Preemption and the War on Terror in Europe", *European Journal of International Relations,* 14, p. 169. For a critical view on the definition, see also: EU Network of Independent Experts in Fundamental Rights, *op. cit.*.

[275] EU Network of Independent Experts in Fundamental Rights, *op. cit.*, p. 7.

[276] The trend is not especially new. Already in 1996, France defined as an offence the "*criminal association in relation to a terrorist undertaking"*, with the aim of preventing terrorism before the commission of any crime (Human Rights Watch, *op. cit.,* p. 1). The measure has been criticized on different grounds, such as the lack of legal precision of the offence; the low standard of proof for decisions to arrest suspects and place them under formal investigation; a presumption in favour of pre-trial detention; the prominent use of intelligence material in judicial investigations and apparent reliance of certain convictions on weak evidence (Human Rights Watch, *op. cit.,* p. 19).

[277] Council of Europe Convention on the Prevention of Terrorism, CETS, No. 196. It entered into force in June 2007. It has been signed by 28 countries, and ratified by 15.

[278] Banisar, *op. cit.*, p. 8.

[279] Typically defined as the direct promotion of criminal acts with the intent of inspiring another person to commit the act (Banisar, *op. cit.*, p. 20).

law, the banning of 'public provocation' is much more controversial.[280] Certain national developments go in similar directions, even if the reliance on wide definitions of offences in counter-terrorism legislation are believed to possibly result in persons engaged in legitimate political or social dissent being branded as terrorists.[281]

54. Another way in which future-centred antiterrorism approaches impact on law is through new approaches to preventive detention. If existing legislation on detention already responds to dangerous individuals through preventive detention,[282] based upon widely accepted rationales,[283] the fight against transnational organised crime and international terrorism have been interpreted as both pointing towards a new category of dangerousness to allow for such type of detention.[284]

55. The 2005 EU Counterterrorism Strategy is based on four dimensions of counter-terrorism: 'prevent', 'protect', 'pursue' and 'respond'. The main aim of the 'prevent' dimension of the EU Strategy is to target the sources of terrorism and the ways in which terrorism spreads through society, an idea which generally corresponds to traditional conceptions of 'prevention' as a structural approach, aimed at tackling the roots of the problem, in opposition to 'repression' strategies. However, a particular element of the 'prevent' dimension of the Strategy is more problematic. It involves the surveillance and the identification of trends that may be indicators of terrorist or 'radicalised' activity, raising significant civil liberties and human rights issues, in particular as monitoring of internet activity and communications engages the right to privacy, and censorship of websites may infringe the right to freedom of expression.[285]

56. The proactive approach to counterterrorism has been particularly influential internationally in relation to profiling and data mining practices. Information technology has indeed been regarded as a privileged tool to 'help find terrorists before they strike'.[286] The literature on profiling does not always deal with profiling as developed in conjunction with data mining. In particular, there is a vast amount of literature, especially from the US, dealing with so-called 'racial' and ethnic profiling, which is actually a different practice, even if both issues can sometimes overlap.[287] There is currently no consensual definition of profiling at EU level,[288] or among scholars.

57. Ethnic profiling is believed to occur when a decision of whom to stop and question proceeds from the individual's ethnicity itself,[289] or when the police relies on formal profiles listing a particular ethnicity as one among many factors that might give rise to reasonable suspicion in certain circumstances.[290] These practices are globally condemned, and generally incompatible with

---

[280] The Council has finally incorporated such an approach into the EU legal framework in December 2008.
[281] Casale, Davide (2008), "EU Institutional and Legal Counter-Terrorism Framework", *Defence Against Terrorism Review,* 1(1), p. 69.
[282] Moeckli, Daniel (2006), *Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection*. paper presented at the Conference of the Association of Human Rights Institutes, September, p. 2.
[283] Such as insanity, chronic or career offending, or the need to respond to an imminent and short-term danger.
[284] Albrecht, Hans-Jörg (2006), *Country Report on Germany,* Max-Planck-Institute for Foreign and International Criminal Law, p. 45.
[285] Alegre, *op. cit.,* p. 20. It shall be noted that in 2007 the EU launched the 'Check the Web' programme to increase the monitoring of Islamist web sites across the EU, co-ordinated by Europol. The relation between crime and electronic communications has notably been tackled by the Council of Europe, notably through its 2001 Convention on Cybercrime (Council of Europe Convention on Cybercrime, Treaty No. 18. It came into force on 7 January 2004. On this Convention, see: De Hert, Paul, Gloria González Fuster and Bert-Jaap Koops (2006), "Fighting Cybercrime in the Two Europes: The Added Value of the EU Framework Decision and the Council of Europe Convention", *International Review of Penal Law,* 77(3-4), pp. 503-524; Keyser, Mike (2003), "The Council of Europe Convention on Cybercrime", *Journal Of Transnational Law And Policy,* 12(2), pp. 287-326). An optional protocol on Xenophobia and Hate Speech was introduced in 2002, prohibiting the dissemination of racist speech including threats and insults and denial and justification of genocide (Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189).
[286] Ham, Shane and Robert D. Atkinson (2002), *Using Technology to Detect and Prevent Terrorism*, Progressive Policy Institute, January, p. 2.
[287] See, in particular: Schreurs, Wim, Mireille Hildebrandt, Els Kindt and Michaël Vanfleteren (2008) "Cogitas, Ergo Sum: The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector", in Hildebrandt, Mireille and Serge Gutwirth (eds.), *Profiling the European Citizen*, Springer, London, pp. 241-270.
[288] Declaration of Ms Verkleij at the House of Lords (European Union Committee of the House of Lords (2008), *The Passenger Name Record (PNR) Framework Decision*, HL Paper 106, London, Evidence: p. 45).
[289] Davies, Sharon L. (2005), *Profiling Terror,* Public Law and Legal Theory Working Paper Series No. 48, Center for Interdisciplinary Law and Policy Studies Working Paper Series No. 31, The Ohio State University, October, p. 58.
[290] *Ibidem*, p. 60.

international law.[291] Ethnic profiling is contrary to a basic principle of the rule of law according to which law enforcement actions respond to an individual's conduct; to cast suspicion on people because of their origin or religion violates the principle of equal treatment.[292] In Europe, recent discussions on ethnic profiling have essentially focused on how to ensure that the prohibition of ethnic profiling as a specific form of discrimination does not remain ineffective in a number of EU Member States,[293] with a particular focus on the possibility that 'overly rigid' understandings (or, actually, misunderstandings) of the requirements of data protection law may result in an obstacle to the effective monitoring of the behaviour of law enforcement activities.[294] It shall be noted that ethnic profiling can be related in general to the activities of law enforcement authorities, but can also take place as a general practice at borders, either through abuse of immigration databases or through specific decisions.[295]

58. Data mining techniques are usually applied in the context of counterterrorism in an attempt to develop predictive models based on known, but also on unknown patterns, in order to identify people, objects, or actions as 'deserving further attention',[296] or to be targeted for 'special treatment'.[297] Current practices have been said to mark a shift from profiles being descriptive, based on an analysis of crimes already committed, to profiles designed for proactive detection of offences as yet unknown to the police, meant to be predictive.[298] Data mining has amongst its structural objectives, first, "*figuring out who the bad guys are*",[299] and, second, classifying people on the basis of the alleged characteristics of the "*the bad guys"*. The use of these techniques at borders facilitates the segregation of 'legitimate' mobility from 'illegitimate' mobility,[300] or, in other terms, the separation of "*people who are ordinary, happy, everyday travellers who are not meeting the profile of people who might be a risk"*[301] from the others, who happen to meet the profile.

