Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable 5.1: Discussion paper on legal approaches to security, privacy and personal data protection

Authors: Gloria González Fuster, Serge Gutwirth (VUB), Ivan Székely, Erik Uszkiewicz (EKINT)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 January 2013
Submission date:	03 February 2013

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

Document history

Version	Date	Changes
1.0	02 February 2013	First version of deliverable

Contents

1 GENERAL INTRODUCTION

Security and privacy are typically regarded as polymorphic notions. They have a multiplicity of meanings, not only across different fields and academic disciplines, but also from a legal perspective – and even specifically as components of European Union (EU) law. In EU law, they now intersect with an additional (perhaps less contested, but possibly not less elusive) legal notion: personal data protection.

This paper considers legal conceptualisations of security, privacy and personal data protection and their interconnections in the EU. Its aim is to provide a basic reference on legal knowledge for the PRIvacy and Security MirrorS (PRISMS) project,[1] and to be directly relevant for the preparation of the survey (Work Package 9), as well as a first step towards further discussion on the project's legal research (Work Package 5).

[1] PRISMS project website: http://prismsproject.eu/.

2 SECURITY

The analysis begins by discussing security, first by providing an overview of its various legal meanings, and second a review of its concrete manifestations in EU law.

2.1 INTRODUCING SECURITY

Traditionally, there have been many legal conceptions of security. Modern national orders commonly identify security with "national security" (sometimes also labelled "internal security"), which can be broadly understood as the absence of threats that might weaken States, or their democratic constitutional framework.[2] For the purposes of discussing how it intersects with privacy and personal data protection, three main legal understandings of security can be brought to the fore:

- (national) security in the sense of State integrity, conceived as the preservation or upholding of the State and State's mechanisms.[3] This understanding, especially entrenched in German legal doctrine, envisages security as a sort of constitutional imperative, thus not requiring further formal recognition.[4] From this standpoint, security is directly concerned with protection the State, but serves indirectly also the protection of individual rights, as it safeguards the very possibility of their insurance (by safeguarding the rule of law);[5]

- (national) security as a possible ground justifying interference by the State with individual rights,[6] which, because of its restricting nature, requires formal recognition: for instance, the European Convention for Human Rights (ECHR) explicitly mentions national security as a legitimate purpose which can be used (under certain conditions) to restrict freedom of expression,[7] freedom of assembly and association[8] or the right to respect for private life.[9]

- (national) security as possible justification to refuse disclosure of information. In English common law, this particular possibility is embodied by the "public interest immunity" principle, which allows refraining from disclosing evidence to litigants where disclosure would be damaging to the "public interest".[10]

In the provisions of the ECHR, the term "security" also surfaces in the wording of Article 5, titled "Right to liberty and security". Here, however, the word has a peculiar meaning, intrinsically linked to the idea of physical liberty of the person, and the confinement of State power to coerce individuals through arbitrary arrest and detention.[11] In this context, security is

---

[2] Lageot, Céline (ed.), *Dictionnaire plurilingue des libertés de l'esprit. Étude de droit européen comparé*, Bruylant, Brussels, 2008, p. 664.
[3] Ibid, p. 668.
[4] Ibid.
[5] Ibid.
[6] Ibid, p. 670.
[7] Art. 10(2) ECHR.
[8] Art. 11(2) ECHR.
[9] Art. 8(2) ECHR.
[10] Lageot, op. cit, note 2, p. 672.
[11] Michaelsen, Christopher, "Balancing Civil Liberties Against National Security? A Critique of Counterterrorism Rhetoric", *University of NSW Law Journal*, Vol. 29, No. 1, 2006, p. 11.

thus to be understood as security of the person, regarded as potentially endangered by any deprivation of liberty. It is thus not possible to extract or infer from Article 5 of the ECHR a right to security (or right to ~~liberty and~~ security) in the sense of a general duty of the State to protect individuals from threats.[12]

Other European languages normally have various words and expressions that can be sometimes used as synonymous to the English "security". In French, for instance, a possible synonym is *sécurité*. The French version of ECHR (which is its authentic version, together with the English one) systematically uses *sécurité nationale* as equivalent to "national security". The ECHR, however, also uses sometimes the French *sécurité* as synonym of another English word – "safety", e.g., in Article 9(2), when establishing that freedom to manifest one's religion or beliefs can be restricted on grounds of *sécurité publique* (in English, "public safety"). The same ECHR, furthermore, also uses as equivalent to the English "public safety" a different French expression: *sûreté publique.*[13]

2.2 Security and EU law

The elasticity of the word 'security', as well as the various nodes of meaning it can denote, are mirrored in the various inscriptions of the term coexisting in EU law – both in its primary and its secondary law. This section puts forward some of the most significant.[14]

2.2.1 Security as in the Common Foreign and Security Policy

A first common usage of the term occurs in relation with EU's external action. One of the EU's general objectives in "its relations with the wider world" is to contribute to security.[15] For this purpose, the EU has its Common Foreign and Security Policy,[16] covering "all areas of foreign policy and all questions relating to the *Union's security*".[17] According to the Preamble to the Treaty on European Union (TEU), the implementation of the EU Common Foreign and Security Policy includes the progressive framing of a common defence policy, thereby reinforcing the European identity and its independence "in order to promote peace, *security*[18] and progress in Europe and in the world". The policy is conducted by the High Representative of the Union for Foreign Affairs and Security.[19]

The Treaties oblige the EU to pursue policies and actions in order to, among other things, "safeguard its values, fundamental interests, *security*,[20] independence and integrity",[21] and

---

[12] Macovei, Monica, "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,* n° 5, Council of Europe, 2004, p. 6.
[13] Arts. 8(2) and 10(2) ECHR. *Sûreté* is the term used in the French version of Art. 5 ECHR*: droit à la liberté et à la sûreté*.
[14] It is, however, not an exhaustive account of all manifestations of security in EU law. Regarding primary law, other usages include security as in social security (Arts. 48, 153(1)(c), 153(4), 156 TFEU), and, in the context of EU's energy policy, as security of energy supply (Art. 194(1)(b) TFEU).
[15] In addition to contributing to peace, the sustainable development of the Earth, solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter (Art. 5 TEU).
[16] Formerly known as the second pillar.
[17] Art. 24 TEU.
[18] Emphasis added.
[19] Art. 18(2) TEU.
[20] Emphasis added.

"preserve peace, prevent conflicts and strengthen *international security*,[22] in accordance with the purposes and principles of the United Nations Charter, with the principles of the Helsinki Final Act and with the aims of the Charter of Paris, including those relating to external borders".[23] A specific component of the Common Foreign and Security Policy is the "common security and defence policy", the aim of which is to provide the EU with an operational capacity drawing on civilian and military assets.[24]

All of these references engage simultaneously two basic connotations of security: security as (the EU's own) stability and (international) security as the sum of (and the condition for) all States' security.[25] In this context, security integrates defence, although it is not reduced to it. It can be described as associated with the security of the EU, the security of its Member States, and the security of third countries in general.

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

A second significant usage of the term security happens in relation with EU's Area of Freedom, Security and Justice, which, according to the Preamble to the TEU, as among its main objectives the insurance of the "safety and security" of the peoples of the Member States. Launched in 1997 by the Treaty of Amsterdam, the Area of Freedom, Security and Justice rapidly produced a remarkable volume of law,[26] notably due to the fact that the same Treaty incorporated into the EU the Schengen Agreements, which had been signed outside its framework.

The TEU describes the Area of Freedom, Security and Justice as an area "without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime".[27] The Treaty on the Functioning of the EU (TFEU) further details its features,[28] and specifies that, in its name, the EU "shall endeavour to ensure a high level of *security*[29] through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws".[30] The grouping of all these separate elements as serving objectives of security has been the object of much controversy.[31]

In relation to this Area of Freedom, Security and Justice, the EU and Member States have shared competence.[32] Their respective realms of competence are delineated in EU primary

---

[21] Art. 21(2)(a) TEU.
[22] Emphasis added.
[23] Art. 21(2)(c) TEU.
[24] Art. 42 TEU.
[25] In the understanding that, as the 1990 Charter of Paris for a New Europe words it, security is indivisible.
[26] Walker, Neil, "In search of the Area of Freedom, Security and Justice: A Constitutional Odyssey", in Neil Walker (ed.), *Europe's Area of Freedom, Security and Justice*, Oxford University Press, Oxford, 2004, p. 3.
[27] Art. 3(2) TEU.
[28] Art. 67(2) TFEU.
[29] Emphasis added.
[30] Art. 67(3) TFEU.
[31] See, for instance: Anderson, Malcolm, and Joanna Apap, *Changing Conceptions of Security and their Implications for EU Justice and Home Affairs Cooperation*, The Centre for *European* Policy Studies (CEPS) Policy Brief, No. 26, October 2002.
[32] Art. 4 TFEU.

law mobilising notions such as internal security or national security, for which no precise definition is provided. The TEU sets out that security as an essential State function, and that it includes the ensuring of the territorial integrity of the State, maintaining law and order and safeguarding *national security*".[33]

The TFEU foresees that EU-level operational co-operation on *internal security*[34] is to be promoted and strengthened,[35] even though the establishment of the Area of Freedom, Security and Justice must at the same time "not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of *internal security*".[36] Substantiating some limits of EU action, the EU Court of Justice is excluded from the review of "the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State" and the exercise of Member States' responsibilities with regard to the maintenance of law and order and the safeguarding of *internal security*.[37] National security is portrayed as "the sole responsibility of each Member State,[38] which does not preclude the fact that Member States are free to organise possible co-operation and co-ordination between Member States in relation to safeguarding *national security*.[39]

The security pursued through the EU Area of Freedom, Security and Justice might in a sense be regarded as a European security, notably because this area aims to contribute to a high level of security across the EU. Because it touches upon internal security, the Area of Freedom, Security and Justice has been described as generating a "European system of internal security",[40] or as conferring a European dimension to the notion of internal security.[41] In this field, nevertheless, security is internally divided into facets that are indeed common, shared, jointly developed or others that remain the exclusive competence of Member States (sometimes, but not systematically, referred to as national security). Therefore, security in the Area of Freedom, Security and Justice is far from being exclusively about European security; it concerns also various facets of Member States' national and internal security, "Europeanised" to a certain extent.

The notion of security enacted by the Area of Freedom, Security and Justice is, furthermore, partially adjacent to the security sought with the development of the Common Foreign and Security Policy: the major locus where they encounter each other are external borders, which are alluded to by the Treaties in both contexts.

[33] Second sentence of Art. 4(2) TEU. Emphasis added.
[34] Emphasis added.
[35] Art. 71 TFEU.
[36] Art. 72 TFEU, which partially replaced the former art 33 TEU (on this provision, see: Delarue, Jean Marie, "Titre VI Dispositions relatives à la coopération policière et judiciaire en matière pénale", in Isabelle Pingel (ed.), *Commentaire article par article des traités UE et CE : de Rome à Lisbonne,* Helbing Lichtenhahn, Bâle, 2010, p. 159.
[37] Art. 276 TFEU. Emphasis added.
[38] Art. 4(2) TEU.
[39] Art. 73 TFEU.
[40] Tuori, Kaarlo, "European Security Constitution", in Martin Scheinin (ed.), *Law and Security: Facing the dilemmas*, EUI Working Papers Law 2009/11, European University Institute (EUI), Department of Law, 2009, p. 4.
[41] Monar, Jörg, "Préface", in Pierre Berthelet, *Le paysage européen de la sécurité intérieure,* P.I.E. Peter Lang, Brussels, 2009, p. 23.

2.2.3 *Security as a limitation of EU primary law*

These occurrences of the word "security" do not exhaust all of its manifestations in EU primary law. A special Article of the TFEU, i.e., Article 346, establishes two important boundaries to the general scope of the EU Treaties' provisions. First, it foresees that no Member State can be obliged to supply information the disclosure of which "it considers contrary to the essential interests of *its security",* [42] a provision closely linked to the idea of security as grounds for the public interest immunity described above. Second, Article 346 of the TFEU also sets out that any Member State may take the measures "it considers necessary for the protection of the essential interests of *its security*"[43] in connection with arms, munitions and war material.[44]

Here, the possessive "its" definitely refers to the Member State that makes use of its prerogative to retain information, or to take certain measures on war material. From this standpoint, security clearly refers to the security of the Member State.

2.2.4 *Public security as a ground to restrict free movement*

An additional, and no less significant, acceptation of security emerges through its usage in the idiom "public security". The notion of public security is repeatedly advanced by the Treaties as constituting a legitimate ground to interfere with fundamental freedoms of the internal market. Public security is identified as a legitimate ground to restrict quantitatively imports and exports (as well measures having equivalent effect) between Member States, which are in principle prohibited,[45] as a legitimate ground to limit the freedom of movement for workers within the EU,[46] to justify provisions foreseeing a special treatment for foreign nationals relative to their right to establishment in the Member State of their choice,[47] and to justify restrictions by Member States on the movement of capital.[48]

In this frame, security is qualified as public, and thus in a sense it appears to be concerned with the security of the general population, but constitutes nonetheless a ground that allows Member States to interfere with freedoms that, in EU law, have some qualities of rights – and, thus, they can be enacted by Member States against claims by individuals. Security materialising here is the security of the population as perceived by Member States, as opposed to the EU's internal market and the individual's prerogatives.

2.2.5 *Security as in network and information security and cyber-security*

Turning now to EU secondary law, a noteworthy usage of the term security occurs through the idiom "information security", and more concretely as an element of what is labelled as network and information security (sometimes referred to as NIS). Such network and information security is concerned with protecting against disruption of information and communication technology systems, infrastructures and services, including the Internet.[49] In

[42] Art. 346(1)(a) TFEU. Emphasis added.
[43] Emphasis added.
[44] Art. 346(2)(a) TFEU.
[45] Art. 36 TFEU, in conjunction with Arts. 34 and 35 TFEU.
[46] Art. 45(3) TFEU. See also Art. 202 TFEU.
[47] Art. 52 TFEU.
[48] Art. 65(1)(b) TFEU.
[49] Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009/C 321/01), OJ C 321, 29.12.2009, Arts. 1 and 2.

2004, a key agency in this field was established as the European Network and Information Security Agency (ENISA).[50] Since then, the EU's approach to network and information security has been much debated, resulting notably in a 2009 Council Resolution hinting that a rethinking of the European approach is needed.[51]

Discussions on the security of information networks are increasingly linked to the notion of cyber security, a term recently embraced by the European Commission to present its approach on vital information and communication infrastructures.[52] In these contexts, security alludes globally to the protection of information carried out through networks and of the networks themselves.

2.2.6 Security protecting classified information

Security can as well be used in the context of the security rules applying to protect classified information.[53] The EU applies to information an EU security classification, which classifies different types of information according to the degrees of prejudice that their disclosure could provoke. Depending on how information is classified, different security measures apply. These measures can be personnel security,[54] physical security,[55] and industrial security measures.[56] When classified information is handled through communication and information systems, procedures of information assurance will apply, with the objective of ensuring that the information conveyed is duly protected.[57] Acts contrary to the applicable rules might constitute a breach of security.[58] From this perspective, security is a property of information.

---

[50] European Parliament and the Council, Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), OJ L 077, 13.03.2004.

[51] Council Resolution of 18 December 2009, op. cit., n. 49.

[52] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: Achievements and next steps: towards global cyber-security, COM(2011) 163 final, Brussels, 31.3.2011.

[53] Key instrument is Council Decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU), OJ L 141, 27.5.2011.

[54] Ibid., Art. 7.

[55] Ibid., Art. 8.

[56] Ibid., Art. 11.

[57] Ibid., Art. 10.

[58] Ibid., Art. 13.

3 PRIVACY

There are numerous legal conceptions of privacy, in particular, regarding its scope, its foundations and its nature. In EU law, its conceptualisation is closely intertwined with the conceptualisation of the respect for private life, an expression for which the word privacy is often used as a substitute – not only in the literature, but also by the legislator.

3.1 INTRODUCING PRIVACY (AND PRIVATE LIFE)

3.1.1 A basic map for privacy

An overview of literature on privacy reveals the possibility to map multiple acceptations of the word "privacy" by dividing them into a few basic categories, corresponding to different meanings of the adjective "private", from which the noun privacy derives. Schematically, it could be said that the most common conceptions of privacy correspond either:

1. to an understanding of privacy as protecting what is envisaged as private as opposed to public;[59] the meanings of public in their turn are also multiple, so there are many ways to read private as opposed to public and, notably:

    a. envisaging public as referred to governmental authority, or the community;[60] private is thus read as not official, or not pertaining to the State or society in general, but related to family life, or to the home; a peculiar drift in this conception of the relation between private and public is to describe the existence of various spheres corresponding to different degrees of connexion to the polity (such as an intimate sphere, a private sphere, a social sphere, a public sphere);[61] from this standpoint, in any case, a private life would be a life which is not the public life of official obligations, community decisions or general social interactions.

    b. envisaging public as referred to what is shared, exposed, common, open to the public; private is thus read as related to a space not open to the public; this includes what is unexposed, hidden, confidential, concealed, secret,[62] generally out of reach; from this perspective, a private life would be a life which is not public in the sense that it is generally not disclosed, but also to the possibility of being let alone, or even to a *ius solitudinis*;[63]

2. to an understanding of privacy as protecting what is private, not in the sense as opposed to public, but in the sense of individual, personal, unique or one's own: from

[59] This opposition between private and public can be pictured as two distinct zones separated by a boundary, or as spreading through a continuum that would link privacy to publicity (Nippert-Eng, Christena, *Islands Of Privacy*, The University of Chicago Press, Chicago, 2010, p. 4).
[60] Duby, Georges, "Ouverture", in Philippe Ariès and Georges Duby (eds.), *Histoire de la vie privée : 2. De l'Europe féodale à la Rennaissance*, Editions du Seuil, Paris, 1999, p. 18.
[61] See notably Arendt, Hannah, *The Human Condition*, Chicago, The University of Chicago Press, Chicago, 1998, p. 38; Habermas, Jürgen, *The Structural Transformation of the Public Sphere*, Polity, Cambridge, 1992, p. 55.
[62] Duby, op. cit., n. 60, p. 18.
[63] Pérez Luño, Antonio Enrique, *Derechos humanos, estado de derecho y constitución (10a edición)*, Tecnos, Madrid, 2010, p. 339.

this view, to claim respect for private life is to affirm everybody's right to live as they choose, as opposed to controlled, alienated, estranged from their selves.

This classification only maps out indicatively possible perspectives on privacy. Generally, conceptions of privacy are based simultaneously on a number of these elements. It can be easily argued, for instance, that for individuals to be able to effectively live freely, they need to be assured that some facets of their life will remain undisclosed, for instance, through the concomitant legal notions of the inviolability of the home or confidentiality of communications.

Conversely, some conceptions warn against granting an excessive emphasis to some of the above-mentioned understandings of private. In this sense, some scholars have advanced the idea that for individuals to be effectively individuals, they cannot be detached from what is social and public.[64] To enjoy a private life (in the sense of a life of their own), individuals would need more than a merely private life.

There is still an additional key conception of privacy requiring special mention: privacy envisaged as an individual's control over information about them.[65] This particular meaning surfaced in the United States at the end of 1960s. It is sometimes labelled privacy of information,[66] information privacy[67] or informational privacy,[68] but also often just privacy.[69] The condition of relevant information as being about the individuals concerned eventually lead to the usage of the expression personal information: privacy can thus be described as individuals' control over their personal information. The adjective "personal" in "personal information" under this information privacy perspective refers, therefore, to information related to a particular individual. The adjective personal, however, is sometimes read even in this context as private, generating much ambiguity on the nature of the information protected by such (informational) privacy.

3.1.2 *Foundations and nature of privacy*

The grounds on which are rooted existing conceptions of privacy are varied. The vision of privacy as primarily concerned with ensuring that individuals can live their own lives is sometimes linked to an identification of privacy with freedom: privacy has notably been described as the fortress of personal freedom,[70] what grants freedom to establish an individual path in life, and the potential to resist any interference with this freedom,[71] or individual

---

64 German sociologist Norbert Elias, for example, emphasised that what transforms children into specific, distinct individuals are their relations with others, and that the different structures of interiority shaping individual consciousness are precisely determined by the outside world (Elias, Norbert, *La société des individus*, Librairie Arthème Fayard, Paris, 1991, pp. 58 and 65.

65 Westin, Alan F., *Privacy and freedom*, Atheneum, New York, 1970, p. 7.

66 Rössler, Beate, "Privacies: An Overview", in Beate Rössler (ed.), *Privacies*, Stanford University Press, Stanford, 2004, p. 4.

67 Noting that information privacy is often contrasted with decisional privacy: Solove, Daniel J., Marc Rotenberg and Paul M. Schwartz, *Information privacy law*, Aspen Publishers, New York, NY, 2006, p. 1.

68 Turkington, Richard C., and Anita L. Allen, *Privacy Law: Cases and Materials*, West Group, St. Paul, MN, 1999, p. 75.

69 As in Westin, op. cit., n 65, or the US Privacy Act of 1974.

70 Sofsky, Wolfgang, *Defensa de lo privado: Una apología*, Pre-textos, Valencia, 2009, p. 53.

71 Gutwirth, Serge, *Privacy and the information age*, Rowman & Littlefield Publishers, Oxford, 2002, p. 2.

freedom par excellence.[72] From this perspective, there is a tendency to situate privacy's roots in the Enlightenment and in the works of early thinkers of political liberalism.[73]

But the idea of living one's own life can also be connected to the notion of human dignity. This view's basic assumption is that it is inherent to human condition to develop freely and that, therefore, human dignity presupposes the acknowledgement of self-determination.[74] Here, individuality is coupled with the full development of the personality,[75] and this is associated with the notion of personhood, or the quality of being a human being. This position has been especially popular in German doctrine, as in Germany privacy protection is granted by the Federal Constitutional Court through a joint reading of the right to dignity and on the free development of personality, as recognised in the German Basic Law. The right construed through such joint reading of dignity and the free development of personality has, however, also been overtly described as "a general right to freedom of action",[76] which in a way reinstates freedom as a key element of privacy foundations, even in German legal thought.

Privacy, full development of the personality and personhood are sometimes also connected to the notion of identity.[77] As a matter of fact, this word has several meanings that appear to be directly relevant to privacy; in particular, it can refer to identity as personality, but also to the idea of identification (or individualisation).[78]

Ultimately, it could be asserted that there exist basically two possible ways to attempt to legally delimit and define privacy: either inductively or deductively. Inductively, one can try to consider all occurrences when privacy is brought to the fore, and attempt to infer from there what is privacy. Deductively, one could examine *why* is privacy needed in constitutional democratic societies and, from there, investigate what must be privacy's nature. A brilliant illustration of an inductive effort are Daniel J. Solove's latest attempts to apprehend privacy – in this case, applied concretely to US legal reality.[79] For him, the focal point for a theory of privacy should be the problems (privacy) law should address.[80] From a different standpoint, examples of deductive efforts seemingly tend to emphasise the idea that privacy must be connected to the construal of the modern democratic State, as a freedom (or the freedom by default) that marks its boundaries.[81] From this perspective, the focal point of any theory of privacy would be more accurately described as the problems that law should not address – but rather leave to the individual.

3.2 PRIVACY IN EU LAW

In EU law, the term privacy is used primarily to refer to the right to respect for private established by Article 8 of the ECHR. This is a phenomenon peculiar to EU law, as actually

[72] Rigaux, François, *La vie privée, une liberté parmi les autres?*, Larcier, Brussels, 1992, p. 9.
[73] Ruiz Miguel, Carlos, *La configuración constitucional del derecho a la intimidad,* Universidad Complutense de Madrid, Madrid, 1992, p. 7.
[74] Pérez Luño, op. cit., n. 63, p. 324.
[75] Edelman, Bernard, *La personne en danger*, Presses Universitaires de France, Paris, 1999, p. 509.
[76] Alexy, Robert, *A Theory Of Constitutional Rights*, Oxford University Press, London, 2010, p. 223.
[77] Rodotà, Stefano, *La vita e le regole: Tra diritto e non diritto*, Feltrinelli, Milan, 2009, p. 22.
[78] Bioy, Xavier, "L'indetité de la personne devant le Conseil constitutionnel", *Revue Française de Droit Constitutionnelle*, Vol. 1, No. 65, 2006, p. 74.
[79] Solove, Daniel J., *Understanding Privacy,* Harvard University Press, Cambridge, MA,, 2008.
[80] Ibid., p. 75.
[81] See, for instance: Rigaux, op. cit., n 72.

Article 8 of the ECHR itself does not use the word privacy. In the words of this provision, "(e)veryone has *the right to respect for his private and family life*,[82] his home and his correspondence". The European Court of Human Rights, based in Strasbourg and the ultimate interpreter of the ECHR, has over the decades resisted the use of the term privacy to allude to the rights enshrined in Article 8 of the ECHR.

EU secondary law, however, portrays Article 8 of the ECHR as establishing a right to privacy. This is crucially the case in Directive 95/46/EC (the Data Protection Directive),[83] which, in addition, ranks precisely such privacy among the key objectives pursued by its provisions.[84] The word privacy is also widely used in legislation developing and complementing the Data Protection Directive, such as, for instance, Directive 2002/58/EC (the e-Privacy Directive).[85]

The EU Charter of Fundamental Rights[86] mirrors Article 8 of the ECHR with a provision not using the word privacy but preferring, instead, the conventional respect for private and family life: the EU Charter's Article 7 establishes indeed that "(e)veryone has the right to respect for his or her private and family life, home and communications".[87] As the rights contained in the Charter's Article 7 clearly correspond to those comprised by Article 8 of the ECHR, they need to be interpreted as having the same meaning and scope – as mandated by the Charter's horizontal provisions.[88] Thus, both from a reading of Directive 95/46/EC and from the EU Charter it must be deduced that to determine what is 'privacy' in EU law it is pivotal to investigate what is the right to 'respect for private life' in the Strasbourg system. As a matter of fact, already long before the proclamation of the EU Charter the EU Court of Justice had already been integrating into its case law Strasbourg's case law on the right to respect for private life.[89]

The European Court of Human Rights has repeatedly maintained that the right to respect for private life recognised in Article 8 of the ECHR needs to be interpreted by recognising that 'private life' is a broad notion. Arguing that it 'does not consider it possible or necessary to attempt an exhaustive definition' of the notion, it has nevertheless emphasised that it would be 'too restrictive' to limit its scope of protection to an 'inner circle' in which individuals may live their lives without developing relationships with others,[90] and has stressed that there is no reason of principle to sustain that the notion of 'private life' shall be taken to exclude professional or business activities.[91] With these observations, it has significantly minimised

[82] Emphasis added.
[83] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 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. See notably Recital 10.
[84] Art. 1(1) of Directive 95/46/EC.
[85] European Parliament and the Council, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002.
[86] Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010.
[87] The second paragraph of Art. 8 ECHR is regarded as covered by Art. 52(1) of the Charter, which specifies that limitations to the exercise of EU fundamental rights are possible if, subject to the principle of proportionality, they are necessary and genuinely meet the objectives of general interest of the EU – which can certainly include security – and if they are provided for by law and respect the essence of those rights and freedoms.
[88] Concretely, Art. 52(3) EU Charter.
[89] For an early instance, see: Judgment of the Court of 5 October 1994, *X v Commission of the European Communities*, Case C-404/92 P, para 17 ('The Court of Justice has held that the right to respect for private life, embodied in Article 8 of the EHRC and deriving from the common constitutional traditions of the Member States, is one of the fundamental rights protected by the legal order of the Community').
[90] *Niemietz v Germany,* Judgement of the Court of 16 December 1992, Series A no. 251-B, para 29.
[91] Ibid.

the possible relevance of the private/public dichotomy for determining the scope of 'private life', and tended instead to conceive of the right to respect to private life as protecting the freedom to live a life of one own.

The notion of 'private life' has been notably extended through its contiguity with the other rights mentioned in Article 8(1) of the ECHR. The Strasbourg Court has for instance maintained that telephone, fax and e-mail communications are covered by the notions of 'private life' and 'correspondence',[92] and thus not solely through the latter. And under this broad notion of 'private life', the Strasbourg Court has included the protection of individuals against the processing of data related to them.[93] Taking the wording of Article 8 of the ECHR as a starting point, the Court has had recourse to ideas that originated in data protection law both to broaden the scope of Article 8(1) ECHR, and to refine its assessment on the possible lawfulness of interferences as per Article 8(2) ECHR. In EU law, however, this protection against data processing through Article 8 of the ECHR has been flanked since 2000 by the recognition of another right, the EU fundamental right to the protection of personal data.

[92] See, for instance, *Liberty and Others v. The United Kingdom*, Judgment of 1 July 2008, Application no. 58243/00, Strasbourg, para 56.

[93] See among others: *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116; *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II; *Rotaru v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V. See also De Hert, Paul, and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in Serge Gutwirth, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 3-44.

4 PERSONAL DATA PROTECTION

Until relatively recently, there was some reluctance in the literature to consider personal data protection as a notion fully separate from privacy, and thus to engage in any discussion of its conceptualisation as an autonomous legal concept. The recognition in 2000 by the EU Charter of a fundamental right to the protection of personal data (in Article 8) different from the right to the respect for private life (in Article 7) was a major stimulus to reconsider such position, even though the legacy of decades of envisioning personal data protection primarily through the frame of privacy is still palpable in most of the discussion around it.

4.1 INTRODUCING PERSONAL DATA PROTECTION

The linkage between personal data protection and privacy had been solidifying in Europe through the decades due to, among other factors, the multiplicity of meanings of the word privacy. The term privacy, as noted above, can crucially be read both:

> a) as synonymous with the right to respect for private life enshrined by Article 8 of the ECHR, which has been construed in the case law of the European Court of Human Rights as integrating the protection of individuals against the processing of data about them: thus, privacy is sometimes read as including personal data protection; and
>
> b) as in informational privacy, regarded as the US (and global) way of addressing the regulation of the processing of data about individuals, which has many historical connections with European personal data protection: thus, privacy is also sometimes advanced as a (reasonably comparable) alternate to personal data protection.

Instrumental to the consolidation of the linkage between privacy and personal data protection in Europe was the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, signed in 1981, and known as Convention 108. Convention 108 was the first international instrument recognising data protection, which the instrument described as respect for individuals' rights and fundamental freedoms, and in particular, the right to *privacy*,[94] with regard to automatic processing of personal data relating to them.[95] Therefore, Convention 108 not only put forward internationally the legal notion of data protection,[96] but also emphasised that this notion served the right to privacy – which it already equated with the right enshrined in Article 8 of the ECHR.