59. In the US, the government's reliance on data mining for law enforcement and national security purposes is considered an area of great growth,[302] and has already triggered notable controversy. Internationally, it is well studied that risk management techniques have been incorporated in counter-terrorism policies through various sectors, the most notables being the monitoring of borders and international financial flows.[303] How is predictive data mining relevant in the context of the EU legal framework? On the one hand, predictive data mining can be relevant insofar as personal data are transferred from the EU to US and subsequently used by US authorities for data mining practices. On the other hand, the EU legal framework can also support the use of such techniques.[304]

---

[291] Open Society Justice Initiative (2008), *Submission for a Roundtable of the Civil Liberties Committee of the European Union*, Brussels, 30 June, p. 3.
[292] *Idem.*
[293] Exceptionally addressing ethnic profiling as EU police policy (in reference to a 2002 EU Working Party on Terrorism recommendation on the use of 'terrorist profiling'): Hayes, Ben (2005), "A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe", in *Ethnic Profiling by Police in Europe,* Open Society Justice Initiative, pp. 32-43.
[294] De Schutter, Olivier and Julie Ringelheim (2008), "Ethnic profiling: A Rising Challenge for European Human Rights Law", *The Modern Law Review,* 71(3), p. 363. See also: Ringelheim, Julie (2006), *Processing Data on Racial or Ethnic Origin for Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?*, Center for Human Rights and Global Justice Working Paper, No. 13, NYU School of Law, New York.
[295] In relation with this type of profiling, the UK House of Lords delivered a key judgement on the *Roma Rights Case* (Open Society Justice Initiative (2008), *Submission for a Roundtable of the Civil Liberties Committee of the European Union*, Brussels, 30 June, p. 6).
[296] Taipale, Kim (2007), *The Privacy Implications of Government Data Mining Programs*, Testimony before the US Senate Committee on the Judiciary, January 10, p. 6.
[297] Lyon, David (ed.) (2003), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, New York, p. 20.
[298] De Schutter and Ringelheim, *op. cit.,* p. 361.
[299] Cybenko, George (2005), "AI And The Modern Networked Organization", *IEE Intelligent Systems,* Vol. 20, No. 5, September-October, p. 8.
[300] Amoore, Louise (2006), "Biometrics borders: Governing mobilities in the war on terror", *Political Geography,* 25, p. 336. According to a EC representative, *"you might say that that looks like profiling"* (declaration of Ms Verkleij at the House of Lords, European Union Committee of the House of Lords (2008), *The Passenger Name Record (PNR) Framework Decision*, HL Paper 106, London, Evidence: p. 45).
[301] Declaration of Ms Meg Hillier at the House of Lords (European Union Committee of the House of Lords (2008), *The Passenger Name Record (PNR) Framework Decision*, HL Paper 106, London, Evidence: p. 11).
[302] For an overview, see: Stanley, Jay and Barry Steinhardt (2007), *Even Bigger, Even Weaker: The Emerging Surveillance Society: Where are we now?* , American Civil Liberties Union (ACLU).
[303] See: Amoore, Louise and Marieke De Goede (2005), "Governance, risk and dataveillance in the war on terror", *Crime, Law & Social Challenge,* 43, pp. 149-173.
[304] For instance, through the so-called Third Money Laundering Directive (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 L 309, 25/11/2005, pp. 15–36).

60. As an element of a Counter-Terrorism Package, the European Commission adopted on 6 November 2007 a proposal concerning a common EU approach on the use of passenger data (PNR) for law enforcement purposes.[305] According to the proposal, the data processed and shared among all Member States is to "*fulfil the purpose of developing risk indicators and establishing patterns of travel and behaviour*".[306] Although the European Commission has refused to label this activity as a profiling activity, others have.[307] In any case, the system would lead to identify certain categories of passengers as 'high-risk passengers', presumably to subject them to further actions, or at least further examination. 'The Future Group' envisions in its already mentioned 2008 report "*an increasingly connected world in which public security organizations will have access to almost limitless amounts of potentially useful information*", and asks Member States to prioritise investment in "*technologies that enable automated data analysis*".[308]

61. There is an almost universal agreement about the need to assess the efficacy of data mining systems.[309] Their efficacy is especially discussed in the context of counterterrorism,[310] as predictive data mining appears especially ill-suited tool for such a purpose.[311] Profiling practices through predictive data mining are believed to potentially interfere with many different rights,[312] and most of the literature agrees on the idea that these techniques cannot be developed without special legal and technical safeguards, such as strict provisions on oversight and review, and the need to subject them to judicial review.[313] Part of the legal challenges related to predictive data mining concern the actual collection or acquisition of data to be mined, while others concern further processing of the data.[314] Almost all disclosed US government programs using personal data for data mining have in common their reliance on data supplied by the private sector.[315] According to data protection rules, the specificity of the purpose of processing constitutes a specific criterion determining the lawfulness of processing activities. The US approach to the re-use of data is different.[316] Does the use of predictive data mining practices by itself challenge the presumption of innocence? Some have been argued that as long as it merely serves for the 'allocation' of (security) resources, no issue of presumption of innocence is directly relevant.[317] In many circumstances, predictive data mining practices present risks going well beyond what the right to privacy and data protection can cope with on their own,[318] as they can provoke deep discrimination giving rise to concerns of social justice.[319]

---

[305] EC (2007), *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.
[306] *Ibidem*, p. 10.
[307] Ludford, Sarah (2008). *Working Document on problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control*, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, 30.09.2008, p. 4.
[308] 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,* Report, June, p. 43.
[309] Cate, Fred H. (2008), "Government Data Mining: The Need for a Legal Framework", *Harvard Civil Rights-Civil Liberties Law Review* (CR-CL), 43(2), p. 476.
[310] See, for instance: Jonas, Jeff and Jim Harper (2006), "Effective Counterterrorism and the Limited Role of Predictive Data Mining", *Policy Analysis,* 584, December, p. 7. These arguments have been described as 'the pseudo-technical arguments' (Taipale (2007), *op. cit.*, p. 7).
[311] Especially considering that as the technique requires a significant number of known instances of a particular behaviour in order to develop valid predictive models (Seifert, Jeffrey W. (2007), *Data Mining and Homeland Security: An Overview*, Congressional Research Service (CRS) Report for Congress, Updated January 18, p. 3).
[312] Such as equal treatment and the prohibition of discrimination, privacy and data protection, the right to liberty and the freedom of movement, right to property, freedom to conduct a business, right to fair trail, right to family and private life, and right to asylum (Pap, András (2008), *Ethnicity and Race-Based Profiling in Counter-Terrorism, Law Enforcement and Border Control,* Study for Policy Department C, Citizens' Rights and Constitutional Affairs, Directorate General Internal Policies, European Parliament, PE 408.326, November, p. 17).
[313] Taipale (2007), *op. cit.*, p. 4. See also: Rubinstein, Ira S., Ronald D. LEE & Paul M. Schwartz (2008), "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", *The University of Chicago Law Review,* 75, p. 266.
[314] Applying this distinction: Solove, Daniel J. (2008), "Data Mining and the Security-Liberty Debate", *University of Chicago Law Review,* 74, pp. 343-360.
[315] Cate, *op. cit.*, p. 451.
[316] In the US, the Supreme Court has refused to restrict the government's access to data held by third parties holding there can be no reasonable expectation of privacy in information held by a third party (see: Cate, *op. cit.*, pp. 435-489).
[317] For a defence of predictive data-mining as a tool, even if with limited purposes: TAIPALE, K.A. (2005), "The Trusted Systems Problem: Security Envelopes, Statistical Threat Analysis, and the Presumption of Innocence", *IEE Intelligent Systems,* VoL. 20, No. 5, September-October, pp. 80-82. See also: TAIPALE, K. A. (2004), "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and The Lessons of King Ludd", Yale Journal of Law and Technology, Vol. 7, No. 123, December 2004, pp. 125-201.
[318] Lyon, David (ed.) (2003), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, New York, p. 2.
[319] *Ibidem,* p. 1.

62. In general, criminal 'threat analysis' is believed to potentially lead to serious misuse of databases with information of many innocent individuals;[320] and even simple 'fishing net' investigative techniques (filtering data through pre-established criteria) have been considered to violate the principle of proportionality, as they interfere with the privacy of a large number of innocent individuals.[321] This argument received special support in 2006 as the Federal Constitutional Court of Germany provided a key judgement regarding an attempt of German authorities to identify 'sleepers' of terrorist organizations resorting to the so-called *Rasterfahndung* method. The 'fishing net' method foresaw the screening of data from public and private bodies in order to track individuals presenting a series of features, following criteria which included: being male, Muslim, national of or born in a country with predominantly Muslim population, a current or former student.[322] On 4 April 2006, the German Constitutional Court ruled that the *Rasterfahndung* was in breach of the fundamental right of informational self-determination. Predictive data mining exponentially increases the interferences with the private life of individuals, as it does not simply filter data through pre-established criteria, but massively processes data precisely in order to formulate criteria, that it afterwards applies and constantly re-assesses.

63. If any policy of prevention carries with it particular risks of abuse,[323] it can be said that the combination of different forward-looking security approaches triggers special, aggravated risks. Current techniques of prediction have been said to create a mixture of fiction and reality, merging the boundaries of the virtual and the actual, thereby introducing fiction into reality.[324] A particular problem emerges from the coexistence of 'loose' definitions of terrorist offences, on the one hand, and especially extended powers of investigation, surveillance and prosecution adopted in the name of antiterrorism, on the other hand. This coexistence can lead to abusive use of such special powers and undue restrictions of fundamental rights of individuals, notably the right to privacy, the right to a fair trail or the right to liberty and security.[325] The way in which counterterrorist strategies unfold within existing legislation, envisioning freedom and uncontrolled spaces as potential risks to be put under a general suspicion, interferes notably with civil society.[326] Criminologists have already devoted for many years special attention to the development of proactive approaches to crime, as well as to surveillance practices, which are now much debated in the context of counterterrorism. Using the expression 'new penology', transformations undergone by the US penology in the last decades had been interpreted as a shift from a penology based on punishment or treatment of individuals towards a penology axed on surveillance and control of 'risk groups', announcing the emergence of a new model of justice, 'actuarial justice'.[327] Recent restrictions on human rights, and particularly the weakening of the presumption of innocence, can in this sense be seen as one of the effects of the changes that have taken place in the criminal justice field since the late 1970s, as inherent to the structure and operational logic of the risk-focused crime-control model.[328]

Surveillance and Anti-Surveillance

[320] Anderson (1995), *op. cit.*, p. 150.
[321] Albrecht, *op. cit.,* p. 12.
[322] Similar investigative methods had been implemented in the 1970s without any statuary basis, which was however necessary then since the Federal Constitutional Court had established in 1983 the right to self-determination of personal data (Albrecht, *op. cit.,* p. 11).
[323] Swire, *op. cit.*, p. 117.
[324] Bigo, Didier and Elspeth Guild (2007), "The Worst-case Scenario and the Man on the Clapham Omnibus" in Goold, Benjamin J., and Lazarus, Liora (eds.) (2007), *Security and human rights*, Hart, Oxford, Portland, p. 115.
[325] EU Network of Independent Experts in Fundamental Rights (2003), *The balance between freedom and security in the response by the European Union and its Member States to the terrorist threats*, Thematic Comment, p. 20.
[326] Albrecht, *op. cit.,* p.4.
[327] Mary, Philippe (2001), "Pénalité et gestion des risques: vers une justice "actuarielle" en Europe?", *Déviance et Société*, 25(1), p. 33. Such an approach is based notably on the acceptance of a level of delinquency as normal (*ibidem*, p. 35), and implies also a degree of detachment from the offence and an increased reliance on proactive approaches (Tsoukala, Anastassia (2008), *Security, Risk and Human Rights*: *A Vanishing Relationship?*, CEPS Special Report, CEPS, Brussels, September, p. 4).
[328] Tsoukala, *op. cit.*, p. 3 and p. 10. Human rights, and in particular the ECtHR jurisprudence, had been considered as insufficient to effectively moderate the trend of criminalisation of European policies, in the light of movements towards a 'penal state' following the US model (De Hert, Paul, Serge Gutwirth, Sonja Snacken and Els Dumortier (2007), « La montée de l'Etat pénal: que peuvent les droits de l'Homme? », in Yves Cartuyvels (ed.), Les droits de l'Homme, bouclier ou épée du droit pénal?, Bruylant/Publications des Facultés universitaires Saint-Louis, Bruxelles, pp. 235-290).

64. One of the main changes provoked by 9/11 was a reinforcement of 'surveillance' practices.[329] The term 'surveillance' can as a matter of fact have many different meanings: as in secret surveillance practices, as in border surveillance, or as in 'surveillance society'.[330] If the notion of 'surveillance' was traditionally confined narrowly to certain specific activities, it has tended to encompass many different practices.[331] Some view the current situation in terms of the construction of a 'surveillant assemblage', envisioned as a system transcending institutional boundaries, based on the interlinking of databases and the use of capacities originally unrelated with the criminal justice system for its purposes.[332] Illustrating the different meanings of 'surveillance', the notion of a 'bifurcation' of surveillance underlines the simultaneity of two phenomena taking place in the context of criminal justice: the extension of (soft) 'surveillance' practices to the general population in the name of crime control, and the intensification of (hard) 'surveillance' practices directed towards a minority.[333]

65. The judiciary has certainly a key role to play in ensuring that security measures do not delineate a 'surveillance society' and are not implemented in violation of human rights.[334] At national level, courts have not been inactive in verifying compliance with individual rights.[335] If data protection and privacy dominate 'anti-surveillance' debates, there is also an increasing recognition of the limits of both rights[336] and of the need to ascertain the differences in scope, rationale and logic between privacy on the one hand, and data protection on the other,[337] as well as of the need to take into account the social nature and consequences of categorisation practices, and thus the need for greater transparency and accountability.[338]

V. Main Findings And Paths For Further Research

66. The security-law nexus is not marked in Europe by any structural opposition. European law integrates security concerns, and EU security policies incorporate human rights considerations. There has been no will to modify these basic parameters, not even in the context of the fight against terrorism. Having said that, there are, however, a series of frictions between certain EU security initiatives and the protection of individual rights, and there is a general consensus on the idea that security measures can in practice impinge on human rights and civil liberties. The endorsement of a 'balancing approach' has not always lead to well-balanced decisions, and might actually systematically lead to erroneous conceptions of the ways in which security and law, and security and human rights, profoundly relate to each other.

---

[329] Haggerty, Kevin D. and Amber Gazso (2005), "Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats", *Canadian Journal of Sociology*, 30(2), p. 169.

[330] An expression which can be used as a rhetorical device to underline certain aspects of the contemporary world (Lyon, David (2004), "Surveillance Technologies: Trends and Social Implications", in Organisation for Economic Co-operation and Development (OECD), *The Security Economy*, Paris, p. 131).

[331] Fox, Richard (2001), "Someone to watch over us: Back to the panopticon?", *Criminal Justice,* 1(3), p. 266.

[332] Haggerty, Kevin D. and Richard V. Ericsson (2000), "The surveillant assemblage", *British Journal of Sociology*, 51(4), pp. 616-617.

[333] Norris, Clive (2007), "The Intensification and Bifurcation of Surveillance in British Criminal Justice Policy", *European Journal on Criminal Policy and Research*, 13, p. 155.

[334] Even if other mechanisms can be imagined to complement the protection granted by it. In this sense, for instance: Rotenberg, Marc (2006), Marc Rotenberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, Social Science Research Network Working Paper Series, September, p. 60.

[335] The German Constitutional Court, for instance, issued a series of decisions in 2008 considerably limiting or altogether discarding some security laws in Germany: on police laws of Hessen and Schleswig Holstein allowing for automatic identification and storage of vehicle registration plates of private cars by video cameras without suspicion in order to compare the data with police databases (1 BvR 2074/05, 11.3.2008), and on some aspects of the a federal law implementing the Data Retention Directive (1 BVr 256/08, 11.3.2008) (Geyer Florian (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice,* Research Paper No. 9, CEPS, Brussels, May, p. 1).

[336] Schermer, Bart Willem (2007), *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, SKIS Dissertation Series no. 2007-05, Leiden University Press, p. 147. See also: Lyon, David (2007), *Surveillance Studies: An Overview*, Polity Press, Cambridge, p. 169.

[337] De Hert, Paul and Serge Gutwirth (2006) "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power" in Claes, E., A. Duff and Serge Gutwirth (eds.), *Privacy and the criminal law*, Intersentia, Antwerp-Oxford-New York, p. 62.

[338] Lyon, David (2004), "Surveillance Technologies: Trends and Social Implications", in Organisation for Economic Co-operation and Development (OECD), *The Security Economy*, Paris, p. 140.

67. A series of paths especially requiring further consideration in the analysis of value assumptions linked to the cross-border legal dilemmas relevant to current and anticipated challenges of European security have been identified:

- The use of the triangle 'mobility, security and privacy' as a metaphor guiding current European security choices appears to potentially drive to the elaboration of biased proposals. The 2008 report of 'The Future Group' summarises a new formulation of the 'balancing paradigm' as "*balancing citizens' expectations of privacy against their expectations of proactive protection*".[339] It is crucial to critically assess this vision in the light of existing knowledge on the 'balancing approach', as well as of the scholarship on proactive approaches to security.

- Recent developments concerning EU data protection law confirm the double nature of data protection. If it is, on the one hand, a potential obstacle to data processing, it is also, on the other, an enabler and legitimising factor for such data processing. This is notably applicable in the context of the current reinforcement of transatlantic cooperation with the US. There is a need to explore how to keep data protection core principles (concretely, the subjective rights it grants to individuals) effective in such a cross-border situation, in order to avoid the transformation of data protection instruments into mere enablers of data transfers, deprived of any counter-powering strength.

- Security approaches to technology reveal that there is in Europe a parallel tendency towards, in the name of security, both disregard the strong promotion of 'privacy-by-design', on the one hand, and actually favour the generalisation of what we could call an '*impossibility of privacy* by design', on the other hand. Not only do decision-makers appear to be reticent to firmly impose privacy requirements to technological devices, they actually also very carefully consider possibilities of forcing through law the technological impossibility of 'opacity' (for instance, through compulsory retention of electronic communications data). The possible back up of the right to privacy with new rights, such as the right to the integrity and confidentiality of information systems, should be studied in detail in the light of such developments.