The prominence given to the word privacy in Convention 108 could be partially explained by the fact that, despite being an instrument of the Council of Europe, Convention 108 was not a European-only enterprise: it was negotiated with the participation of representatives from various non-European countries, including the US, and of the Organisation for Economic Co-operation and Development (OECD), which was preparing simultaneously what were to become its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. US law and doctrine have never accepted the usage of the idiom *data protection* to refer

---

[94] In the French version (the official version in addition to the English version): '*et notamment de son droit à la vie privée*' (Art. 1, Convention 108).
[95] Art. 1, Convention 108.
[96] As such, the idiom had surfaced in English as a loan translation of the German *Datenschutz*.

to what they call (informational) privacy, whereas international organisations had already started to intermittently adopt the word *privacy*.[97]

The impact of Convention 108 and of its construal of data protection as serving in particular privacy spread in three major directions. First, it rendered easier for the European Court of Human Rights to interpret the right to respect to private life enshrined in Article 8 of the ECHR as including elements of personal data protection. Since then, the Strasbourg Court has repeatedly referred to Convention 108 when developing its case law on the issue of data processing.

Second, it supported the propagation across European national legal orders of the idea according to which there existed effectively a link between data protection laws and the insurance of privacy, and that such connection was special, and more significant than the bond between data protection and any other human right. Until then, the link was inexistent, or at least invisible, in data protection laws, and was just a link in other instances: the French *loi informatique et libertés* of 1978,[98] for example, identified as its key priority to ensure that the developments of computers did not interfere with privacy (*vie privée)* as well as with human identity (*l'identité humaine*), human rights (*droits de l'homme*) and individual or public freedoms (*libertés individuelles ou publiques*). Generally, European data protection laws tended to refrain from specifying formally the interests or values they served.[99] But Convention 108 obliges ratifying countries to adopt laws substantiating its provisions and, in doing so, many transferred into their legal systems the data protection / privacy linkage. In some cases, the very naming of such privacy to which data protection was attached appeared to be a challenge, and some European countries created new words to reflect what was perceived as a new reality.[100]

Third, and finally, Convention's 108 provision granting a privileged status to privacy in data protection law was imported almost word for word into EU law. The key instrument of EU personal data protection law, Directive 1995/46/EC, thus establishes since 1995 that "Member States shall protect the fundamental rights and freedoms of natural persons, and *in particular their right to privacy*[101] with respect to the processing of personal data".[102] Based on this wording, the EU Court of Justice later built case law that further emphasised that personal data served privacy – understood as Article 8 of the ECHR. And, as Member States transposed the instrument into their legal systems, the linkage spread further and consolidated across Europe.

Taking this into account, it is understandable that many conceptualisations of (personal) data protection in the literature assume that it has a special connection with privacy.[103] Until 2000, it was relatively common to maintain that the right to privacy had evolved through the years, and had progressively come to include the protection of personal data, which was thus one of

---

[97] See, in particular, Council of Europe, Recommendation (68) 509 on Human Rights and Modern Scientific and Technological Developments, adopted by the Assembly on 31st January 1968 (16th Sitting).
[98] *Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978.*
[99] Bygrave, Lee A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague, London, New York, 2002, p. 8.
[100] The Spanish law, adopted in 1992, introduced into Spanish the word *privacidad* (as a loan translation from the English privacy) (Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal).
[101] Emphasis added.
[102] Art. 1(1) of Directive 95/46/EC.
[103] See, for instance, Flaherty (1989), op. cit., pp. xiii and xiv.

its components. Privacy's modernisation (and expansion) commonly occurred at the expense of what were described as older visions of (reduced) privacy.[104] The new privacy, characterised by its integration of personal data protection, was described as offensive, which suggested that it was originally strictly defensive.[105]

Nowadays, it is increasingly usual to depict the right to privacy and the right to the protection of personal data as separate notions.[106] And this leads to the question of what is the specific nature of personal data protection – an issue on which there is, as a matter of fact, no consensus. Existing understandings of the European right to the protection of personal data typically oscillate between two poles: one approach envisages the right as representing, in substance, an overall prohibition against the processing of personal data (which could be labelled a *prohibitive* notion), whereas another view conceives of the right as constituting instead, in essence, a series of rules applying to the processing of personal data, regulating and limiting such processing but not forbidding it [or as a *permissive* (or regulatory) notion].

Constructing a picture of privacy and personal data protection as two distinct entities sometimes also highlights the similarities between them. This understanding often sustains the vision of personal data protection as a general prohibition of the processing of data about individuals.[107] Sometimes, however, scholars and jurists have put forward a conception of personal data protection as essentially divergent from privacy. An exemplar of such a characterisation is the categorisation of privacy and data protection in terms of *opacity v. transparency* tools. From this perspective, the basic feature of privacy would be that it aims to protect individuals by saturating their opacity in front of power, drawing normative limits,[108] whereas the key feature of data protection would be that its aim is to reinforce the transparency of power's exercise by organising and regulating the ways any processing of personal data must be carried out in order to remain lawful.[109] Privacy and data protection would thus by default serve divergent rationales, even if they can be punctually coincidental.[110] Data protection as such would not aim at protecting against data processing, but only from some unlawful data processing practices.[111] This view appears to fit what some have called a *permissive* notion, in the same way as other depictions of data protection as offering positive and dynamic protection (at variance with the negative and static protection of privacy).[112]

---

[104] See, for instance: Pérez Luño, op. cit., p. 336. This trend persists in non-European literature; see, for instance: Schulhofer, Stephen J., *More essential than ever: The Fourth-Amendment in the Twenty-First Century*, Oxford University Press, Oxford, 2012, p. 8.

[105] See, for instance, Poullet, Yves "Pour une troisième generation de réglementation de protection des données" in María Verónica Pérez Asinari and Pablo Palazzi (eds.), *Défis du droit à la protection de la vie privée: perspectives du droit européen et nord-américain / Challenges of Privacy and Data Protection Law: Perspectives of European and North American Law*, Bruylant, Brussels, 2008, pp. 297-365.

[106] See, for instance, Hustinx, Peter J., "Data Protection in the European Union", *P&I*, 2005, pp. 62-65. www.edps.europa.eu/.../EDPS/.../05-04-21_Data_Protection_EN.pdf

[107] Blume, Peter, "Lindqvist Revisited – Issues concerning EU data protection law", in Henning Koch (ed.), *Europe: the new legal realism: essays in honor of Hjalte Rasmussen*, DJØF, Copenhagen, 2010, p. 86.

[108] De Hert, Paul, and Serge Gutwirth, "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power", in Erik Claes, Antony Duff and Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Intersentia, Antwerp-Oxford, 2006, pp. 61-104; and Gutwirth, Serge, "Biometrics between opacity and transparency", *Annali dell'Istituto Superiore di Sanità*, Vol. 43, No. 1, 2007, pp. 61-65.

[109] Ibid., p. 62.

[110] Ibid., p. 63.

[111] De Hert and Gutwirth, op. cit., 2009, n, 93, p. 3.

[112] Rodotà, Stefano, "Data Protection as a Fundamental Right", in Serge Gutwirth, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, 2009, pp. 77-82.

4.2 PERSONAL DATA PROTECTION AND EU LAW

The current status of personal data protection in EU law is very much indebted to the changes brought about by the Lisbon Treaty in December 2009. Two developments are of major relevance: the enshrinement of the right to the protection of personal data as a EU fundamental right and the incorporation into the Treaties of a new legal basis for the rules developing such right.

4.2.1 A new EU right: right to the protection of personal data

The Lisbon Treaty gave legally binding force to the Charter of Fundamental Rights of the EU, originally proclaimed in 2000. Article 8 of the EU Charter establishes a right to the protection of personal data, which reads as follows:

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

There are some discrepancies in the doctrine on the interpretation of the Charter's Article 8, which actually mirror and sustain divergent conceptions of the essence of personal data protection. Crucially, there are discrepancies on what constitutes the right's content, what amounts to a limitation of the right and which limitations are lawful.

It is commonly understood that, as a general rule, the Charter defines in its first Articles the content of rights and principles, whereas guidance on their interpretation and on the determination of lawful limitations appears in the Charter's final general provisions. Following this line of thinking, Article 8 of the Charter would establish a right, while the requirements applicable to lawful limitations of the right would be described in the Charter's horizontal provisions (in particular, the Charter's Article 52).

Some argue, however, that Article 8 of the Charter should be regarded as an exemption to the mentioned general rule: its content would need to be interpreted as being constituted solely by Article 8(1), according to which everyone has the right to the protection of their data, and Articles 8(2) and 8(3) would describe the lawful limitations of the right, stating when and how can data be processed.[113] The EU Court of Justice has implicitly backed this understanding by occasionally referring to the right as established by Article 8(1) of the Charter, even though it does sometimes refer to the right as being recognised by Article 8 as a whole.[114] At the heart of these interpretative divergences lie contrasted perceptions of what defines the core of personal data protection: either a general prohibition of processing personal data or a general authorisation (under certain conditions).

---

[113] See, notably, Siemen, Birte, *Datenschutz als europäisches Grundrecht*, Duncker & Humblot, Berlin, 2006, p. 283.

[114] On the variable case law on balancing the EU right to the protection of personal data, see: González Fuster, Gloria, "Balancing intellectual property against data protection: a new right's wavering weight", *IDP Revista de Internet, Derecho y Política*, Vol. 14, 2012, pp. 43-46.

The EU Court of Justice has not yet provided clear guidance on this issue, and its case law has been erratic as regards the very identification of the existence of a right to the protection of personal data, its possible interpretation as an autonomous right, and the provisions relevant for the determination of lawful limitations to it. The Court, for instance, has maintained that there is a right jointly established by Articles 7 and 8 of the Charter, which it referred to as "the right to respect for private life with regard to the processing of personal data",[115] and asserted that the limitations which may lawfully be imposed on such right are exactly the same as those tolerated in relation to Article 8 of the ECHR.[116]

One can interpret Article 8 of the Charter in many ways, and the relation between its provisions remains unclear. In addition to the ECHR and Charter provisions, as well as relevant Strasbourg and Luxembourg case law, it is necessary to take account that, according to the Treaties, the Charter's rights need to be interpreted "with due regard to the explanations referred to in the Charter",[117] which in their turn refer to Directive 95/46/EC and a Regulation complementing it.[118] Both "contain conditions and limitations for the exercise of the right to the protection of personal data".[119] The Charter also mandates that the rights appearing in the Treaties must be exercised "under the conditions and within the limits defined by those Treaties",[120] which means that there is an obligation to bear in mind Article 16 TFEU and its explicit association of EU rules with regard to the processing of personal data and the free movement of such data.[121]

The EU Court of Justice habitually equates any processing of personal data with a limitation of the EU right to the protection of personal data, implying that the right's core content is substantiated in Article 8(1) of the Charter.[122] Following this line of thinking, it would logical to refer to the requirements substantiated in Article 8(2) and 8(3) to determine the possible lawfulness of any limitation of the right. But the EU Court of Justice tends instead to assess the lawfulness of limitations by engaging in a complex reading of Article 8 of the Charter in conjunction with the Charter's Articles 7 and 52(1), as well as Article 8 of the ECHR.[123]

Determining what is the core content of the right to the protection of personal data, and what are its limits, is not only of interest for the preciseness and richness of theoretical discussions. It is a question that touches directly the question of its status as a fundamental right. Traditionally, one of the basic features of fundamental rights has been precisely the fact that they can only be limited (and interfered with) under special, controlled conditions: the possible limitations must be strictly limited.

---

[115] Judgment of the Court (Grand Chamber) of 9 November 2010, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 2010 I-11063, § 52.
[116] Ibid.
[117] Art. 6(1) TEU. See also Art. 52(7) of the EU Charter.
[118] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001.
[119] Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, p. 20.
[120] Art. 52(2) Charter.
[121] As well as the fact that Art. 16(2) TFEU highlights that the rules adopted shall be without prejudice to the specific rules for processing in the area of Common Foreign and Security Policy.
[122] See, for instance, Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland*, (Judgment of the Court (Third Chamber) of 5 May 2011), para 49.
[123] An illustrative example is the judgment for Joined Cases C-92/09 and C-93/09, where the EU Court of Justice stated that "the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the ECHR", *Volker and Markus Schecke and Eifert,* op. cit., para 52.

Pending a clarification by the EU Court of Justice on how all the mentioned provisions interrelate and, especially, on the exact content and limits of the EU right to the protection of personal data, the obligations stemming from its recognition remain vague. More worryingly, they appear to be potentially modifiable by changes in EU secondary law, to which remit the Charter's explanations.

4.2.2 An innovative legal basis

The second key change brought about by the Lisbon Treaty for EU personal data protection is Article 16 of the TFEU. This provision, echoing Article 8 of the Charter, reaffirms that everybody has the right to the protection of personal data concerning them. In addition, it explicitly requires the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of EU law, and the rules relating to the free movement of such data. In reality, the innovative features of Article 16 of the TFEU are two: one that has been much acknowledged and celebrated, and a second one that has seemingly been less noticed.

4.2.2.1 Protection of individuals across EU law

The first one concerns the fact it provides a single legal basis for the regulation of personal data protection across (almost all) EU law, and thus opens the door to the possibility to put an end to the long-established division of EU personal data protection law into two separate areas, depending on whether the processing concerned "first pillar" (broadly, related to the internal market) or "third pillar" (on police and judicial co-operation in criminal matters) activities. The general collapse of the division of the EU into pillars was precisely one of the major innovations of the Lisbon Treaty. The development had been widely anticipated by many who regarded as problematic the way in which EU data protection law was developing due to such pillar division.

Whereas Directive 95/46/EC provided a general, basic set of rules applicable to the first pillar, the third pillar lacked an equivalent instrument.[124] After many years of inter-institutional tensions, a Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (the Data Protection Framework Decision) was adopted, but, nonetheless, it still did not provide a comparable level of protection.[125] The existence of very different rules applicable to the first and third pillar generated many frictions on how to determine which activities fell under which scope.[126]

If Article 16 of the TFEU heralds the end of the division between first and third pillar EU data protection, it sustains nevertheless a peculiar regime to be applied to the former second pillar: the second sentence of its second paragraph declares indeed that "rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39" of the

---

[124] On data protection in the third pillar, see Boehm, Franziska, *Information sharing and data protection in the Area of freedom, security and justice: towards harmonised data protection principles for information exchange at EU-level*, Springer, Berlin, 2012.

[125] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

[126] See, for instance, 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.