- Profiling through predictive data mining raises many questions that still need to be fully ethically and legally assessed, such as how to translate into the deployment of these practices the requirements of proportionality and lawfulness. There are issues that can be dealt with from the perspective of the protection of personal data (if accurately described), but also others which relate to the degree of privacy incompatible with anonymous surveillance and systematic observation of deeds and actions, triggering protection in the name of the right to privacy.[340] Forward-looking security strategies can be generally problematic insofar as they establish ways of rendering illegal what has yet to happen, thus facilitating arbitrariness and having a dangerous negative impact on legitimate dissent. Principles of criminal law such as the presumption of innocence should be placed solidly in the discussions of these practices.

- The ECtHR and the ECJ have recently provided many important insights on different fundamental issues, directly linked to a series of current legal challenges faced by EU security. Their case law, as well as pertinent national case law, proves that the judiciary is genuinely interested in offering tools for the enhanced deployment of security policies. Such case law should be further explored for a better understanding of the dilemmas underpinning the mentioned legal challenges. Upcoming security measures must be examined in time to ensure their optimal legislative development, notably in terms of transparency, and to duly take into consideration the eventual necessity for new safeguards, be their legal and/or technological.

[339] 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,* Report, June, p. 43.
[340] Dinant, Jean-Marc, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy (2008), *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg, p. 31.

VI. References

Literature

ACED FÉLEZ, Emilio (2007), "Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm", *Revista de Derecho constitucional europeo*, Enero-Junio, 7, pp. 65-96.

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.

AGAMEN, Giorgio (1998), *Homo sacer: sovereign power and bare life*, Stanford University Press, Stanford.

ALBRECHT, Hans-Jörg (2006), *Country Report on Germany*, Max-Planck-Institute for Foreign and International Criminal Law.

ALDRICH, Richard J. (2004), "Transatlantic intelligence and security cooperation", *International Affairs*, 80(3), pp. 733-755.

ALEGRE, Susie et al., *The Hague Programme: Strengthening Freedom, Security and Justice in the EU*, European Policy Centre (EPC) Working Paper no. 15, February.

ALEGRE, Susie (2008), *The EU's External Cooperation in Criminal Justice and Counter-Terrorism: An Assessment of the Human Rights Implications with a particular focus on Cooperation with Canada*, CEPS Special Report, Centre for European Policy Studies, Brussels, September.

AMNESTY INTERNATIONAL (2008) *State of Denial: Europe's Role in Rendition and Secret Detention*, London.

AMOORE, Louise (2006), "Biometrics borders: Governing mobilities in the war on terror", *Political Geography*, 25, pp. 336-351

AMOORE, Louise and Marieke DE GOEDE (2005), "Governance, risk and dataveillance in the war on terror", *Crime, Law & Social Challenge*, 43, pp. 149-173.

ANDENAS, Mads and Stefan ZLEPTNIG (2003), "Surveillance and Data Protection: Regulatory Approaches in the EU and Member States", *European Business Law Review*, 14(6), pp. 765-813.

ANDERSON, Malcolm et al. (1995), *Policing the European Union*, Oxford University Press, Oxford.

ANDERSON, Malcolm and Joanna APAP (2002), *Changing Conceptions of Security and their Implications for EU Justice and Home Affairs Cooperation*, CEPS Policy Brief, No. 26, October.

ANDERSON, Malcolm (2007), "Internal and External Security in the EU: Is There Any Longer a Distinction?", in GÄNZLE, Stefan and Allen G. SENS (eds.), *The Changing Politics of European Security: Europe alone?*, Palgrave, Hampshire, pp. 31-46.

APAP, Joanna and Sergio CARRERA (2003), *Maintaining Security Within Borders: Towards a Permanent State of Emergency in the EU?*, CEPS Policy Brief, Number 41, November, CEPS, Brussels.

ARADAU, Claudia and Rens VAN MUNSTER (2007), "Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future", *European Journal of International Relations*, 13, pp. 89-115.

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

ARAI-TAKAHASHI, Yutaka (2002), *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR,* Intersentia, Antwerpen-Oxford-New York.

AUS, Jonathan P. (2003), *Supranational Governance in an 'Area of Freedom, Security and Justice': Eurodac and the Politics of Biometric Control*, Sussex European Institute Working Paper No. 72.

--- (2006), *Eurodac: A Solution Looking for a Problem?*, European Integration online Papers (EIoP), 10(6), 21 July.

--- (2006), *Decision-making under Pressure: The Negotiation of the Biometric Passports Regulation in the Council*, ARENA Working Paper, No. 11, Centre for European Studies, University of Oslo, September.

BALDACCINI, Anneliese, Elspeth GUILD and Helen TONER (2007), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, Oxford.

BALKIN, Jack M. (2008), "Critical Legal Theory Today", available at SSRN: http://ssrn.com/abstract=1083846.

BALLESTEROS MOFFA, Luis Ángel (2008), "Hacia un difícil equilibrio entre privacidad y seguridad: la conservación de datos en las comunidades electrónicas y la transferencia de datos de pasajeros por las compañías aéreas", *Revista Española de Derecho Administrativo*, 137 (2008), pp. 31-55.

BALZACQ, Thierry, Didier BIGO, Sergio CARRERA and Elspeth GUILD (2006), *Security and the Two-Level Game: the Treaty of Prüm, the EU and the Management of Threats*, CEPS Working Document, No. 234, CEPS, Brussels, January.

BALZACQ, Thierry and Sergio CARRERA (2006), *Security Versus Freedom? A Challenge for Europe's Future*, Ashgate, Aldershot.

BANISAR, David (2008), *Speaking of terror: A survey of the effects of counter-terrorism legislation on freedom of the media in Europe*, Council of Europe, November.

BIERSTEKER, Thomas J. and Sue E. ECKERT (2006), *Strengthening Targeted Sanctions Through Fair and Clear Procedures*, Report commissioned by the governments of Germany, Switzerland and Sweden, Watson Institute for International Studies.

BIGNAMI, Francesca (2007), *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining*, Duke Law School Working Paper Series, Paper 75.

--- (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.

BIGO, Didier (2005), "Globalized-in-security: the Field and the Ban-opticon" in SOLOMON, John and Naoki SAKAI, *Traces: Translation, Philosophy and Colonial Difference*, 4, p. 5.

--- (2006), "Security, exception, ban and surveillance", in LYON, David (ed.), *Theorizing Surveillance: The panopticon and beyond*, Willian Publishing, Portland, pp. 46-68.

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 Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November.

BIGO, Didier, Sergio CARRERA, Elspeth GUILD and R.B.J. WALKER (2007), *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project*, Research Paper No. 4, CEPS, Brussels, February, p. 18.

BORYS, W.J. (2006) *"Need To Know" To "Need To Share": How Terrorism Is Changing The Intelligence Community's Culture*, Canadian Forces College.

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.

BROEDERS, Dennis (2007), "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants", *International Sociology*, 22(1), pp. 71-92.

BRONITT, Simon (2008), "Balancing Security and Liberty: Critical Perspectives on Terrorism Law Reform" in Miriam GANI and Penelope MATHEW (ed.), Fresh Perspectives on the 'War on Terror', pp. 65-83.

BROUWER, Evelien (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers, Leiden.

BULTERMAN, Mielle (2006), "Fundamental Rights and the United Nations Financial Sanction Regime: The Kadi and Yusuf Judgments of the Court of First Instance of the European Communities", *Leiden Journal of International Law*, 19, pp. 753-772.

BUNYAN, Tony (2002), « Surveillance des télécommunications : fin de partie », *Culture et Conflits*, vol. 46, pp. 65-71.

--- (2006), *The "principle of availability"*, Statewatch, December.

--- (2008), *The Shape of Things to Come: EU Future report*, Statewatch, September.

BURGESS, Peter J. (2008), *Security After Privacy: The Transformation of Personal Data in the Age of Terror*, Policy Brief, PRIO, 5/2008.

--- (2008), *Security as Ethics*, Policy Brief, PRIO, 6/2008.

BURGESS, J. Peter and David RODIN (2008), *The Role of Law, Ethics and Justice in Security Practices*, Security: Advancing a Framework for Enquiry (SAFE) Conference report, International Peace Research Institute, Oslo (PRIO) Papers, Oslo.

BURKERT, Herbert (1999), *Privacy-Data Protection: A German/European Perspective*, 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Massachusetts.

BUSCH, Heiner (2006), *The dream of total data collection – status quo and future plans for EU information systems*, Statewatch Bulletin Vol. 16, No. 5/6.

BYERS, Michael (2008), "Preemptive Self-defense: Hegemony, Equality and Strategies of Legal Change", *The Journal of Political Philosophy*, 11(2), pp. 171-190.

BYGRAVE, Lee A. (1998), "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology*, 6, pp. 247-284.

--- (2000), "Minding the machine: Art. 15 of the EC Data Protection Directive and automated profiling", *Privacy Law and Policy Reporter*, 40.

--- (2001), "The Place of Privacy In Data Protection Law", *University of NSW Law Journal*, Vol. 6.

--- (2002), "Privacy-Enhancing Technologies: Caught between a Rock and a Hard Place", *Privacy Law & Policy Reporter*, 9, pp. 135-137.

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

BYRNES, Andrew (2008), "More Law or Less Law? The Resilience of Human Rights Law and Institutions " in Miriam GANI and Penelope MATHEW (ed.), *Fresh Perspectives on the 'War on Terror'*, pp. 127-158.

CALOZ-TSCHOPP, Marie Claire and Pierre DASEN (2007), *Globalization, migration and human rights: a new paradigm for research and citizenship, Volume I*, Bruylant, Bruxelles.

CÁMARA VILLAR, Gregorio (2007), "La garantía de los derechos fundamentales afectados por la Convención de Prüm", *Revista de Derecho constitucional europeo*, Enero-Junio(7), pp. 97-118.

CAMERON, Iain (2003), "European Union Anti-terrorist Blacklisting", *Human Rights Law Review*, 2(2), pp. 225-256.

c.a.s.e. COLLECTIVE (2006), "Critical Approaches to Security in Europe: A Networked Manifesto", *Security Dialogue*, 37(4), pp. 443-487.

CATE, Fred H. (2008), "Government Data Mining: The Need for a Legal Framework", *Harvard Civil Rights-Civil Liberties Law Review* (CR-CL), 43(2), pp. 435-489.

CAVOUKIAN, Ann (2003), *National Security in a Post-9/11 World: The Rise of Surveillance… the Demise of Privacy?*, Information and Privacy Commissioner of Ontario.

Commissioner for Human Rights (2008), *Protecting the Right to Privacy in the Fight Against Terrorism*, Council of Europe, Strasbourg, 4 December.

CONTE, Alex (2008), *Handbook on Human Rights Compliance While Countering Terrorism*, Center on Global Counterterrorism Cooperation, January.

COT Institute for Safety, Security and Crisis Management (ed.) (2007), *Notions of Security: Shifting Concepts and Perspectives*, Transnational Terrorism, Security and the Rule of Law (TTSRL), Deliverable 1, Work Package 2, February.

CREPEAU, François, Delphine NAKACHE and Idil ATAK (2007), "International Migration: Security Concerns and Human Rights Standards", *Transcultural Psychiatry*, 44, pp. 311-337.

CRITCHELL-WARD, Ann and Kara LANDSBOROUGH-McDONALD (2007), "Data Protection Law in the European Union and the United Kingdom", *Comparative Law Yearbook of International Business*, 29, pp. 515-578.

CYBENKO, George (2005), "AI And The Modern Networked Organization", *IEE Intelligent Systems*, 20(5), September-October, pp. 79-80.

DALFERTH, Simon (2004), *Enlarging the Area of Freedom, Security and Justice: Europeanisation, Policy Transfer and the Police*, September, Charles University.

DAVIES, Sharon L. (2005), *Profiling Terror*, Public Law and Legal Theory Working Paper Series No. 48, Center for Interdisciplinary Law and Policy Studies Working Paper Series No. 31, The Ohio State University, October.

DE GOEDE, Marieke (2008), "The Politics of Preemption and the War on Terror in Europe", *European Journal of International Relations*, 14, pp. 161-184.

DE HERT, Paul (2005), "Balancing security and liberty within the European human rights framework: A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review*, 1(1), pp. 68-96.

--- (2005), *Biometrics: legal issues and implications*, Background paper, Institute of Prospective Technological Studies, Sevilla.

DE HERT, Paul, Gloria GONZÁLEZ FUSTER and Bert-Jaap KOOPS (2006), "Fighting Cybercrime in the Two Europes: The Added Value of the EU Framework Decision and the Council of Europe Convention", *International Review of Penal Law*, 77(3-4), pp. 503-524.

DE HERT, Paul and Serge GUTWIRTH (2003), "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location based services and the virtual residence", in Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)*, European Commission, July.

--- (2006) "Privacy, Data Protection and Law enforcement, opacity of the individuals and transparency of power" in CLAES, E., A. DUFF and Serge GUTWIRTH (eds.), *Privacy and the criminal law*, Intersentia, Antwerp-Oxford-New York, pp. 61-104.

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

DE HERT, Paul, Serge GUTWIRTH, Sonja SNACKEN and Els DUMORTIER (2007), « La montée de l'Etat pénal: que peuvent les droits de l'Homme? », in Yves CARTUYVELS (ed.), *Les droits de l'Homme, buclier ou épée du droit pénal?*, Bruylant/Publications des Facultés universitaires Saint-Louis, Bruxelles, pp. 235-290.

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 for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), October.

DE HERT, Paul, Vagelis PAPAKONSTANTINOU and Cornelia RIEHLE (2008), "Data protection in the third pillar: cautious pessimism", in M. Martin (Ed.), *Crime, rights and the EU: The future of police and judicial cooperation*, JUSTICE, London.

DEL CASTILLO VÁZQUEZ, Isabel-Cecilia (2007), *Protección de datos: cuestiones constitucionales y administrativas (El derecho a saber y la obligación de callar)*, Aranzadi, Thomson Civitas, Cizur Menor.

DEN BOER, Monica (2003), *9/11 and the Europeanisation of Anti-terrorism Policy: a Critical Assessment*, Notre Europe Policy Papers, N° 6, September.

--- (2008), *Immigration and Its Effects on the Security Discourse in Europe: Time for Demystification*, Amsterdam Law Forum, Vol. 1, No. 1.

DE SCHUTTER, Bart (2001), "Data Protection in the Area of Freedom, Security and Justice", in Collegium (2001), *Special Edition — Proceedings of the Conference: 'Integrated Security in Europe, a Democratic Perspective'*, No. 22, XII.2001, Bruges, pp. 51-55.

DE SCHUTTER, Olivier (2007), "L'agence des droits fondamentaux", *Journal des tribunaux du droit européen*, avril, 138, pp. 97-102.

DE SCHUTTER, Olivier and Julie RINGELHEIM (2008), "Ethnic profiling: A Rising Challenge for European Human Rights Law", *The Modern Law Review*, 71(3), pp. 358-384.

DI MARTINO, Alessandra (2004), *Datenschutz im Europäischen Rech*t, WHI Paper 15/04, Walter Hallstein-Institut für Europäisches Verfassungsrecht für Europäisches Verfassungsrecht, Humboldt-Universität zu Berlin.

DINANT, Jean-Marc, Christophe LAZARO, Yves POULLET, Nathalie LEFEVER and Antoinette ROUVROY (2008), *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg.

DOCQUIR, Benjamin (2008), *Le droit à la vie privée*, De Boeck, Larcier, Bruxelles.

DUNNE, Tim and Nicholas J. WHEELER (2004), "'We the Peoples': Contending Discourses of Security in Human Rights Theory and Practice", *International Relations*, 2004, 18(1), pp. 9-23.

ECKES, Christina (2007), "Case T-228/02, *Organisation des Modjahedines du peuple d'Iran v. Council and UK (OMPI)*, Judgement of the Court of First Instance (Second Chamber) of 12 December 2006", *Common Market Law Review*, 44, pp. 1117-1129.

EPSTEIN, Charlotte (2007), "Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders", *International Political Sociology*, I, pp. 149-164.

European Group on Ethics in Science and New Technologies (2005), *Ethical aspects of ICT implants in the human body*, 16 March.

ETZIONI, Amitai (2004), *The Common Good*, Polity Press, Malden.

EU Network of Independent Experts in Fundamental Rights (2003), *The balance between freedom and security in the response by the European Union and its Member States to the terrorist threats*, Thematic Comment

European Union Committee, House Of Lords (2008), *FRONTEX: The EU external borders agency*, Report with evidence, 9th Report of Session 2007-08, 5 March, The Stationery Office Limited, London.

FAURE ATGER, Anaïs (2008), *The Abolition of Internal Border Checks in an Enlarged Schengen Area: Freedom of movement or a web of scattered security checks?* , Research Paper No. 8, CHALLENGE, Brussels, p. 18.

FLAHERTY, David H. (1989), *Protecting Privacy In Surveillance Societies*, University of North Carolina Press, Chapel Hill.

FOX, Richard (2001), "Someone to watch over us: Back to the panopticon?", *Criminal Justice*, 1(3), pp. 251-276.