TEU, which in its turn establishes that, insofar as Common Foreign and Security Policy is concerned, rules on the protection of personal data shall not be adopted following the ordinary legislative procedure, but exclusively by the Council.[127]

4.2.2.2 Free movement of data across EU law

A second key innovation brought about Article 16 of the TFEU, which has been less discussed, is that it not only imposes on the EU legislator a mandate to legislate on personal data protection across (almost) the whole spectrum of EU law: it also imposes a requirement on them to regulate the free movement of such data to the same extent, and therefore including the Area of Freedom, Security and Justice. Prior to the Lisbon Treaty, EU law already incorporated a reference to the need to adopt rules on the free movement of data, but only in reference to data processed by institutions and bodies of the European Communities (thus, only to the institutions and bodies of the first pillar).[128]

The notion of free movement of (personal) data was integrated into EU law through Directive 95/46/EC. It was imported there directly from Convention 108, the preamble of which declares that its signatories recognise "that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples". Convention 108 devotes its Chapter III to transborder data flows, and forbids the restriction of the free flow of data among participating countries "for the sole purpose of the protection of privacy".[129] The roots of this notion of transborder data flows were in discussions undertaken by the OECD in the mid-1970s. The concept of transborder data flows plays an eminent role in the 1980 OECD Guidelines, precisely titled *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which were focused on preventing restrictions of flows of personal data that could, it was argued, "cause serious disruption in important sectors of the economy".[130] In this sense, the OECD Guidelines mandate Member countries to attempt to ensure that transborder flows of personal data are uninterrupted,[131] to refrain from restricting such flows except in extraordinary cases,[132] and to "avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection".[133]

The integration into EU law of the notion of the free movement of personal data via Directive 95/46/EC gave to the notion an additional dimension. The Directive was indeed formally concerned with the establishment of the internal market,[134] the objective of which is to protect the so-called fundamental freedoms of the EU: the free movement of goods, capital, services and people. These fundamental freedoms have been conventionally regarded by the EU Court of Justice as the very core of the EU project, and thus granted a particular, almost constitutional status, which was indirectly transmitted to the notion of the free movement of data (despite the fact that data cannot easily be categorised – at least exclusively – as goods). Thanks to Directive 95/46/EC, in any case, the notion acquired such a fundamental status, which allegedly justified its recognition as commensurate with the protection of human rights

[127] Art. 39 TEU.
[128] Art. 286 of the Treaty establishing the European Community.
[129] Art. 12(2) Convention 108.
[130] See the Preface to the OECD Council Recommendation establishing the Guidelines.
[131] Para 16 of OECD Guidelines.
[132] Ibid., para 17.
[133] Ibid., para 18.
[134] Its legal base was Article 100a (later Article 95) of the Treaty establishing the European Community.

that the Directive 95/46/EC equally served. This symmetry or equivalent value between the protection of human rights (and notably privacy) and the internal market (and notably the free movement of data) was mirrored in the Directive's name: 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*. It was also reflected in its opening recognition of objectives: it (a) obliges Member States to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data",[135] (b) prevents Member States from restricting or prohibiting "the free flow of personal data between Member States for reasons connected with the protection afforded".[136]

With Article 16 of the TFEU, this fundamental freedom of the free movement of personal data has not only acquired explicit Treaty-level recognition, but it has now extended beyond the internal market, and expanded to EU law in general. Free flows of data are not only to be ensured across markets, but also from one side to the other of the Area of Freedom, Security and Justice.

4.2.3 An evolving EU personal data protection legal framework

The EU personal data protection legal framework is currently under review, partly due to a perceived need to adapt it to the changes caused by the Lisbon Treaty.[137] To this end, the European Commission presented in January 2012 a whole legislative package, currently under negotiation. It consists of two legislative proposals accompanied by a Communication.[138] The first legislative draft is a proposal for a *Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data*,[139] designed to replace the existing centrepiece of EU personal data protection law, Directive 95/46/EC, and thus is expected to constitute the future generally applicable EU personal data protection instrument.[140] The second draft is a proposal for a *Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*,[141] and it is intended to (roughly) replace Framework Decision 2008/977/JHA.[142]

---

[135] Art. 1(1) of Directive 95/46/EC.
[136] Ibid., Art. 1(2).
[137] See Bigo Didier, Sergio Carrera Sergio, Gloria González Fuster, Elspeth Guild, Paul De Hert, Julien Jeandesboz and Vagelis Papakonstantinou, *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, European Parliament, Directorate General For Internal Policies, Policy Department C: Citizens' Rights And Constitutional Affairs, Civil Liberties, Justice and Home Affairs, 2011.
[138] European Commission, Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25.1.2012.
[139] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25.1.2012.
[140] It should also bring an amendment to Directive 2002/58/EC.
[141] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.1.2012, Brussels.
[142] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

The two proposed instruments have been based on Article 16(2) of the TFEU. The borderline between them is no longer replicating the EU pillar divide, which was dismantled by the Lisbon Treaty. Thus, the proposed Regulation is not exclusively concerned with the internal market and the respect of individuals' fundamental rights and freedoms, but also explicitly designed to contribute to the accomplishment of the EU Area of Freedom, Security and Justice.[143]

Also in line with Lisbon innovations, the legislative package introduced by the European Commission advances a construction of EU personal data protection legislation as the embodiment of the (new) EU fundamental right to the protection of personal data, marking a shift away from its traditional framing according to which the major objective of EU personal data protection law is to serve the insurance of the right to respect for private life, or right to privacy. Under the proposed framework, EU personal data protection law is envisaged instead as (primarily) the substantiation of the EU fundamental right to the protection of personal data. Article 1(2) of the proposed Regulation asserts: "This Regulation protects the fundamental rights and freedoms of natural persons, and *in particular their right to the protection of personal data*."[144] Article 1 of the proposed Directive defines its object as "protecting the fundamental rights and freedoms of natural persons and *in particular their right to the protection of personal data*".[145] The idea of EU personal data protection law serving, among all rights and freedoms, the right to privacy has therefore been replaced with the assertion that it develops first and foremost the EU right to the protection of personal data.[146] In addition, there is no reference in the proposed Regulation to Convention 108.[147]

If the pertinence of alluding to the right to the protection of personal data in post-Lisbon EU personal data protection instruments is hardly debatable, the suitability of referring to such right not *in addition to* the right to respect for private life, but *in place of it*, is nevertheless questionable.[148] The organs of the Council of Europe are currently discussing the upcoming modernisation of Convention 108[149] and are also considering the possible mention, in the revised instrument, of the right to the protection of personal data, but they are contemplating it as a supplement to references to Article 8 of the ECHR, and not as an alternative to them.[150] The disappearance of privacy from the EU data protection legal landscape directly affects its relationship with security.

---

[143] COM(2012) 11 final [p. 17].
[144] COM(2012) 11 final, p. 40. Emphasis added.
[145] Emphasis added. As well as ensuring that the exchange of personal data by competent authorities in the EU is not restricted for reasons connected with the protection of individuals with regard to the processing of personal data (COM(2012) 10 final, p. 26).
[146] See also: Costa, Luiz, and Yves Poullet, "Privacy and the regulation of 2012", *Computer Law & Security Review*, Vol. 28, No. 2012, pp. 254-262 [p. 255].
[147] Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, WP 191, Brussels, 23 March 2012, p. 5.
[148] Hornung, Gerrit, "A general data protection regulation for Europe? Light and shade in the Commission's draft of 25 January 2012", *SCRIPT-ed*, Vol. 9, No. 1, 2012, pp. 64-81 [pp. 66-67].
[149] Work is ongoing since 2009. See Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Final document on the modernisation of Convention 108, T-PD (2012)04Mos, 15 June 2012, Strasbourg, p. 4.
[150] Ibid., p. 9.

5 INTERSECTIONS

The multifaceted notions of security, privacy and personal data protection inevitably meet in a variety of ways. Some of their encounters are seemingly unproblematic.[151] In EU policy and law, major frictions between security, on the one hand, and privacy and personal data protection, on the other hand, occur most often in two specific contexts: first, security can act as a generator of measures potentially encroaching on the fundamental rights to privacy (respect for private life) and to the protection of personal data; second, security can materialise modulating, restricting or limiting the application of such fundamental rights or of the legal instruments that substantiate them.

5.1 SECURITY MEASURES AFFECTING PRIVACY AND PERSONAL DATA PROTECTION

The development of the Area of Freedom, Security and Justice has triggered a vast number of initiatives involving the massive processing of personal data.[152] As noted above, the objective of security in this specific area is linked to a broad spectrum of issues, including border controls, asylum, immigration and the prevention and combating of crime, as well as measures for co-ordination and co-operation between police and judicial authorities and other competent authorities. This (broad) notion of security has been, and still is, the driving force behind many (of the numerous) EU-level initiatives championing the processing of information about individuals.

In 2010, the European Commission published a Communication providing an overview of EU-level measures regulating the collection, storage or cross-border exchange of personal information linked to the establishment of the Area of Freedom, Security and Justice.[153] The many measures described include the Swedish Initiative,[154] regulating the exchange of information and intelligence between national law enforcement authorities for the purpose of conducting criminal investigations or criminal intelligence operations; the Prüm Decision,[155] providing for automated exchange of DNA profiles, fingerprint data and vehicle registration for investigating criminal offences, preventing criminal offences, and maintaining public security; the Schengen Information System (SIS),[156] a large-scale system containing alerts on persons and objects, used both within the Schengen area and at its external frontiers, and

---

[151] For example, it is difficult to argue against that idea that network and information security can serve, in principle, privacy (as in Council Resolution 2009/C 321/01, op. cit., n. 49, Art. 1.

[152] See González Fuster, Gloria, Serge Gutwirth and Paul de Hert, *Privacy and Data Protection in the EU Security Continuum*, INEX Policy Brief No. 12, CEPS, June 2011**;** Berthelet, Pierre, *Le paysage européen de la sécurité intérieure*, P.I.E. Peter Lang, Brussels, 2009; Geyer, Florian, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", CEPS, Brussels, 2008.

[153] European Commission, Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice, COM(2010) 385 final, Brussels, 20.07.2010.

[154] 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, OJ L 386, 29.12.2006.

[155] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008; Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008.

[156] 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.

scheduled to be replaced by SIS II; EURODAC,[157] a centralised automated fingerprint identification system with information about individuals who request asylum in a Member State and third-country nationals apprehended in connection with the irregular crossing of external borders; the Visa Information System (VIS),[158] facilitating the examination of visa applications and external border checks "while contributing to the prevention of threats to Member States' internal security"[159]; Eurojust,[160] an EU body whose objective is to improve the co-ordination of investigations and prosecutions in Member States and to enhance co-operation; and Europol,[161] supporting Member States in preventing and combating organised crime, terrorism and other forms of serious crime in cross-border cases, and providing a platform to exchange criminal intelligence and information, and which manages the Europol Information System, a database of information on cross-border crime.

These initiatives are only a few examples of a series of measures which are constantly being refined, multiplied and subject to review – commonly in order to expand their scope.[162] Recently, the area of border management (understood as an extremely broad notion) has witnessed a particular effervescence of proposals involving the processing of personal data.[163] In addition, two border-related initiatives that originally had been put forward as unconcerned with personal data processing have been drifting towards the processing of personal data and a progressive entanglement with personal data flows: namely, the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX)[164] and the European Border Surveillance System (Eurosur).

In 2012, the European Commission presented its vision for the future of EU law enforcement information exchange in its Communication *Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM).*[165] Based on the assumption that exchanging information between Member States is an essential tool for EU law enforcement authorities,[166] it presents a series of recommendations for future action. It suggests in

---

[157] Council Regulation (EC) 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.

[158] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.6.2004; 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, 13.8.2008. The management of EURODAC and VIS (and eventually of SIS II) is the responsibility of an agency operational since December 2012, the EU Agency for Management of Large-Scale IT Systems.

[159] COM(2010) 385 final, p. 7.

[160] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 6.3.2002.

[161] Council Decision 2009/371/JHA establishing the European Police Office (Europol), OJ L 121, 15.5.2009/

[162] See European Commission, Communication from the Commission to the European Parliament and the Council: First Annual Report on the implementation of the EU Internal Security Strategy, COM(2011) 790 final, Brussels, 25.11.2011.

[163] European Commission, Smart borders – options and the way ahead, Communication to the European Parliament and the Council, COM(2011) 680 final, 25.10.2011. See also González Fuster, Gloria, and Serge Gutwirth, "When 'digital borders' meet 'surveilled geographical borders': Why the future of European border management is a problem", in Peter Burgess and Serge Gutwirth (eds.) *A Threat Against Europe? Security, Migration and Integration*, VUB Press, Brussels, pp.171 - 190.

[164] Council Regulation (EC) 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.

[165] European Commission, Communication to the European Parliament and to the Council, Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), COM(2012) 735 final, Brussels, 7.12.2012.

particular that the role of Europol shall be further enhanced. To this purpose, it argues that Member States should rely more systematically on the Europol channel for their information exchanges,[167] and declares that a forthcoming proposal will aim to create, through these means, a EU-wide picture of cross-border criminality accessible through Europol.[168] The Communication also indicates that Eurosur is to be integrated together with Frontex in a Common Information Sharing Environment (CISE) through which general law enforcement shall have access to the information exchanged (in prevention of irregular migration and cross-border crime).[169]

The EU also supports security objectives through additional means, such as research funding. The Security theme of the Seventh Framework Programme is devoted to security conceived in a broad sense: the theme is designed to contribute to the implementation of EU external policies, to the creation of the EU Area of Freedom, Security and Justice, and "to policy areas such as transport, health, civil protection, energy, development and environment".[170] Thus, many meanings of security coexist in this context, and furthermore some of the security research activities focus precisely on security as an evolving concept, among allusions to the "fluctuating" landscape of security.[171] What appears to link all these multiple meanings of security in EU-funded Security Research is that they are addressed through the development of knowledge and, most notably, technologies,[172] which can interfere with the fundamental rights of the individual.

There is no doubt that both the establishment of the Area of Freedom, Security and Justice and EU support of security research must be carried out in full compliance with EU fundamental rights. This raises the practical question of how to make sure that this happens – which is an issue related to the conditions of the EU legislative process, and the constraints applicable to the funding of EU research. But it also leads to another major question: what does it mean exactly to develop (EU) security (technology) in full compliance with EU fundamental rights? What is the capacity of such EU fundamental rights to limit, influence, modulate or counter the spread of (EU) security measures and technologies involving the (massive) processing of personal data?

5.2 THE RIGHT TO RESPECT FOR PRIVATE LIFE AND SECURITY

For the purposes of EU law, the most relevant legal provision on the intersection between the right to respect for private life and security is Article 8 of the ECHR. The ECHR explicitly mentions in its Article 8(2) the interests of national security and prevention of crime as grounds that can potentially render legitimate any interference by public authorities with the exercise of the right to respect for private life – if the interference is in accordance with the law and "necessary in a democratic society".[173]

---

[166] Ibid., p. 2.
[167] Ibid., p. 14. Europol has a secure communications tool Secure Information Exchange Network Application (SIENA)
[168] Ibid.
[169] Ibid., p. 5. See also Hayes, Ben, and Mathias Vermeulen, *Borderline: The EU's New Border Surveillance Initiatives,* Heinrich Böll Foundation, Berlin, 2012, p. 9.
[170] European Commission, Work Programme 2013 – Cooperation – Theme 10 – Security, C (2012) 4536 of 09 July 2012, p. 6.
[171] Ibid., p. 80-81.
[172] Ibid., p. 6.
[173] Art. 8(2) ECHR.

As stated above, Article 8(2) of the ECHR sets out the specific conditions whereby the right to respect for private life can be restricted. Article 8(2) operates in addition to another general restricting provision, which is Article 15 on derogation in time of emergency: Article 15 enables all but the absolute rights to be suspended in time of war or other public emergency threatening the life of the nation,[174] situations which can be labelled as national security emergencies.[175]

The European Court of Human Rights has never defined "national security interests", but its case law shows that the ground has been raised mainly in cases concerning the security of the state and the democratic constitutional order from threats posed by enemies both within and without.[176] Major cases in which the national security purpose has been mentioned have involved infringements of the right to respect for private life occasioned by secret surveillance. Secret surveillance is regarded as constituting and interference with Article 8, which can nevertheless be considered legitimate.[177] A key requirement is that secret surveillance must be subject to satisfactory safeguards against arbitrary abuse.[178] The basic idea is that the State must be able to undertake secret surveillance,[179] but that there is a risk of undermining or even destroying democracy on the ground of defending it.[180] States have been allowed a wide margin of appreciation with respect to positive rather than negative obligations and matters of national security, such as secret surveillance.[181]

Appendix I provides a detailed analysis of the case law of the ECHR regarding the acceptance of security as a legitimate ground for restricting the right to privacy and data protection.

5.3 PERSONAL DATA PROTECTION AND SECURITY

If the tensions between security and privacy have caught the attention of many scholars, the issue of how to place the protection of personal data in the security/privacy nexus has been less explored.[182] Nonetheless, the majority of encroachments between security and fundamental rights unfold in EU law specifically through the processing of personal data. The interconnections between personal data protection and security in EU law are evolving, and must be analysed taking into account the recent shifts in the inscription of personal data protection in EU primarily law.