GEYER, Florian (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, Research Paper No. 9, CEPS, Brussels, May.

GOLDER, Ben and George WILLIAMS (2006), "Balancing National Security and Human Rights: Assessing the Legal Response of Common Law Nations to the Threat of Terrorism", *Journal of Comparative Policy Analysis,* 8(1), pp. 43-62.

GONZÁLEZ FUSTER, Gloria, Paul DE HERT and Serge GUTWIRTH (2008), "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law, Computers & Technology*, 22(1-2), pp. 191-202.

GONZÁLEZ FUSTER, Gloria and Paul DE HERT (2007), "PNR and compensation", in LODGE, Juliet (ed.) (2007), *Are You Who You Say You Are? The EU and Biometric Borders,* Wolf Legal Publishers, Nijmegen, pp. 101-109.

GONZÁLEZ FUSTER, Gloria and Serge GUTWIRTH (2008), *Data Protection in the EU: Towards 'Reflexive Governance'?*, REFGOV Working Paper Series, FR-19, July, Brussels.

GONZÁLEZ VAQUÉ, Luis (2006), "El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EE.UU. para la transmisión de datos sobre los pasajeros de las compañías aéreas", *Revista Española de Derecho Europeo*, 20, octubre - diciembre, pp. 557-576.

GOOLD, Benjamin J., and LAZARUS, Liora (eds.) (2007), *Security and human rights*, Oxford, Portland, Hart.

GRAMMATIKAS, Vassilios (2006). *EU Counter-terrorist Policies: Security vs. Human Rights?*, HUMSEC Working Paper.

GREER, Steven (1997), *The exceptions to Articles 8 to 11 of the European Convention on Human Rights,* Council of Europe, Strasbourg.

GUILD, Elspeth (2007), *Security and European Human Rights: protecting individual rights in times of exception and military action*, Wolf Legal Publishers, Nijmegen,

GUILD, Elspeth and Didier BIGO (2003), « Schengen et la politique des visas », *Culture et Conflits*, 49, 1/2003, pp. 5-21.

--- (2003), « Le visa Schengen : expression d'une stratégie de « police » à distance », *Culture et Conflits*, 49, 1/2003, pp. 22-37.

GUILD, Elspeth and Evelien BROUWER (2006), *The Political Life of Data: the ECJ Decision on the PNR Agreement between the EU and the US*, Policy Brief No. 109, CEPS, Brussels, July.

GUILD, Elspeth and Florian GEYER (2006), *Justice and Home Affairs Issues at European Union Level*, Written evidence submitted by the Centre for European Policy Studies (CEPS) to the Select Committee on Home Affairs (House of Commons), CEPS, Brussels, November.

--- (2008), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot.

GUILD, Elspeth, Sergio CARRERA and Florian GEYER (2008), *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?* , CEPS Policy Brief No. 154, CEPS, Brussels, March.

GUNASEKARA, Gehan (2006), "The 'final' privacy frontier? Regulating trans-border data flows", *International Journal and Information Technology*, 15(3), pp. 362-393.

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

--- (2007), "Biometrics between opacity and transparency", *Annali dell'Istituto Superiore di Sanità*, 43(1), pp. 61-65.

HAGGERTY, Kevin D. and Amber GAZSO (2005), "Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats", *Canadian Journal of Sociology*, 30(2), p. 169.

HAGGERTY, Kevin D. and Richard V. ERICSON (2000), "The surveillant assemblage", *British Journal of Sociology*, 51(4), pp. 605-622.

HAM, Shane and Robert D. ATKINSON (2002), *Using Technology to Detect and Prevent Terrorism*, Progressive Policy Institute, January.

HAYES, Ben (2005), "A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe", in *Ethnic Profiling by Police in Europe,* Open Society Justice Initiative, pp. 32-43.

HEISENBERG, Dorothee (2005), *Negotiating Privacy: the European Union, the United States and Personal Data Protection*, Lynne Rienner Publishers, London.

HIJMANS, Hielke (2006), "The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority", *Common Market Law Review,* 43, pp. 1313-1342.

HILDEBRANDT, Mireille and Serge GUTWIRTH (eds.) (2008), *Profiling the European Citizen*, Springer, London.

HILLS, Alice (2003), *Towards a rationality of democratic border management*, Geneva Centre for the Democratic Control of Armed Forces (DCAF), March.

HOBBING, Peter (2006), *A comparison of the now agreed VIS package and the US-VISIT system*, Briefing Paper, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament.

--- (2008), *Tracing Terrorists: The EU-Canada Agreement in PNR matters*, CEPS Special Report, CEPS, Brussels, September.

HUFNAGEL, Saskia (2008), *German perspectives on the right to life and human dignity in the 'war on terror'*, Social Science Research Network, Legal Scholarship Network, ANU College of Law Resarch Paper No. 08-18, The Australian National University College of Law.

HUMAN RIGHTS WATCH (2008), *Preemting Justice: Counterterrorism Laws and Procedures in France*, July.

JEANDESBOZ, Julien (2008), *An Analysis of the Commission Communications on Future Development of FRONTEX and the Creation of a European Border Surveillance System (EUROSUR)*, Briefing Paper for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, June.

JONAS, Jeff and Jim HARPER (2006), "Effective Counterterrorism and the Limited Role of Predictive Data Mining", *Policy Analysis*, 584, December.

KARANJA, S. K. (2006), "SIS II Legislative Proposals 2005: Gains and Losses!", *Yulex*, 2005, pp. 81–103.

KEYSER, Mike (2003), "The Council of Europe Convention on Cybercrime", *Journal Of Transnational Law And Policy*, 12(2), pp. 287-326.

KINDT, Els (2007), "Biometric application and the data protection legislation: The legal overview and the proportionality test", *Datenschutz und Datensicherheit*, 31, pp. 166-170.

KOOPS, Bert-Jaap and Ronald LEENES (2005), "'Code' and the Slow Erosion of Privacy", *Michigan Telecommunications and Technology Law Review*, 12, pp. 115-159.

KRANENBORG, Herke (2008), "Access to documents and data protection in the European Union: on the public nature of personal data", *Common Market Law Review*, 45, pp. 1.079-1.114.

LEVI, Michael and David S. WALL (2004), "Technologies, Security and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, 31(2), June, pp. 194-220.

LIBERATORE, Angela (2005), *Balancing Security and Democracy: The Politics of Biometric Identification in the European Union*, European University Institute Working Papers, RSCAS No. 2005/30.

LODGE, Juliet (2004), "EU homeland security: citizens or suspects?", *Journal of European Integration,* 26(3), pp. 253-279.

LUDFORD, Sarah (2008), *Working Document on problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control*, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, 30.09.2008.

LYON, David (ed.) (2003), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, New York.

LYON, David (2004), "Globalizing Surveillance: Comparative and Sociological Perspectives", *International Sociology*, 19(2), pp. 135-149.

--- (2004), "Surveillance Technologies: Trends and Social Implications", in Organisation for Economic Co-operation and Development (OECD), *The Security Economy*, Paris.

--- (2007), *Surveillance Studies: An Overview*, Polity Press, Cambridge.

MACOVEI, Monica (2005), *The right to liberty and security of the person: A guide to the implementation of Article 5 of the European Convention on Human Rights*, Human rights handbooks No. 5, Council of Europe.

MARTENCZUK, Bernd and Servaas VAN THIEL (eds.) (2008), *Justice, Liberty, Security: New challenges for EU external relations*, VUB Press, Brussels.

MARY, Philippe (2001), “Pénalité et gestion des risques: vers une justice “actuarielle” en Europe?”, *Déviance et Société*, 25(1), pp. 33-51.

MATHIESEN, Thomas (2005), *Lex Vigilatoria: Towards a control system without a state?*, Essays for civil liberties and democracy in Europe, European Civil Liberties Network.

MATTELART, Armand (2008), *La globalisation de la surveillance : Aux origines de l’ordre sécuritaire*, Editions La Découverte, Paris.

MCGINLEY, Marie and Roderick PARKES (2007), *Data Protection in the EU’s Internal Security Cooperation: Fundamental Rights vs. Effective Cooperation?*, Stiftung Wissenschaft und Politik (SWP) Research Paper 5, German Institute for International and Security Affairs, Berlin, May.

MENDEZ, Mario (2007), "Passenger Name Record Agreement: European Court of Justice", *European Constitutional Law Review*, 3(1), pp. 127-147.

MICHAELSEN, Christopher (2006), “Balancing Civil Liberties Against National Security? A Critique of Counterterrorism Rhetoric”, *University of NSW Law Journal*, 29(1), pp. 1-21.

MICHEL, Valérie (2006), "La dimension externe de la protection des données à caractère personnel: acquiescement, perplexité et frustration", *Revue trimestrielle de droit européen*, 42(3), pp. 549-559.

MITSILEGAS, Valsamis, Jörg MONAR and Wyn REES (2003), *The European Union and Internal Security: Guardian of the People?*, Palgrave, Hampshire.

MOECKLI, Daniel (2006), *Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection.* paper presented at the Conference of the Association of Human Rights Institutes, September.

--- (2008), *Human Rights Strategies in an Age of Counter-Terrorism*, SSRN, retrieved from http://ssrn.com/abstract=1189722.

--- (2008), *Human rights and non-discrimination in the 'War on terror'*, Oxford University Press, Oxford.

MOINY, Yves (2005), *Protection of Personal Data and Citizens’ Rights of Privacy in the Fight Against the Financing of Terrorism*, CEPS Policy Brief, CEPS, Brussels, March.

MUNTARBHORN, Vitit, Iris ALMEIDA and Lloyd LIPSETT (2002), *Report of the Think Tank on Promoting Human Rights and Democracy in the Context of Terrorism*, International Centre for Human Rights and Democratic Development, Ottawa, May.

National Commission on Terrorist Attacks upon the United States (2004), *The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States*, Norton, New York.

NEAL, Andrew (2005), *Review of the literature on the 'state of exception' and the application of this concept to contemporary politics*, CHALLENGE Working Paper.

NETTESHEIM, Martin (2007), "U. N. Sanctions Against Individuals – A Challenge To The Architecture of European Governance", *Common Market Law Review*, 44(3), pp. 567-600.

NORRIS, Clive (2007), “The Intensification and Bifurcation of Surveillance in British Criminal Justice Policy”, *European Journal on Criminal Policy and Research*, 13, pp. 139-158.

NTOUVAS, Ioannis (2007), “Air Passenger Data Transfer to the USA: the Decision of the ECJ and the latest developments”, *International Journal of Law and Information Technology*, 16(1), pp. 73-95.

Open Society Justice Initiative (2008), *Submission for a Roundtable of the Civil Liberties Committee of the European Union*, Brussels, 30 June.

PAP, András (2008), *Ethnicity and Race-Based Profiling in Counter-Terrorism, Law Enforcement and Border Control*, Study for Policy Department C, Citizens’ Rights and Constitutional Affairs, Directorate General Internal Policies, European Parliament, PE 408.326, November.

PAYE, Jean-Claude (2004), *La fin de l’état de droit: La lutte antiterroriste de l’état d’exception à la dictature*, La Dispute, Paris.

PEDILARCO, Emanuele (2006), "Protezione dei dati personali: la Corte di giustizia annulla l’accordo Unione Europea - Stati Uniti sul trasferimento dei dati dei passeggeri aeri", *Diritto pubblico comparato ed europeo,* 2006, pp. 1225-1231.

PEERS, Steve (2006), *EU Justice and Home Affairs Law*, Second Edition, Oxford EC Law Library, Oxford: Oxford University Press.

--- (2008), *Proposed New EU Border Control Systems*, Briefing Paper, Civil Liberties, Justice and Home Affairs Committee of the European Parliament, June.

--- (2008), *Changing the institutional framework for EU Justice and Home Affairs law without the Lisbon Treaty*, Statewatch Analysis, July.

PÉREZ ASINARI, María Verónica (2004), "La regulación de los datos de tráfico en la Unión Europea: ¿Entre la seguridad y los derechos fundamentales?", Lexis Nexis, II(4), pp. 49-59.

PETERSEN, Karen Lund (2008), "Risk, responsibility and roles redefined: is counterterrorism a corporate responsibility?", *Cambridge Review of International Affairs*, 21(3), pp. 403-420.

PETROSINO, Anthony (2005), *The United States and Counterterrorism: History, Measures, and Lessons*, Report to the Research and Documentation Centre, Netherlands Ministry of Justice, 17 November.

POIARES MADURO (2008), *Opinion of Advocate General Poiares Maduro in Case C-524/06 (Heinz Huber v Bundesrepublik Deutschland)*, delivered on 3 April 2008.

POULLET, Yves (2002), « Pour une troisième génération de réglementations de protection des données », *Jusletter*, 3, October.

--- (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.

PORRETTO, Gabriele (2008), "The European Union, Counter□Terrorism Sanctions against Individuals and Human Rights Protection" in Miriam GANI and Penelope MATHEW (ed.), *Fresh Perspectives on the 'War on Terror'*, pp. 235-268.

Privacy International (PI) (2004), *Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection*, First Report on 'Towards an International Infrastructure for Surveillance of Movement', February.

QUILLERÉ-MAJZOUB, Fabienne (2005), "Les individus face aux systèmes d'information de l'Union Européenne: l'impossible équation du contrôle juridictionnel et de la protection des données personnelles au niveau européen?", *Journal du droit International*, 132(3), pp. 609-635.

PREUSS-LAUSSINOTTE, Sylvia (2006), « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *Cultures & Conflits*, 64, pp. 77-95.

RAGUSE Maren, Martin MEINTS, Owe LANGFELDT and Walter PEISSL (2008), *Criteria for privacy enhancing security technologies*, Privacy and Security (PRISE).

REDPATH, Jillyanne (2005), *Biometrics and International Migration*, International Migration Law, No. 5, International Organization for Migration (IOM), p. 16.

REES, Wyn (2006), *Transatlantic-Counter Terrorism Cooperation: The New Imperative*, Routdlege, New York.

RIGAUX, François (1992), *La vie privée: une liberté parmi les autres ?*, Larcier, Bruxelles.

RINGELHEIM, Julie (2006), *Processing Data on Racial or Ethnic Origin for Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?*, Center for Human Rights and Global Justice Working Paper, No. 13, NYU School of Law, New York.

ROTENBERG, Marc (2006), Marc Rotenberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, Social Science Research Network Working Paper Series, September.

RUBINSTEIN, Ira S., Ronald D. LEE & Paul M. SCHWARTZ (2008), "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", *The University of Chicago Law Review*, 75, pp. 261-285.

SAGAR, Rahul (2007), "On Combating the Abuse of State Secrecy", *The Journal of Political Philosophy*, 15(4), pp. 404-427.

SCHERMER, Bart Willem (2007), *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, SKIS Dissertation Series no. 2007-05, Leiden University Press.

SEIFERT, Jeffrey W. (2007), *Data Mining and Homeland Security: An Overview*, Congressional Research Service (CRS) Report for Congress, Updated January 18.

SKOKOWSKI, Paul (2002). *Can Biometrics Defeat Terror?,* paper presented at the National Security Forum, March.

SOLOVE, Daniel J. (2008), "Data Mining and the Security-Liberty Debate", *University of Chicago Law Review,* 74, pp. 343-360.

STANLEY, Jay and Barry STEINHARDT (2007), *Even Bigger, Even Weaker: The Emerging Surveillance Society: Where are we now?* , American Civil Liberties Union (ACLU).

STANTON, Jeffrey M. (2008), "ICAO and the biometric RFID passport", in Bennett, Colin J. and David Lyon (eds.) (2008), *Playing the identity card: surveillance, security and identification in global perspective*, Routledge, New York.

STEFANICK, Lorna (2007), "Outsourcing and transborder data flows: the challenge of protecting personal information under the shadow of the USA Patriot Act", *International Review of Administrative Sciences*, 73, pp. 531-548.

STERN, Jessica and Jonathan B. WIENER (2006), "Precaution Against Terrorism", *Journal of Risk Research*, 9(4), pp. 393-447.

SUDRE, Frédéric (ed.) (2005), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, Bruxelles.

SWIRE, Peter P. (2006), "Privacy and Information Sharing in the War on Terrorism", *Villanova Law Review*, 51, pp. 101-129.

TAIPALE, K. A. (2004), "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and The Lessons of King Ludd", Yale Journal of Law and Technology, 7(123), December 2004, pp. 125-201.

--- (2005), "The Trusted Systems Problem: Security Envelopes, Statistical Threat Analysis, and the Presumption of Innocence", *IEE Intelligent Systems*, 20(5), September-October, pp. 80-82.

--- (2007), *The Privacy Implications of Government Data Mining Programs*, Testimony before the US Senate Committee on the Judiciary, January 10.

TAPPEINER, Imelda (2005), "The fight against terrorism: The lists and the gaps", *Utrecht Law Review,* 1(1), pp. 97-125.

TEKOFSKY, Aliza (2006), *Security in European Union External Border Law*, CHALLENGE Working Paper, February 27.

TERRASI, Alfredo (2008), "Trasmissione dei dati personali e tutela della riservatezza: l'accordo tra Unione Europea e Stati Uniti del 2007", *Rivista di diritto internazionale*, 91(2), pp. 375-419.