5.3.1 Security in existing EU secondary law

In existing EU personal data protection legal instruments, one can observe two main types of provisions related to security in the sense of national, public or internal security: those where

[174] Greer, Steven, *The exceptions to Articles 8 to 11 of the European Convention on Human Rights,* Council of Europe, Strasbourg, 1997, p. 5.
[175] Ibid.,p. 18.
[176] Ibid.
[177] Ibid., p. 19.
[178] Ibid.
[179] *Klass and others v Germany,* Judgment of 6 September 1978, Series A 28, para 42.
[180] Ibid., para 49.
[181] Greer, op. cit., n. 174, p. 43.
[182]Burgess, Peter J., *Security After Privacy: The Transformation of Personal Data in the Age of Terror*, PRIO Policy Brief 5/2008, PRIO, Oslo, 2008.

security marks the external boundaries of personal data protection instruments and those where it restricts the scope of application from the inside.[183]

5.3.1.1 Security as external limit of EU data protection legislation

The first type can be associated with structural idiosyncrasies of EU legislation, which has traditionally kept separate (through the pillar divide) internal market issues from matters related to national security or criminal law. Directive 95/46/EC, for instance, was adopted as an internal market instrument at a time when such instruments (under Community law or the first pillar) followed different legislative paths than third pillar matters. Logically, thus, Directive 95/46/EC is applicable only to the processing of personal data by persons whose activities are governed by Community law, while activities falling outside of Community law ("regarding public safety, defence, State security or the activities of the State in the area of criminal laws"[184]) are explicitly recognised as excluded from its scope of application.[185] Council Framework Decision 2008/977/JHA, adopted as a third pillar instrument, is applicable to data processing carried out in relation to many (security) activities excluded from the scope of application of Directive 95/46/EC, but its scope is nevertheless also ultimately demarcated by the boundaries of EU law vis-à-vis national security: in this sense, it explicitly provides that its provisions are "without prejudice to essential national security interests and specific intelligence activities in the field of national security".[186]

5.3.1.2 Security as internal limit of EU data protection legislation

The second type of security-related provisions in EU data protection law is more closely (conceptually and historically) linked to the framing of security as a possible ground justifying interferences with the right to respect for private life. These provisions concern the cases when EU data protection law formally applies, but its substance can be restricted in the name of security. In this sense, for example, Directive 95/46/EC foresees, in its Article 13 on exemptions and restrictions, that Member States can restrict obligations and rights it establishes when such a restriction constitutes a necessary measures [sic] to safeguard, inter alia, national security, defence, public security, or the prevention, investigation, detection and prosecution of criminal offences.[187] This provision was directly inspired by the content of Article 8 of the ECHR. The need to read it in the light of the case law of the European Court of Human Rights on Article 8(2) of the ECHR was eventually stressed by the EU Court of Justice.[188] In line with the case law, this type of provision leaves a wide margin appreciation to Member States to determine what constitutes a necessary measure.[189] Harmonisations of this type of restrictions has only been carried out exceptionally,[190] the most famous example

---

[183] These two types of provisions are described in European Commission, 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, pp. 7-8.
[184] Recital 13 of Directive 95/46/EC.
[185] Art. 3(2) of Directive 95/46/EC.
[186] Art. 1(4) of Council Framework Decision 2008/977/JHA.
[187] Art. 13(1) of Directive 95/46/EC.
[188] See Judgment of the Court of 20 May 2003, Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk*, 2003 I-04989, § 91.
[189] The Council Framework Decision 2008/977/JHA also includes provisions falling under this category, such as Art. 17(2).
[190] COM(2007) 87 final, p. 8.

being the approximation carried out through Directive 2006/24/EC,[191] regarding the systematic retention of communications data.

5.3.1.3 Security as security of processing of EU data protection legislation

The word *security* surfaces in EU data protection legal instruments with meanings unrelated to national or public or internal security. The most important other usage is probably in association with the notion of processing. Directive 95/46/EC devotes a full Article to security of processing, described as the implementation of "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing".[192]

5.3.2 Security and post-Lisbon EU data protection

With the collapse of the pillar structure caused by the Lisbon Treaty, one of the elements that justified a particular function of security in EU data protection law disappeared. Nevertheless, and although Article 16 of the TFEU provides nowadays a single legal basis for the regulation of personal data protection across all the fields of EU law, the Lisbon Treaty also advanced new factors affecting the relation between security and personal data protection. In particular, there are two Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon that modulate the significance of Article 16 of the TFEU:

- Declaration 20 proclaims that "whenever rules on protection of personal data to be adopted on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter", and "recalls that the legislation presently applicable (see in particular Directive 95/46/EC) includes specific derogations in this regard";[193] and

- Declaration 21 maintains "specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation … may prove necessary because of the specific nature of these fields".[194]

The European Commission has definitely mirrored these declarations in its drafting of legislative proposals for the future EU data protection legal framework. In this sense, it has echoed the call for specific rules of Declaration 21 in the construction of a separate proposal (the proposed Directive) to be applicable "with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties"[195] (processing under these activities is formally excluded from the material scope of the proposed Regulation).[196] And it has included in its two proposed instruments provisions taking account of the specific characteristics of national security, as put forward in Declaration 20.

---

[191] 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.
[192] Art. 17(1) of Directive 95/46/EC.
[193] Declaration 20 on Article 16 of the Treaty on the Functioning of the European Union.
[194] Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.
[195] COM(2012) 10 final.
[196] Art. 2(2)(e) of the proposed Regulation.

As in existing legislation, national security operates in the proposed instruments as an external limit or boundary demarking their scope of application: they are to apply only to the processing of personal data in the course of activities falling under the scope of EU law, which explicitly excludes data processing concerning national security.[197] Another security-related external boundary is the exclusion of the processing of personal data by the Member States when carrying out activities in relation to the Common Foreign and Security Policy.[198]

Based on the notion of 'security of processing' of current EU data protection law, in the proposed Regulation a section is devoted to 'data security'.[199] Here, the main novelty is the incorporation of an obligation to notify some 'data breaches',[200] defined as a sort of 'breaches of security'.[201]

The major changes related to the security / personal data protection nexus as it materialises in the proposed legislative instruments can be linked to the disappearance of the right to respect for private life as basic reference in the area. Traditionally, the EU legislator had been construing restrictions of EU data protection law as interferences with the right to respect for private life, but, now, having replaced the right to respect for private life with the right to the protection, it faces the challenge of devising them under the new light. And it seems to be a particularly difficult challenge in the context of the many hesitations surrounding the content of (and lawful limitations to) the EU right to personal data protection.

As a consequence of the undecided structure of the EU fundamental right to the protection of personal data, personal data processing undertaken in the name of security can be regarded either as an interference or as a lack of interference with such right. Article 8(2) of the EU Charter states that the processing of personal data must be grounded on the basis of consent of the person concerned or on some other legitimate basis laid down by law, which might include a basis laid down by law in the name of security.

The proposed Regulation's Article 6(1) foresees that the processing of personal data can be considered lawful, inter alia, if it is necessary for the performance of a task carried out in the public interest (a notion which can be read as including security) or in the exercise of official authority vested in the controller. Article 6(3) later adds that, in such cases, the processing must be grounded in EU or national law, which shall *in addition* respect the essence of the right to the protection of personal data, and be proportionate to the legitimate aim pursued. The wording of this latter provision echoes Article 52(1) of the Charter,[202] which establishes the general applicable requirements to any limitations of the Charter's rights to be considered lawful: thus, it could be deduced that the European Commission, when designing this provision, was approaching the grounding of processing of personal data in the public interest as a limitation of the fundamental right to personal data protection – which implies a reading of Article 8(2) of the Charter as detailing not the substance, but the limitations of the right.

[197] See Art. 2(2)(a) of the proposed Regulation (COM(2012) 11 final, p. 40), and Art. 2(3)(a) of the proposed Directive (COM(2012) 10 final, p. 26). The formulation of this limitation has been criticised by the European Data Protection Supervisor (EDPS), who believes the meaning of the expression is unclear: see European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Data protection reform package, 7 March 2012, Brussels, p. 15.
[198] COM(2012) 11 final, p. 19, and art 2(2)(c) of the proposed Regulation.
[199] COM(2012) 11 final, p. 10.
[200] Ibid.
[201] COM(2012) 11 final, p. 42.
[202] As confirmed by the reference to the Charter in Recital 36 of the proposed Regulation.

The proposed Regulation also includes a provision overtly devoted to possible restrictions to the different rights and obligations proposed by the instrument, Article 21.[203] This provision establishes that both EU law and national law may restrict the scope of the major part of the Regulation's provisions if such a restriction 'constitutes a necessary and proportionate measure in a democratic society' for achieving any of a series of listed purposes, including public security. Here, it is patent that the drafters were thinking of describing derogations that would possibly constitute limitations to the fundamental right to the protection of personal data.[204] The Preamble to the Proposed Regulation notes that such restrictions should be in compliance with the requirements of the Charter and of the ECHR,[205] but, unfortunately, Article 21 fails to refer thoroughly to the requirements established by any of them: compared to Article 52(1) of the Charter, it misses the requirement of respecting the essence of the right to the protection of personal data and, compared to Article 8 of the ECHR, not only does it not fully incorporate the content of the condition in accordance with the law (which is wider than merely demanding that the measure appears in a law), but it also broadens the possible grounds justifying restrictions to even explicitly include (as a legitimate ground justifying a restriction to the right to the protection of personal data) any monitoring which would be connected, even occasionally with security.[206]

In sum, the proposed legislative package, instead of compensating its detachment of EU data protection law from the right to privacy with a solid construction of the EU right to the protection of personal data as enshrined by the EU Charter, further exacerbates the tensions and confusion surrounding its content and limits. It alludes to requirements generally applicable to limitations of the Charter's rights (i. e., to be provided for by law, respect the essence of those rights, respect the principle of proportionality, be necessary, pursue an objective of general interest recognised by the EU or protect the rights and freedoms of others)[207] when describing possible grounds to legitimise the processing of personal data,[208] and it fails to refer to them in full when detailing the conditions applicable to possible restrictions of applicable rights and obligations – opting instead for a partial echoing of the requirements of interferences with the right to respect for private life of Article 8 of the ECHR.[209] The outcome is, on the one hand, a sustained ambiguity as to what is the content of the right and, on the other, noteworthy uncertainty on the limits of its limits.

[203] Concerning the proposed Directive, see Art. 11(4) and Art. 13. Security as an important ground of public interest is also granted a role to potentially legitimise data transfers to third countries that would be otherwise unlawful (COM(2012) 11 final, p. 31).
[204] See also: COM(2012) 11 final, p. 9.
[205] Ibid., p. 26.
[206] Art. 21(1)(e) of the proposed Regulation.
[207] Art. 52(1) Charter.
[208] Art. 6(3) of the proposed Regulation.
[209] Art. 21 of the proposed Regulation.

6 CONCLUDING REMARKS: A FUNDAMENTAL DEBATE?

Security, privacy and personal data protection are legal notions that can be apprehended from multiple perspectives. This paper has stressed that their meaning for the purposes of EU law is multiple, and often ambivalent. It has also found evidence that the particular unfolding of these legal notions in EU law reveals a series of noteworthy asymmetries, which have crucial repercussions on how they intersect.

Security, we have noted, is a word the meaning of which can refer in EU law to many different types of security, differently related to issues of sovereignty: notably, it can refer to security of the State in the sense of the preservation of its integrity, public security as a ground justifying interferences with fundamental EU (market) freedoms, (essential) national security as what is excluded from the reach of EU law, (international) security as pursued by the EU Common Foreign and Security Policy; (EU) security as what is pursued through the Area of Freedom, Security and Justice, and, finally, security interests as grounds justifying interferences with the right to respect for private life and restrictions and modulations of the right to the protection of personal data. Security appears thus somehow as an elastic notion, sometimes moving upwards towards its EU dimension, sometimes retreating back towards its national (or even essentially national) character. Due to this versatility, security takes sometimes the shape of a Janus-faced notion, especially in relation to personal data processing: under its EU light (as an objective of the Area of Freedom, Security and Justice), it supports the proliferation of (EU security) initiatives relying on the systematic processing of personal data, whereas, simultaneously, under its national light (as a prerogative of the State), it justifies (national) restrictions to the provisions that are supposed to mitigate the risks linked to the former.

Privacy is recognised as a EU fundamental right, and was imported into the EU catalogue of fundamental rights from Article 8 of the ECHR. This provision is principally concerned with protecting the individual against interferences by the State, even if certainly not reduced to it (and including for instance positive obligations imposed on the State to prevent interferences by private parties).

Personal data protection is also recognised nowadays as an EU fundamental right, but it is a right of a different lineage. It has no direct equivalent in any of the classical sources that have led to the determination fundamental rights in EU law: neither in the ECHR, nor in the common constitutional traditions of the Member States.[210] It is thus in a sense a product of the EU Charter, and its emergence has been significantly affected by the Lisbon Treaty. Being a relatively recent right, one could consider that the determination of its substance is normal, but (still) relatively unsettled. What is perhaps more relevant is that its establishment as an EU fundamental right has been structurally linked to a series of peculiar circumstances: it has been "constitutionalised" (in the sense of inscribed in primary law) together with the free movement of personal data across EU law, and with a series of limitations that invite to seriously challenge its qualification as fundamental.

The shortcomings of the fundamental status of the EU fundamental right to the protection of personal data become critical when it is used as substitute for the right to respect for private life in the security / privacy nexus. Practical consequences of this displacement are observable in the legislative framework on personal data protection advanced in January 2012 by the

[210] The right to the protection of personal data is recognised as a fundamental right in some Member States, but it cannot be regarded as constituting a common constitutional tradition among them.

European Commission. But, more generally, they invite further investigation of the relation between (EU/non-EU) security and EU fundamental rights.

7 BIBLIOGRAPHY

Alexy, Robert, *A Theory Of Constitutional Rights*, Oxford University Press, London, 2010.

Anderson, Malcolm and Joanna Apap, *Changing Conceptions of Security and their Implications for EU Justice and Home Affairs Cooperation*, The Centre for European Policy Studies (CEPS) Policy Brief, No. 26, October 2002.

Arendt, Hannah, *The Human Condition*, Chicago, The University of Chicago Press, Chicago, 1998.

Ariès, Philippe, and Georges Duby (eds.), *Histoire de la vie privée : 2. De l'Europe féodale à la Rennaissance*, Editions du Seuil, Paris, 1999.

Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, WP 191, Brussels, 23 March 2012.

Bigo, Didier, Sergio Carrera Sergio, Gloria González Fuster, Elspeth Guild, Paul De Hert, Julien Jeandesboz and Vagelis Papakonstantinou, *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, 2011.

Bioy, Xavier, "L'identité de la personne devant le Conseil constitutionnel", *Revue Française de Droit Constitutionnelle*, Vol. 1, No. 65, 2006, pp. 73-95.

Blume, Peter, "Lindqvist Revisited - Issues concerning EU data protection law", in Henning Koch (ed.), *Europe: the new legal realism: essays in honor of Hjalte Rasmussen*, DJØF, Copenhagen, 2010.

Boehm, Franziska, *Information sharing and data protection in the Area of freedom, security and justice: towards harmonised data protection principles for information exchange at EU-level*, Springer, Berlin, 2012.

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

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

Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Final document on the modernisation of Convention 108, T-PD (2012)04Mos, Strasbourg, 15 June 2012.

Costa, Luiz, and Yves Poullet, "Privacy and the regulation of 2012", *Computer Law & Security Review*, Vol. 28, No. 2012, pp. 254-262.

De Hert, Paul, and Serge Gutwirth, "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power", in Erik Claes, Antony Duff and Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Intersentia, Antwerp, 2006, pp. 61-104.