TSOUKALA, Anastassia (2008), *Security, Risk and Human Rights*: *A Vanishing Relationship?*, CEPS Special Report, Centre for European Policy Studies, Brussels, September.

TRECHSEL, Stefan (2001), "The Relevance of the ECHR and the Charter of Fundamental Rights of the EU for the Area of Freedom, Security and Justice", in *Collegium* (2001), *Special Edition — Proceedings of the Conference: 'Integrated Security in Europe, a Democratic Perspective'*, No. 22, XII.2001, Bruges, pp. 90-118.

United Kingdom Delegation (2007), *Mobility, Security and Privacy*, Contribution to the Fourth meeting of the High Level Advisory Group on the future of EU Home Affairs Policies, December.

VAN KLINK, Bart Van and Oliver LEMBCKE (2007), "Can Terrorism Be Fought within the Boundaries of the Rule of Law? - A Review of Recent Literature in Political Philosophy", *Rechtsfilosofie & Rechtstheorie*, 36(2), pp. 9-26.

VILASAU, Mónica (2006), "La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad", *Revista d'Internet, Dret i Política*, No. 3.

WAEVER, Ole (2005), "The Constellation of Securities in Europe', in AYDINLI, Ersel and James N. ROSENAU, *Globalization, Security, and the Nation State*: *Paradigms in transition*, State University of New York Press, Albany, pp. 151-174.

WALDRON, Jeremy (2003), "Security and Liberty: The Image of Balance", *The Journal of Political Philosophy*, 11(2), pp. 191-210.

ZELLER, Judit, Nóra CHRONOWSKI, Tímea DRINÓCZI and Miklós KOCIS (2007), "Biometrics: Identification, Verification or Disintegration of Personal Identity?", *Central European Political Science Review*, 8(30), pp. 84-121.

Policy and legal documents

Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *Official Journal of the European Union*, L 183, 20/05/2004, pp. 84-85.

Agreement between the governments of the states of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, signed at Schengen, 14 June 1985.

Treaty establishing the European Community, OJ C 325, 24 December 2002.

Treaty on European Union, OJ C 325, 24 December 2002.

Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS 108, Council of Europe, Strasbourg, 28 January 1980, and Additional Protocol to the Convention regarding supervisory authorities and transborder data flows, ETS 181, Council of Europe, Strasbourg, 8 November 2001.

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, pp. 19–62.

Council Act of 26 July 1995 drawing up the Convention based on Article K.3d of the Treaty on European Union on the establishment of a European Police Office (Europol Convention), OJ C 316, 27.11.1995.

Council Act 95/C316/02 of 26 July 1996 drawing up the Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the use of information technology for customs purposes, OJ C 316, 27.11.1995, pp. 33-42.

Council Act of 12 March 1999 on the rules governing the transmission of personal data by Europol to third states and third bodies, OJ C 88, 30.03.1999.

Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, pp. 1-15.

Council Act of 28 February 2002 amending the Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third states and third bodies, OJ C 76, 27.03.2002, pp. 1-2.

Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States Department of Homeland Security, Bureau of Customs and Border Protection, *Official Journal of the European Union*, L 183, 20/05/2004, p. 83.

Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.06.2004, pp. 5-7.

Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 06.03.2002, pp. 1-13.

Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.08.2008, pp. 129-136.

Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, pp. 3–7.

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) and Statements made by certain Member States on the adoption of the Framework Decision, OJ L 190, 18.7.2002, pp. 1–20.

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 the European Union (2005), *A Strategy for the External Dimension of JHA: Global Freedom, Security and Justice*, 30 November.

--- *The European Union Counter-Terrorism Strategy*, 30 November.

--- (2008), *Note from the Presidency to COREPER on EU US Summit, 12 June 2008 – Final Report by EU-US High Level Contact on information sharing and privacy and personal data protection*, 28 May, Brussels.

Council of Europe Convention on the Prevention of Terrorism, CETS, No. 196.

Council of Europe Convention on Cybercrime, Treaty No. 18. It came into force on 7 January 2004, and Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189.

Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, pp. 1-10.

--- No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 62, 5.3.2002, pp. 1-5.

--- No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25.11.2004, pp. 1-11.

--- No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ, L 385, 29.12.2004, pp. 1-6.

--- No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, OJ L 53, 22.02.2007, pp. 1-14.

Council Resolution of 17 January 1995 on the lawful interception of telecommunications, OJ C 329, 4.11.1996, pp. 1–6.

Council of the European Union, General Secretariat (2002), *EU Schengen Catalogue, External borders control, removal and readmission: Recommendations and best practices*, February.

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

--- 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, pp. 1–16.

--- 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002, pp. 37-47.

--- 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 L 309 , 25/11/2005, pp. 15–36.

--- 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.

European Commission (EC) (2005), *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, COM(2005) 475 final, 4.10.2005, Brussels.

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

--- (2005), *Communication from the Commission: A Strategy on the external dimension of the Area of Freedom, Security and Justice,* COM(2005) 491 final, 12.10.2005.

--- (2005), *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.

--- (2007), *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.

--- (2007), *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.

--- (2007), *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.

--- (2008), *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, 13.2.2008, Brussels.

--- (2008), *Communication from the Commission to the Council and the European Parliament: Report on Implementation of the Hague Programme for 2007*, COM(2008) 373 final, 2.7.2008, Brussels.

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

European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 November) as amended by Protocol No. 11 and its Protocol of 1952.

High Level Advisory Group on the Future of European Justice Policy (2008*), Proposed Solutions for the Future EU Justice Programme*, June.

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*, Report, June.

Justice and Home Affairs Council (1999), *Action plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an Area of Freedom, Security and Justice*, adopted on 3 December 1998, OJ C 19, 23.1.1999, pp. 1-15.

Organisation for Economic Co-operation and Development (OECD) (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted in the form of a *Recommendation of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data* on 23rd September, Paris.

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, pp. 4-23.

Rules of procedure of the processing and protection of personal data at Eurojust, adopted by the college of Eurojust on 21 October 2004 and approved by the Council on 24 February 2005, OJ C 68, 19.3.2005. pp. 1-10.

Case law

European Court of Human Rights

Klass v. Germany, Judgement of September 1978, Series A N° 28.

Z v. Finland, Judgment of 25 February 1997, Reports of judgments and Decisions 1997-I.

Amann v. Switzerland, Application no. 27798/95, Judgement of 16 February 2000.

Rotaru v. Romania [GC], Application no. 28341/95, Judgement of 4 May 2000.

Association for European Integration and Human Rights and Ekimdzhiev, Application no. 62540/00, Judgement of 28 June 2007.

Saadi v Italy, Application no. 37201/06, Judgment of 28 February 2008.

Iliya Stefanov v. Bulgaria, Application no. 65755/01, Judgement of 22 May 2008.

Liberty and Others v. The United Kingdom, Application no. 58243/00, Judgement of 1 July 2008.

I v. Finland, Application no. 20511/00, Judgement of 17 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 and Court of First Instance

Bodil Lindqvist, C-101/01, Judgment of the Court of 6 November 2003, [2003] ECR I-12971.

European Parliament v. Council and Commission, Joined Cases C-317 and C-318/04, Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721.

Organisation des Modjahedines du peuple d'Iran v. Council and UK (OMPI), Case T-228/02, Judgement of the Court of First Instance (Second Chamber) of 12 December 2006.

Yassin Abdullah Kadi, Al Barakaat International Foundation v Council of the European Union, Commission of the European Communities, United Kingdom of Great Britain and Northern Ireland, Joined Cases C-402/05 P and C-415/05 P, Judgment of the Court (Grand Chamber) of 3 September 2008.

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

VII. List of Acronyms

ACLU	American Civil Liberties Union
AFSJ	Area of Freedom, Security and Justice
CEPS	Centre For European Policy Studies
CFSP	Common Foreign and Security Policy
CIS	Customs Information System
ECHR	European Convention on Human Rights and Fundamental Freedoms
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
FIDIS	Future of Identity in the Information Society
EC	European Community
EDPS	European Data Protection Supervisor
ESDP	European Security and Defence Policy
EU	European Union
ICAO	International Civil Aviation Organisation
IMS	Information Management Strategy
JHA	Justice and Home Affairs
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal
OMPI	Organisation des Modjahedines du peuple d'Iran
PETs	Privacy Enhancing Technologies

PNR	Passenger Name Records
PRISE	Privacy Enhancing Shaping of Security Research and Technology
REFGOV	Reflexive Governance in the Public Interest
SIS	Schengen Information System
TEC	Treaty of the European Community
TEU	Treaty of the European Union
UK	United Kingdom
UN	United Nations
US	United States
VIS	Visa Information System
VWP	Visa Waiver Program