--- "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in Serge Gutwirth, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 3-44.

Delarue, Jean Marie, "Titre VI Dispositions relatives à la coopération policière et judiciaire en matière pénale" in Isabelle Pingel (ed.), *Commentaire article par article des traités UE et CE : de Rome à Lisbonne,* Helbing Lichtenhahn, Bâle, 2010.

Edelman, Bernard, *La personne en danger*, Presses Universitaires de France, Paris 1999.

European Commission, 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.

--- Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice, COM(2010) 385 final, Brussels, 20.07.2010.

--- Smart borders – options and the way ahead, Communication to the European Parliament and the Council, COM(2011) 680 final, 25.10.2011.

--- Communication from the Commission to the European Parliament and the Council: First Annual Report on the implementation of the EU Internal Security Strategy, COM(2011) 790 final, Brussels, 25.11.2011.

--- Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25.1.2012.

--- Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.

--- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25.1.2012.

--- Communication to the European Parliament and to the Council, Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), COM(2012) 735 final, Brussels, 7.12.2012.

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Data protection reform package, 7 March 2012, Brussels.

González Fuster, Gloria, "Balancing intellectual property against data protection: a new right's wavering weight", *IDP Revista de Internet, Derecho y Política*, Vol. 14, 2012, pp. 43-46.

González Fuster, Gloria, and Serge Gutwirth, "When 'digital borders' meet 'surveilled geographical borders': Why the future of European border management is a problem", in Peter Burgess and Serge Gutwirth (eds.), *A Threat Against Europe? Security, Migration and Integration*, VUB Press, Brussels, pp.171 - 190.

González Fuster, Gloria, Serge Gutwirth and Paul de Hert, *Privacy and Data Protection in the EU Security Continuum*, INEX Policy Brief No. 12, CEPS, June 2011.

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

Gutwirth, Serge, *Privacy and the information age*, Rowman & Littlefield Publishers, Oxford, 2002.

--- "Biometrics between opacity and transparency", *Annali dell'Istituto Superiore di Sanità*, Vol. 43, No. 1, 2007, pp. 61-65.

Habermas, Jürgen, *The Structural Transformation of the Public Sphere*, Polity, Cambridge, 1992.

Hayes, Ben and Mathias Vermeulen, *Borderline: The EU's New Border Surveillance Initiatives,* Heinrich Böll Foundation, Berlin, 2012.

Hornung, Gerrit, "A general data protection regulation for Europe? Light and shade in the Commission's draft of 25 January 2012", *SCRIPT-ed*, Vol. 9, No. 1, 2012, pp. 64-81.

Hustinx, Peter J., "Data Protection in the European Union", *P&I*, 2005, pp. 62-65. www.edps.europa.eu/.../EDPS/.../05-04-21_Data_Protection_EN.pdf

Lageot, Céline (ed.), *Dictionnaire plurilingue des libertés de l'esprit. Étude de droit européen comparé*, Bruylant, Bruxelles, 2008.

Macovei, Monica, "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,* n° 5, Council of Europe, 2004.

Michaelsen, Christopher, "Balancing Civil Liberties Against National Security? A Critique of Counterterrorism Rhetoric", *University of NSW Law Journal*, Vol. 29, No. 1, 2006, pp. 1-21.

Monar, Jörg, "Préface", in Pierre Berthelet, *Le paysage européen de la sécurité intérieure,* P.I.E. Peter Lang, Brussels, 2009, pp. 23-28.

Nippert-Eng, Christena, *Islands Of Privacy*, The University of Chicago Press, Chicago, 2010.

Elias, Norbert, *La société des individus*, Librairie Arthème Fayard, Paris, 1991.

Pérez Luño, Antonio Enrique, *Derechos humanos, estado de derecho y constitución (10a edición)*, Tecnos, Madrid, 2010.

Poullet, Yves, "Pour une troisième generation de réglementation de protection des données" in María Verónica Pérez Asinari and Pablo Palazzi (eds.), *Défis du droit à la protection de la vie privée: perspectives du droit européen et nord-américain / Challenges of Privacy and Data Protection Law: Perspectives of European and North American Law*, Bruylant, Brussels, 2008, pp. 297-365.

Rigaux, François, *La vie privée, une liberté parmi les autres?*, Larcier, Brussels, 1992.

Rodotà, Stefano, "Data Protection as a Fundamental Right", in Serge Gutwirth, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, 2009, pp. 77-82.

--- *La vita e le regole: Tra diritto e non diritto*, Feltrinelli, Milano, 2009.

Rössler, Beate, "Privacies: An Overview", in Beate Rössler (ed.), *Privacies*, Stanford University Press, Stanford, 2004, pp. 1-18.

Ruiz Miguel, Carlos, *La configuración constitucional del derecho a la intimidad,* Universidad Complutense de Madrid, Madrid, 1992.

Schulhofer, Stephen J., *More essential than ever: The Fourth-Amendment in the Twenty-First Century*, Oxford University Press, Oxford, 2012.

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

Sofsky, Wolfgang, *Defensa de lo privado: Una apología*, Pre-textos, Valencia, 2009.

Solove, Daniel J., *Understanding privacy,* Harvard University Press, Cambridge, MA, 2008.

Solove, Daniel J., Marc Rotenberg and Paul M. Schwartz, *Information privacy law*, Aspen Publishers, New York, NY, 2006.

Tuori, Kaarlo, "European Security Constitution", in Martin Scheinin (ed.), *Law and Security: Facing the dilemmas*, EUI Working Papers Law 2009/11, European University Institute (EUI), Department of Law, 2009, pp. 1-6.

Turkington, Richard C., and Anita L. Allen, *Privacy Law: Cases and Materials*, West Group, St. Paul, MN, 1999.

Walker, Neil, "In search of the Area of Freedom, Security and Justice: A Constitutional Odyssey", in Neil Walker (ed.), *Europe's Area of Freedom, Security and Justice*, Oxford University Press, Oxford, 2004, pp. 3-40.

Westin, Alan F., *Privacy and freedom*, Atheneum, New York, 1967.

APPENDIX I: THE CASE LAW OF THE ECHR REGARDING THE ACCEPTANCE OF SECURITY AS A LEGITIMATE GROUND FOR RESTRICTING THE RIGHT TO PRIVACY AND DATA PROTECTION

by Erik Uszkiewicz, EKINT [211]

The European Convention on Human Rights (ECHR)[212] guarantees the right to respect for private life, family life, home and correspondence. Article 8 says the following:
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.

According to the text, it becomes clear that the rights which are guaranteed by this article are not absolute: public authorities may interfere with the rights guaranteed by Article 8 in certain circumstances. These circumstances are: the interferences have to be in accordance with law and the interference should be "necessary in a democratic society". Legal restriction can be regarded as Convention compliant only in these cases. One or more of the legitimate aims listed in paragraph 2 can be considered as acceptable grounds for limitation by the State of an individual's rights according to this Article. In the following, we will analyse the case law of the European Court of Human Rights (ECtHR or Strasbourg) from the aspect of accepting security as a legitimate ground for restricting the right to privacy and data protection.[213]

The first case relevant to our topic is *Klass and Others* v. *Germany*.[214] The ECtHR deemed the petition admissible, despite the fact that the complainants had turned to the Court in the subject of potentially being under surveillance. The defendant government of the Federal Republic of Germany took the view that what the complainants had really sought to achieve was a constitutional review. Yet the Court arrived at the following:

> As to the facts of the particular case, the Court observes that the contested legislation institutes a system of surveillance under which all persons in the Federal Republic of Germany can potentially have their mail, post and telecommunications monitored, without their ever knowing this …. To that extent, the disputed legislation directly affects all users or potential users of the postal and telecommunication services in the Federal Republic of Germany. Furthermore … this menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8 (Art. 8). … Having regard to the specific circumstances of the present case, the Court concludes that each of the applicants is entitled to "(claim) to be the victim of a violation" of the Convention, even though he is not able to allege in support of his application that he has been subject to a

[211] See also the Appendix II, which contains the most relevant information relating to the cases analysed in this study in a tabular format.
[212] http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/CONVENTION_ENG_WEB.pdf
[213] Kilkelly, Ursula, *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights,* Council of Europe, Strasbourg, 2001, p. 6. http://echr.coe.int/NR/rdonlyres/77A6BD48-CD95-4CFF-BAB4-ECB974C5BD15/0/DG2ENHRHAND012003.pdf
[214] Klass and Others v. Germany, Judgment of 6 September 1978, Application no. 5029/71.

> concrete measure of surveillance. [Case of Klass and Others v. Germany (Application no. 5029/71) Judgment of 6 September 1978, pp. 37-38.]

The following principles in the findings of this judgment are worthy of attention. First, the challenge of terrorism: democratic societies nowadays find themselves threatened by terrorism and highly sophisticated forms of espionage; consequently, the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. Nevertheless, the Court, being aware of the danger, inherent in secret surveillance measures, "of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

In connection with the information of the concerning person: the main principle is that the concerned person has to be informed about the relevant circumstances at least after the interception, but rules often provide exemptions for the States, where it is likely that such information would prejudice the purpose of the intervention, such as national security.

In this case, the Court found no violation of Article 8: the law challenged by the applicants (imposing restrictions on the secrecy of mail, post and telecommunications) was found by the Court to be necessary in a democratic society in the interests of national security and for the prevention of disorder or crime.

The case of *Malone* v. *The United Kingdom*[215] is directly concerned only with the issue of interceptions effected by or on behalf of the police. In this case, the police intercepted the telephone conversations of Mr. Malone (as a suspected receiver of stolen goods) under a warrant issued by the Home Secretary in accordance with the law. In its judgment, the Court emphasised that if the power of the executive is exercised in secret, the risks of arbitrariness are evident. For this reason, the law must contain adequate guarantees against abuse. According to Strasbourg, the secret telephone tapping could be necessary in a democratic society: "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime", but it should be borne in mind that the number of warrants granted is relatively low, especially when compared with the rising number of indictable crimes committed and telephones installed. The Court held that Article 8 had been violated in *Malone* because of the obscurity and uncertainty of the relevant domestic law which applied at that time.

This decision clarified that the law has to provide:

- protection against arbitrary interference with an individual's right under Article 8 and
- the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures (for similar argumentation, see the *Halford* v. *The United Kingdom* and *the Khan* v. *The United Kingdom* decisions).

The case of Malone made apparent one of the most important requirements for court decisions, i.e., precise and transparent legislation. In two cases, France was declared responsible of a violation of Article 8 of the ECHR because although the courts continued

[215] *Malone* v. *The United Kingdom*, Judgment of 2 August 1984, Application no. 8691/79.

their contribution to the wiretapping, the law was not sufficiently clear, so that the application of the provisions was not foreseeable for those involved. It did not regulate the amount of time of the eavesdropping, so as to determine the intercepted conversations. In the cases of *Kruslin* v. *France*[216] and *Huvig* v. *France*,[217] the Court declared that telephone tapping is an interference by a public authority without any doubt (see also *Klass* v. *Germany* and *Malone* v. *The United Kingdom*). In case of lawful interceptions, there are some established expectations: the impugned measure should have some basis in domestic law which has to be clear, and the rules on this subject have to be detailed, especially as the available technology is becoming more sophisticated. In short, French law, written and unwritten, does not indicate with reasonable clarity the scope and manner of exercising the relevant discretion conferred on the public authorities. So if law did not indicate with the sufficient clarity the scope and manner of exercise of the authorities' discretion in this area, the solution is not Convention compliant (see also *Rotaru* v. *Romania*).

The case of *Niemietz* v. *Germany*[218] calls the attention to the importance of professional secrecy and the need for special protection. In this case, the police raided a law firm. Although the intervention was based on the law, and the aims of the intervention were lawful, the court found that it was neither necessary nor proportionate because the breach of professional secrecy was not considered proportionate to the circumstances. The warrant was very broad, without any limitation because it contained that the search and seizure should be directed to such documents which are suitable to clarify the identity of a writer of a letter. Thus, one can conclude that professional secrets represent a particularly sensitive phenomenon and demand increased protection. [219]

According to Strasbourg in the case of *Funke v. France*,[220] three of the four component rights protected by ECHR Article 8(1) were at issue: right to respect for private life, home and correspondence. This case concerned the search of the applicant's home by French customs authorities in order to find some financial documents. The Commission considered that the interferences in question were in the interests of "the economic well-being of the country" and "the prevention of crime" so there was an acceptable legitimate aim. However, for the following reasons, the Court found that France had violated the Convention:

a. absence of the need for a judicial warrant;
b. the relevant legislation and practice must afford adequate and effective safeguards against abuse (see also *Klass* v. *Germany*). In contrast, French law appeared to be too lax and full of loopholes for the interferences with the applicant's rights to have been strictly proportionate to the legitimate aim pursued;
c. and the customs authorities had very broad powers; in particular, they had exclusive competence to assess the expediency, number, length and scale of inspections.[221]

---

[216] *Kruslin* v. *France*, Judgment of 24 April 1990, Application no. 11801/85.
[217] ,*Huvig* v. *France*, Judgment of 24 April 1990, Application no. 11105/84.
[218] *Niemietz* v. *Germany*, Judgment of 16 December 1992, Application no. 13710/88.
[219] A lawyer's computer files led to a finding that the search and seizure was disproportionate in violation of Article 8 in the Case of *Wieser and Bicos Beteiligungen GmbH* v. *Austria* (Judgment of 16 October 2007, Application no. 74336/01), and interference with the applicant's residential and business premises was found to be disproportionate with Article 8 because it related to criminal proceedings against his son (and not the applicant) that concerned a relatively minor road traffic offence (*Buck* v. *Germany* Judgment of 12 January 2010, Application no. 4158/05.).
[220] *Funke* v. *France*. Judgment of 25 February 1993, Application no. 10828/84.
[221] Searches without specified judicial warrant were also examined in the following cases: *Lavents* v. *Latvia* (Judgment of 28 November 2002, Application no. 58442/00.), *Camenzind* v. *Switzerland* (Judgment of 16

In the case of *Halford* v. *the United Kingdom*,[222] the Court also found that Merseyside Police had violated Article 8 by intercepting the employee's telephone calls within the internal telephone system at the Merseyside Police Headquarters. From 1983, Ms. Halford was the most senior-ranking female police officer in the United Kingdom. In her office were two telephones, one of which was for private use. In order to obtain information to use against her in a discrimination proceeding, her calls were controlled and no warnings were given to Ms. Halford. In the Court's view, it is clear from its case-law that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8(1). In this case, the Court found that the Interception of Communications Act (1985) which otherwise was adopted after the case of Malone only applied to a "public telecommunications system" and it did not regulate interception of internal systems, so under these circumstances this interference was not "in accordance with the law".

Because of the particular circumstances of the case, we did not find any relevant indication of using "security" or "crime" in the argumentation of the ECtHR but the Court analysed the notions of privacy and private life.[223]

In chronological order, almost at the same time, two relevant decisions were made, the first of which was the case of *Rotaru v. Romania*[224]. This case dealt with secret surveillance and storage of information. In order to grant an additional state aid to the applicant, a public authority needed to obtain various pieces of information about the applicant's past, in particular his studies, his political activities and criminal record, some of which had been gathered more than 50 years earlier. The Court confirmed its previously explained position that powers of secret surveillance of citizens are tolerable under the Convention only in so far as it is strictly necessary for safeguarding the democratic institutions (see *Klass and Others* v. *Germany*). In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of private life. That was all the more so in the instant case as some of the information had been declared false and was deemed likely to injure the applicant's reputation. Romania did not satisfy the requirements of the Convention because the Court found insufficient legal controls on the collection and storage

---

December 1997, Application no. 21353/93.), *Van Rossem* v. *Belgium* (Judgment of 9 December 2004, Application no. 41872/98.). In the case of *Chappell* v. *The United Kingdom* (Judgment of 30 March 1989, Application no. 10461/83), according to the applicant, the decision of the High Court, namely simultaneous searches by 16 or 17 people, made the execution of the order "more oppressive than it should have been". The Court found that the interference was "necessary in a democratic society" to protect the rights of others, that is the plaintiffs' copyright. However, in case of *Ernst and others* v. *Belgium* (Judgment of 15 July 2003, Application no. 33400/96), the Court found against the Convention when warrants ordered the search in journalists' offices, homes and cars at the same time in parallel, and warrants permitted the search for and seizure of "any document or object that might assist the investigation". In the case of *McLeod* v. *The United Kingdom* (Judgment of 23 September 1998, Application no. 2755/94), the police entered into a private house in order to prevent a suspected crime. The interference is verifiable in order to prevent crime or disorder but in this special case, the police action was disproportionate to that aim. In the case of *Keegan* v. *The United Kingdom* (Judgment of 18 July 2006, Application no. 28867/03), the breach of Article 8 rested on that; although the police had a warrant to search a house, the search was premature and unjustified.

[222] *Halford* v. *The United Kingdom*, Judgment of 25 June 1997, Application no. 20605/92.

[223] Violation of Article 8 was also found in the case of *Copland* v. *The United Kingdom* (Judgment of 3 April 2007, Application no. 62617/00). The applicant was required to work closely with the Deputy Principal (DP) at her workplace. During her employment, the applicant's telephone, e-mail and Internet usage were subjected to monitoring at the DP's instigation. Naturally, the Court held that there had been a violation of Article 8 of the Convention. In this judgment, the Court analysed the meaning and the relevance of the "scope of private life".

[224] *Rotaru* v. *Romania*, Judgment of 4 May 2000, Application no. 28341/95.

of information. The Court did not accept the defence of Romania that the requirements[225] in connection with the rights guaranteed by Article 8 were developed before the country's joining the Convention.[226]

In the case of *Khan v. The United Kingdom*,[227] the police had recordered the applicant's conversation with his friend in order to provide proof that Mr. Khan was dealing in drugs. The surveillance equipment had been installed by the police under the regulation of the guidelines cited below. One of the most important statements in the decision was that the Court found the tape recording a conventional method of surveillance. The central argumentation was whether the guidelines could be regarded as sufficient legal basis. According to Strasbourg, there was no domestic law whatsoever regulating the use of covert listening devices at the relevant time; because of this, the interference was not "in accordance with the law".

In both of the above cases, the Government referred to the guidelines on the use of equipment in police surveillance operations (the Home Office Guidelines of 1984) which provides that only chief constables or assistant chief constables are entitled to give authorisation for the use of such devices. The authorising officer should ensure that the following criteria are met:

a. the investigation concerns serious crime,
b. normal methods of investigation have been tried and failed, or because of the nature of things, are unlikely to succeed if tried,
c. there must be a good reason to think that the use of the equipment would be likely to lead to an arrest and a conviction, or where appropriate, to the prevention of acts of terrorism,
d. the use of equipment must be operationally feasible.[228]

The Government would have had to satisfy these regulations that the operation of secret surveillance was "in accordance with the law".

The absence of legal regulation and the insufficient legal basis were examined in some other cases, too. In *Heglas* v. *Czech Republic*,[229] the applicant was an organiser of a robbery but after this serious crime, only his partner was arrested. Under Czech law, the applicant's mobile telephone was placed under surveillance and body-mounted listening devices were used with the help of one of his friends. The problem was that at the relevant time, there was no legal regulation because the surveillance was continued between 21 January and 21 February 2000 and the two cited acts had come into force only on 1 July 2000 and on 1 January 2002. So the Court held that the interference was not "in accordance with the law" and concluded that there had been a violation of Article 8.

In the case of *Bykov* v. *Russia*,[230] the applicant complained, in particular, about a covert recording used as evidence in the criminal proceedings against him and about the length of his

---

[225] In the Government's submission, three conditions had to be satisfied before the interference with the right to respect for private life: information had to have been stored about the person concerned; use had to have been made of it; and it had to be impossible for the person concerned to refute it.

[226] See also the cases of *The Association for European Integration and Human Rights and Ekimdzhiev* v. *Bulgaria* (Judgment of 7 June 2007, Application no. 62540/00) and *Iordachi* v. *Moldova* (Judgment of 10 February 2009, Application no. 25198/02)

[227] *Khan* v. *The United Kingdom*, Judgment of 12 May 2000, Application no. 35394/97.

[228] In judging how far the seriousness of the crime under investigation justifies the use of a particular surveillance technique, authorising officers should ensure that the degree of intrusion into the privacy of those affected is commensurate with the seriousness of the offence.

[229] *Heglas* v. *Czech Republic*, Judgment of 1 March 2007, Application no. 5935/02.

[230] *Bykov* v. *Russia*, Judgment of 10 March 2009, Application no. 4378/02.

pre-trial detention. The Court held that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right for private life and correspondence". In the Court's opinion, these principles apply equally to the use of a radio-transmitting device, which, in terms of the nature and degree of the intrusion involved, is virtually identical to telephone tapping.

The insufficiently clear legal basis in relation to assistance given by the police to an individual in order to record his telephone conversations with the applicant was also determined in the case of *Van Vondel* v. *Netherlands*.[231] The applicant was a police officer in the Netherlands and his telephone conversations with one of his informers had been recorded with devices provided by the police. Authorities are not governed by rules aimed at providing legal guarantees against arbitrary acts. The applicant was deprived of the minimum degree of protection to which he was entitled under the rule of law in a democratic society. The Court found that the interference in issue was not "in accordance with the law" and the notion of "private life" must not be interpreted restrictively.

From several aspects, a quite complex case is *P. G. and J. H.* v. *The United Kingdom*.[232] The applicant was suspected of a serious crime. In order to obtain relevant information, the police placed some listening devices in his home and after his arrest also in his cell without any legal determination. Before his arrest, the police took photographs and video footage of him and audio surveillance was in progress. The applicants complained that their voices were recorded secretly when they were being charged at the police station and while they were being held in their cells (recording of the applicants' voices at a police station, following their arrest on suspicion of being about to commit a robbery). The Court held that because of the surveillance before the arrest, the interference with the applicants' private lives or correspondence was unequivocal, but there was no violation of Article 8, as the process was sufficiently prescribed by domestic law and was used in a proportionate manner. But violation of Article 8 was established because, at the time of the events, there had been no statutory system to regulate the use of covert listening devices by the police on their own premises. In this case, the Court also analysed the meaning of "in accordance with the law" (see in detail *Kopp* v. *Switzerland*) and "necessary in a democratic society". There was also an important part of the judgment which presented the notion of "interference with private life" (see in detail *Dudgeon* v. *The United Kingdom*; *Niemietz* v. *Germany*; *B.* v. *France*).

In the case of *Perry v. The United Kingdom*,[233] the applicant was filmed on video in the custody suite of a police station and this tape was used in a criminal proceeding and a trial. The applicant complained that he was covertly videotaped by the police (in breach of the statutory code of practice) and this procedure violated his right to respect for private life. Perry was in the police station because he had been brought there to attend an identity parade in which he had refused to participate. According to the Government, the filming did not take place in a private place; it was carried out in the custody suite of the police station which was a communal administrative area. Further, the applicant was not filmed for surveillance purposes, but for identification purposes and only for use in the criminal proceedings (it was not broadcast). The Court stated that the permanent recording of the footage and its inclusion in a montage for further use may therefore be regarded as the processing or collecting of personal data about the applicant. The Court stated that the interference was not therefore "in

---

[231] *Van Vondel* v. *Netherlands*, Judgment of 25 October 2007, Application no. 38258/03.
[232] *P. G. and J. H.* v. *The United Kingdom*, Judgment of 25 September 2001, Application no. 44787/98.
[233] *Perry* v. *The United Kingdom*, Judgment of 17 July 2003, Application no. 63737/00.

accordance with the law" as required by the second paragraph of Article 8 and, thus, there had been a violation of this provision.

An interesting case is *Peck* v. *the United Kingdom*,[234] given the fact that Mr. Peck cut his wrists in the streets and cameras installed in public places recorded his action. According to the Court, this interference with the applicant's private life was unnecessary, unreasonable and accordingly unconventional.

In the case of *Uzun v. Germany*,[235] the Court did not dispute that a GPS placed in a vehicle is capable of systematic collection of data but given the fact that German law provides appropriate guarantees and the investigation was conducted because of a serious alleged offence (bomb attacks), the Court did not find a violation of Article 8. In the first case involving GPS, the Court said that GPS caused less of an interference with a person's private life than surveillance of telecommunications; hence, the stricter standards applied in such cases were not directly applicable.

In the light of technological developments, we present two additional cases in this annex. The collection and retention in police records of information about suspects (e.g., fingerprints, cell samples and DNA profiles) can be justified and acceptable for numerous reasons such as prevention of disorder or crime or public safety.

There was no violation of Article 8 in the Case of *Leander* v. *Sweden*,[236] in which the applicant complained that he did not win a public position because of information used against him that the police had collected. The applicant had been at the Naval Museum in Karlskrona, next to a restricted military security zone, and after a personnel control had been carried out on him, the commander-in-chief of the navy decided not to recruit him because he had been a member of the Communist Party and of a trade union. The Court declared that the Swedish Government had been entitled to consider that the interests of national security prevailed over the applicant's individual interests in this case. The Court also found that the Swedish rules are transparent and having regard to the guarantees of rules, the interception was necessary and proportionate due to the national security in a democratic society.

At the beginning of the description of the case of *S and Marper* v. *the United Kingdom*,[237] it is important to clarify the Court's fundamental findings. According to Strasbourg, "The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests." In this case, the applicants' fingerprints, cell samples and DNA profiles were fixed and preserved after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in the other case. The Court said that balance must be struck between use of modern scientific techniques in the criminal-justice system and private life and the former could not be allowed at any cost and would not enjoy priority automatically and unconditionally. The Court held that this type of restriction to the right to private life is justified only if it satisfies the urgent needs of a society, if it is

[234] *Peck* v. *The United Kingdom*, Judgment of 28 January 2003, Application no. 44647/98.
[235] *Uzun* v. *Germany*, Judgment of 2 September 2010, Application no. 35623/05.
[236] *Leander* v. *Sweden*, Judgment of 26 March 1987, Application no. 9248/81.
[237] *S and Marper* v. *The United Kingdom*, Judgment of 4 December 2008, Application nos. 30562/04 and 30566/04.

proportionate to the aim pursued and if the authority is provided by relevant and sufficient reasons.[238]

[238] For cases with similar reasoning, see also *Gardel* v. *France* (Judgment of 17 December 2009, Application no. 16428/05.) in which the 30-year registration period, because of a violent crime, was conventional having regard to the fact that vulnerable groups are entitled to special protection. In the case of *Turek* v. *Slovakia* (Judgment of 14 February 2006, Application no. 57986/00), there was a breach of Article 8 because there was no effective remedy against the data collection in connection with the applicant's former life. In the case of *Hewitt and Harman* v. *The United Kingdom* (Judgment of 9 May 1989, Application no. 12327/86), former NCCL staff Harriet Harman (Legal Officer) and Patricia Hewitt (General Secretary) had been under MI5 surveillance while working at the NCCL. In 1989, the European Court of Human Rights ruled that there was a lack of clarity about when someone might be subjected to surveillance and inadequate safeguards. There had been a breach of the right to respect for the women's private lives protected by Article 8. Cases involving photographs taken during demonstrations and other events include *Friedl* v. *Austria* (Judgment of 31 January 1995, Application no. 15225/89), *Sciacca* v. *Italy* (Judgment of 11 January 2005, Application no. 50774/99), *Nikolaishvili* v. *Georgia* (Judgment of 13 January 2009, Application no. 37048/04) and *Toma* v. *Romania* (Judgment of 24 February 2009, Application no. 42716/02).

APPENDIX II: SECURITY VS. PRIVACY/DATA PROTECTION IN THE CASE LAW OF THE ECTHR

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
5029/71	*Klass and Others* v. *Germany*	6 Sept. 1978	Surveillance of communication – telephone tapping – by a judicial authority and combating terrorism	In this case, the Court found no violation of Article 8: the law challenged by the applicants (imposing restrictions on the secrecy of mail, post and telecommunications) was found by the Court to be necessary in a democratic society in the interests of national security and for the prevention of disorder or crime.	The main principle is that the concerned person has to be informed about the relevant information at least after the interception, but rules are often given exemptions for the States, where it is likely that such information would prejudice the purpose of the intervention, such as national security.	X	X	–	X	X	Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake secret surveillance of subversive elements operating within its jurisdiction. Nevertheless, the Court, being aware of the danger inherent in secret surveillance measures "of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate"	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510

[239] According to the categorization by the ECtHR

* We indicate those cases only where these notions are used in a relevant context. Where these categories are left empty, the text is available in French only, or not available at all.

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
8691/ 79	*Malone* v. *the United Kingdom*	2 Aug. 1984	Surveillance of communi- cation – telephone tapping – by the police	Violation of Article 8 because the interception of the applicant's telephone conversations – in the context of his trial for handling stolen goods – and the "metering" of his calls (registration of the numbers dialled on a particular telephone) had not been in accordance with the law.	limitations for the prevention of crime / limitations for the prevention of disorder	**X**	**X**	**X**	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533
9248/ 81	*Leander* v. *Sweden*	26 March 1987	Files kept by the judicial authorities – in an employment context	The storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8; the subsequent use of the stored information has no bearing on that finding. Use of a secret police file in the recruitment of a carpenter. He had been working as a temporary replacement at the Naval Museum in Karlskrona, next to a restricted military security zone, and after a personnel control had been carried out on him, the commander-in-chief of the navy decided not to recruit him. The applicant had formerly been a member of the Communist Party and of a trade union.	No violation of Article 8: the safeguards contained in the Swedish personnel-control system satisfied the requirements of Article 8. The Court concluded that the Swedish Government had been entitled to consider that the interests of national security prevailed over the applicant's individual interests in this case.	**X**	**X**	**X**	**X**	**X**		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57519

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
10461 /83	*Chappell* v. *the United Kingdom*	30 March 1989		The applicant was a videotape dealer. Some companies, to protect film producers and distributors from activities carried out in breach of copyright, obtained in civil proceedings a court order against the applicant. According to the applicant, the decision of the High Court, namely simultaneous searches by 16 or 17 people, made the execution of the order 'more oppressive than it should have been'. The Court found that the interference was "necessary in a democratic society" to protect the rights of others, that is, the plaintiffs' copyright.		–	X	–	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57459
12327 /86	*Hewitt and Harman and N.* v. *The United Kingdom*	9 May 1989	Files kept by the judicial authorities – in an employment context	Former NCCL staff Harriet Harman (Legal Officer) and Patricia Hewitt (General Secretary) had been under MI5 surveillance while working at the NCCL. In 1989, the European Court of Human Rights ruled that there was a lack of clarity about when someone might be subjected to surveillance and inadequate safeguards. There had been a breach of the right to respect for the women's private lives protected by Article 8.								–

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
11105 /84	*Huvig* v. *France*	24 April 1990	Surveillance of communication – telephone tapping – by a judicial authority	In two cases, France was condemned because, although wiretapping was continued with judicial content, the law was not sufficiently clear, so the application of the relevant provisions was not foreseeable for the concerned. For example, the duration of the interception of telephone conversations was not regulated.		**X**	**X**	**X**	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57627
11801 /85	*Kruslin and Huvig* v. *France*	24 April 1990	Surveillance of communi-cation – telephone tapping – by a judicial authority	In two cases, France was condemned because, although wiretapping was continued with judicial content, the law was not sufficiently clear, so the application of the relevant provisions was not foreseeable for the concerned. For example, it the duration of the interception and the attachment of telephone conversations weren't regulated.	Telephone tapping ordered by an investigating judge in a murder case. Violation of Article 8 because French law did not indicate with the sufficient clarity the scope and manner of exercise of the authorities' discretion in this area.	**X**	**X**	**X**	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57626

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
13564 /88	*L.* v. *Norway*	8 June 1990			The main principle is that, at least after the interception, the concerned has to be informed about the relevant information but often there are some exemptions for the States, when it is likely that such information would prejudice the purpose of the intervention, for example, national security.	–	–	–	**X**	**X**		http://echr.globe24h.com/caselaw/1990/06/19900608/l-v-norway-13564-88.shtml
13274 /87	*F.S. and T.S.* v. *Italy*	6 Sept. 1990	Surveillance of communi-cation – telephone tapping	Third party's telephone interception led to criminal proceedings against him. The European Commission of Human Rights found that the interception was based on the appropriate legal background, and the measure was considered necessary in a democratic society.		–	–	–	–	–		–

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
12433 /86	*Lüdi* v. *Switzer-land*	15 June 1992	Surveillance of communi-cation – telephone tapping	In the present case, the use of an undercover agent did not, either alone or in combination with the telephone interception, affect private life within the meaning of Article 8.		–	X	–	–	–		http://www.interpretconsulting.com/RIPA/Cases/Ludi%20v%20switzerland%20-%20full%20text.pdf
13710 /88	*Niemietz* v. *Germany*	16 Dec. 1992	Stop & search	The applicant lawyer's office was searched by police. The search was found to impinge on professional secrecy to an extent that was disproportionate, primarily because the warrant had been drawn in very wide terms, permitting the search and seizure of 'documents', without limitation.	Importance of professional secrecy; the meaning of private life	X	X	–	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57887

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
10828 /84	*Funke* v. *France*	25 Feb. 1993		This case concerned the search of the applicant's home by French authorities. In January 1980, customs officers and a policeman discovered foreign bank statements during a search of the applicant's home. The customs officers ordered the applicant to produce certain documents, which he subsequently stated he was unable to do.		–	X	–	X	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57809
14838 /89	*A* v. *France*	23 Nov. 1993	Surveillance of communi-cation – telephone tapping – by the police	Recording by a private individual, with the assistance of a police superintendent in the context of a preliminary investigation, of a telephone conversation with the applicant, who, according to the individual concerned, had hired him to carry out a murder. Violation of Article 8 since the recording had not been carried out pursuant to a judicial procedure and had not been ordered by an investigating judge.		X	X	–	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57848

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
21482 /93	*Christie* v. *the United Kingdom*	27 June 1994	Surveillance of communi- cation – telex	Key element: interception and transmission of official telexes by intelligence agencies to other security agencies. The intervention was based on appropriate legal background, and the measure was considered necessary for national security and the economic well-being of the country.		–	**X**	–	**X**	**X**		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-1870
21207 /93	*K.D.* v. *the Nether- lands*	30 Nov. 1994	Surveillance of communication – telephone tapping – by a judicial authority	The European Commission of Human Rights found the application inadmissible, finding that the Dutch law is sufficiently precise.		**X**	**X**	**X**	**X**	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-2412

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
20605/92	*Halford* v. *the United Kingdom*	25 June 1997	Surveillance of communi-cation – telephone tapping – by a judicial authority; files kept by the judicial authorities – in an employment context	The applicant, who was the highest-ranking female police officer in the United Kingdom, brought discrimination proceedings after being denied promotion to the rank of Deputy Chief Constable over a period of seven years. She alleged that her telephone calls had been intercepted with a view to obtaining information to use against her in the course of the proceedings. Violation of Article 8 as regards the interception of calls made on the applicant's office telephones. No violation of Article 8 as regards the calls made from her home, since the Court did not find it established that there had been interference regarding those communications.		**X**	**X**	**X**	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58039

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
23244 /94	*Kopp* v. *Switzer-land*	25 March 1998	Protection of personal data – general principles	Despite the efforts of the law in connection with surveillance of lawyers' communication, the regulation didn't ensure the necessary guarantees. The regulation was not sufficiently precise; it didn't clarify who and under what conditions should decide on such matters. This method has not provided the expected minimum protection in a democratic society for the lawyer applicant.	The storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8; the subsequent use of the stored information has no bearing on that finding.	–	**X**	–	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58144
27671 /95	*Valen-zuela Contreras* v. *Spain*	30 July 1998	Surveillance of communi-cation – telephone tapping – by a judicial authority	Monitoring of telephone line in connection with criminal proceedings against subscriber.	The regulation on such matters must be rigorous and precise to ensure the decision-makers cannot exercise too broad discretion.	**X**	**X**	–	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58208
23618 /94	*Lambert* v. *France*	24 Aug. 1998	Surveillance of communi-cation – telephone tapping – by a judicial authority	The interpretation from French authorities according to which the illegality of wiretapping could be referred to only the telephone line subscribers and a third party no. is unconventional.		**X**	**X**	**X**	**X**	-		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58219

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
27798 /95	*Amann* v. *Switzer-land*	16 Feb. 2000	Protection of personal data – general principles	Creation and storage of the file were not "in accordance with the law", since Swiss law was unclear as to the authorities' discretionary power in this area.		**X**	**X**	**X**	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
28341/95	*Rotaru* v. *Romania*	4 May 2000	Files and access to data – access to data kept by secret services	In order to grant a state aid, a public authority needed to obtain various pieces of information about the applicant's past life in particular, his studies, his political activities and his criminal record, some of which had been gathered more than 50 years earlier. The Court confirmed the previously explained position that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding democratic institutions.	In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life". That is all the more so in the instant case as some of the information had been declared false and was likely to injure the applicant's reputation. Romania did not satisfy the requirements of the Convention because the Court found insufficient legal controls on the collection and storage of information. The Court did not accept the defence of Romania that the requirements in connection with the rights secured by Article 8 were developed before the country's ratification of the Convention.	X	X	X	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
35394 /97	*Khan* v. *the United Kingdom*	12 May 2000	Surveillance of communi-cation – telephone tapping – by the police	For the same reason as in the case of *Malone* v. *The United Kingdom*, the Court found a violation of Article 8 in *Khan* v. *the United Kingdom*. Surveillance of the applicant by means of a listening device in connection with his prosecution for drug-trafficking offences.	Violation of Article 8; surveillance of the applicant by means of a listening device in connection with his prosecution for drug-trafficking offences.	**X**	**X**	–	**X**	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58841
44787 /98	*P.G. and J.H.* v. *The United Kingdom*	25 Sept. 2001	Surveillance of communi-cation – telephone tapping – by the police and surveillance of communi-cation – bugging of a flat	The case concerned the recording of the applicants' voices at a police station, following their arrest on suspicion of being about to commit a robbery. As there was no domestic law regulating the use of covert listening devices at the relevant time …the interference in this case was not "in accordance with the law" as required by Article 8(2) of the Convention, and there was therefore a violation of Article 8.	At the time of the events, there had been no statutory system to regulate the use of covert listening devices by the police on their own premises. The Court also found a violation of Article 8 on account of the police's installation of a covert listening device at a flat used by one of the applicants, which was not in accordance with the law.						The decision was made after 11 September (sic!)	http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-419654-419935

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
48521 /99	*Arm-strong* v. *The United Kingdom*	16 July 2002	Surveillance of communi-cation – telephone tapping	Member States have to place great emphasis on the necessity of sufficiently precise and detailed legislation, and in every other case, authorities have very broad discretion in regard to telephone interceptions. In the absence of these conditions, even in the most important and obvious cases States expose themselves to blame.		–	–	–	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60612
47114 /99	*Taylor-Sabori* v. *The United Kingdom*	22 Oct. 2002	Surveillance of communi-cation – messaging systems	The applicant was charged with conspiracy to supply a controlled drug – using a "clone" of his pager. Violation of Article 8: there had been no statutory system to regulate the interception of pager messages transmitted via a private telecommunication system.		**X**	**X**	–	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60696
44647 /98	*Peck* v. *The United Kingdom*	28 Jan. 2003	Protection of personal data – general principles; new technologies – closed-circuit television	Violation of Article 8 on account of the disclosure to the media of footage filmed in a street by a closed-circuit television (CCTV) camera installed by the local council, showing the applicant cutting his wrists.	The Court found that the disclosures were not accompanied by sufficient safeguards and, therefore, constituted a disproportionate and unjustified interference with Mr Peck's private life.	**X**	**X**	–	–	–	The jurisprudence sets out the following principle with respect to the right to privacy: the concept of private life is interpreted broadly	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60898

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
63737 /00	*Perry* v. *The United Kingdom*	17 July 2003		The applicant was filmed on video in the custody suite of a police station and this tape was used in a criminal proceeding and a trial. The applicant complained that he was covertly videotaped by the police (in breach of the statutory code of practice) and this procedure violated his right to respect for private life.		**X**	**X**	**–**	**X**	**X**		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61228
50210 /99	*Doerga* v. *The Netherlands*	27 April 2004	Surveillance of communication – telephone tapping	The applicant's phone calls from the prison were intercepted. This particular case lacked sufficiently clear legal provisions.		**X**	**X**	**–**	**X**	**X**		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61747
59842 /00	*Vetter* v. *France*	31 May 2005	Surveillance of communication – bugging of a flat	Following the discovery of a body with gunshot wounds, the police, suspecting that the applicant had carried out the murder, installed listening devices in a flat to which he was a regular visitor. Violation of Article 8: French law did not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in relation to listening devices.							The decision is available only in French.	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-69188

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
71611 /01	*Wisse* v. *France*	20 Dec. 2005	Surveillance of communi-cation – telephone tapping – by a judicial authority								The decision is available only in French.	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-71735
62332 /00	*Seger-stedt-Wilberg and Others* v. *Sweden*	6 June 2006	Files kept by judicial authorities	The applicants complained about the storage of certain information about them in Swedish Security Police files and the refusal to reveal the extent of the information stored. Violation of Article 8 on account of the storage of the data, except as regards the first applicant, since the storage of information concerning bomb threats against her in 1990 was justified. No violation of Article 8: the interest of national security and the fight against terrorism prevailed over the interests of the applicants on access to information about them in the Security Police files. Violation of Article 13: no remedy available to secure the destruction of the files or the erasure or rectification of information kept in them.		–	X	X	X	X		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
62617/00	*Copland* v. *The United Kingdom*	3 April 2007	Surveillance of communi-cation –- messaging systems and new technologies – e-mail; files kept by the judicial authorities – in an employment context	The monitoring of the applicant's e-mails in the workplace was in breach of Article 8.	The Court held that the monitoring had not been in accordance with the law, there having been no domestic law at the relevant time to regulate monitoring.	**X**	**X**	**X**	–	–	Such limitation of the right to privacy is deemed as necessary if it is based on national legislation.	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
38258 /03	*Van Vondel* v. *The Nether-lands*	25 Oct.. 2007	Surveillance of communi-cation – telephone tapping – by the police	The applicant was a police officer for the Criminal Intelligence Service. His telephone conversations with one of his informers had been recorded with devices provided by the National Police Internal Investigation Department, in the context of a parliamentary inquiry into criminal investigation methods in the Netherlands due to a controversy surrounding the North-Holland/Utrecht Interregional Criminal Investigation Team. Violation of Article 8: the applicant had been deprived of the minimum degree of protection to which he had been entitled under the rule of law in a democratic society (the Court did not find it acceptable that the authorities had provided technical assistance which was not governed by rules providing guarantees against arbitrary acts).		–	–	X	–	–	Although the Court understands the practical difficulties for an individual who is or who fears to be disbelieved by investigation authorities to substantiate an account given to such authorities and that – for that reason – such a person may need technical assistance from these authorities, it cannot accept that the provision of that kind of assistance by the authorities is not governed by rules aimed at providing legal guarantees against arbitrary acts. It is therefore of the opinion that, in respect of the interference complained of, the applicant was deprived of the minimum degree of protection to which he was entitled under the rule of law in a democratic society.... In the light of the foregoing, the Court finds that the interference in issue was not "in accordance with the law". This finding suffices for the Court to hold that there has been a violation of Article 8 of the Convention.	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-82962

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
30562 /04; 30566 /04	*S. and Marper* v. *the United Kingdom*	4 Dec. 2008	Biometric data and new technologies – electronic databases	"The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests."	Violation of Article 8 on account of the indefinite retention in a database of the applicants' fingerprints, cell samples and DNA profiles after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in the other case.	**X**	**X**	**X**	–	–	The Court considered That any State claiming a pioneer role in the development of new technologies bore special responsibility for "striking the right balance". The Court concluded that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests.	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
25198 /02	*Iordachi and Ors* v. *Moldova*	10 Feb. 2009				–	X	–	X	–	The jurisprudence sets out the following principles with respect to the right to privacy: *the victim of surveillance need not prove that surveillance was specifically used against him or her; laws regulating surveillance have to give a sufficiently clear indication about the circumstances in which, and the conditions under which, surveillance in public places is permissible; effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it.*	http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
4378/02	*Bykov* v. *Russia*	10 March 2009	Radio-transmitting device.	The Court held that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right for private life and correspondence".	In the Court's opinion, these principles apply equally to the use of a radio-transmitting device, which, in terms of the nature and degree of the intrusion involved, is virtually identical to telephone tapping.	**X**	**X**	–	**X**	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91704
35623/05	*Uzun* v. *Gemany*	2 Sept. 2010	New technologies – Global Positioning System (GPS)	Mr Uzun, suspected of involvement in bomb attacks by a left-wing extremist movement, was monitored via GPS and the evidence obtained was used in the criminal proceedings against him. Given that the criminal investigation had concerned very serious crimes, the Court found that the GPS surveillance of Mr Uzun had been proportionate.	First case concerning GPS surveillance before the European Court of Human Rights.	**X**	**X**	**X**	**X**	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-100293

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
420/07	*Köpke* v. *Germany*	5 Oct. 2010	video surveillance	The case concerned covert video surveillance of a supermarket cashier resulting in her dismissal for theft. The Court concluded that the domestic authorities had struck a fair balance between the employee's right to respect for her private life and her employers' interest in the protection of its property rights and the public interest in the proper administration of justice.	The Court observed, however, that the competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life were made possible by new, more sophisticated technologies.	**X**	**X**	**X**	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-101536
30194/09	*Shimovolos* v. *Russia*	21 June 2011	Surveillance of communication – secret surveillance database	The case concerned the registration of a human rights activist in a secret surveillance security database and the tracking of his movement as well as his subsequent arrest. Violation of Article 5 § 1 and a Violation of Article 8: the database in which Mr Shimvolos' name had been registered had been created on the basis of a ministerial order which had not been published and was not accessible to the public. Therefore, people could not know why individuals were registered in it, what type of information was included and for how long, how it was stored and used or who had control over it.		–	**X**	**X**	–	–		http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105217

Appl. no.	Name of decision	Date of decision	Category[239]	Short description	Relevance	privacy*	private life*	data prot.*	security*	nati./ publ. security*	Notes	Source
36662 /04	*Draksas* v. *Lithuania*	31 July 2012	Surveillance of communi-cation – telephone tapping – by a judicial authority									http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-112588
25812 /03	*Kruit-bosch* v. *Romania*	Pending case	Surveillance of communi-cation – telephone tapping – by the police	The case involves audio and video recordings by police officers.								