Project acronym:	IRISS
Project title:	Increasing Resilience in Surveillance Societies
Project number:	290492
Programme:	FP7-SSH-2011-2
Objective:	To investigate societal effects of different surveillance practices from a multi-disciplinary social science and legal perspective.
Contract type:	Small or medium-scale focused research project
Start date of project:	01 February 2012
Duration:	36 months

Deliverable D2.3: The Legal Perspective

A report presenting a review of the key features raised by legal perspectives of surveillance and democracy

Coordinator:	Vrije Universiteit Brussel (VUB)
Dissemination level:	PU
Deliverable type:	Report
Version:	1
Submission date:	31 January 2013

	Lead	Contributors
Overview and overall editor	Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)	
Chapter 1: Introduction to the legal perspective	Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)	
Chapter 2: Surveillance and democracy: totalitarian and contemporary practices	Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)	Ivan Szekely and Beatrix Vissy, Eotvos Karoly Policy Institute (EKINT); Anthony Amicelle, Peace Research Institute Oslo (PRIO); Antonella Galetta Vrije Universiteit Brussel (VUB); Gemma Galdon Clavell, University of Barcelona (UB); Richard Jones, University of Edinburgh (UEdin)
Chapter 3: Surveillance and the European privacy and data protection framework	Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)	Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)
Chapter 4: Regulating Surveillance: comparative analysis of European national experiences	Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)	Ivan Szekely and Beatrix Vissy Eotvos Karoly Policy Institute (EKINT); Charles Raab and Richard Jones, University of Edinburgh (UEdin); Anthony Amicelle and Marit Moe-Price, Peace Research Institute Oslo (PRIO); Antonella Galetta and Gertjan Boulet, Vrije Universiteit Brussel (VUB); Gemma Galdon Clavell University of Barcelona (UB)
Conclusions about the legal perspective	Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)	

IRISS
INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES

IRISS WORK PACKAGE 2
TASK 2.3: THE LEGAL PERSPECTIVE

EXECUTIVE SUMMARY

This is an executive summary of a report presenting a review of the key features raised by legal perspectives of surveillance and democracy. It summarises the main themes and findings emerged in the development of IRISS Task 2.3.

THE LEGAL PERSPECTIVE

Task 2.3 reviews the key contributions to knowledge emerging from legal perspectives of surveillance and democracy. Included within this perspective are approaches which set out formal mechanisms for regulating surveillance technologies, different approaches to protecting fundamental rights and civil liberties and the emergence of legislative safeguards to counter possible infringements, and how these have changed over time in different democratic settings. This Task also considers the emergence and implementation of key laws, such as data protection legislation.

Overview

Task 2.3 consists of three main Chapters. Chapter 2 deals with the relationship between surveillance and democracy; Chapter 3 analyses the European privacy and data protection framework, and Chapter 4 compares European national experiences and approaches in regulating surveillance. IRISS Task 2.3 is closely related to Tasks 2.1 and 2.2, as well as to IRISS Work Package (WP) 1, especially as regards the impacts of surveillance on civil liberties and fundamental rights.

Chapter 2 (on the relationship between surveillance and democracy) contains two main Sections. The first investigates how surveillance was implemented under totalitarian regimes and how it affected the exercise of fundamental rights and civil liberties. The second presents the main issues at stake in the relationship between surveillance and democracy focusing on contemporary surveillance practices.
The relationship between surveillance and democracy entails the implementation of governmental and authoritative powers. However, surveillance is not the exclusive product of dictatorships and authoritative regimes, nor democracy can be ensured keeping our societies free from surveillance. These considerations come as a result of analysis of how surveillance has changed over time and its impacts on fundamental rights and civil liberties in different democratic settings. In the mid-1950s, for example, civil and political rights could be exercised relatively freely under the Communist regime in Hungary, despite the surveillance measures enforced by state authorities. Nonetheless, it is also noteworthy that surveillance does not only have a public dimension, but also a private one which should not be neglected. The risk of surveillance being non-democratic is real, no matter how mature a democracy is. Legislation and regulation have the key role of preventing and avoiding such a risk. However, the existence of a legal framework which is meant to regulate surveillance technologies and their use does not necessarily prevent the spread of surveillance in our societies. The pervasive use of surveillance for deterring and preventing crime and terrorism and the development of surveillance technologies in urban areas are examples of how surveillance, including of an intrusive kind, may continue to be used despite the existence of regulatory frameworks.

Chapter 3 (on the European privacy and data protection framework) includes five main Sections. The first deals with the right to privacy; the second focuses on the right to data protection; the third looks at the relationship between privacy, data protection and surveillance; the fourth investigates the legislative safeguards and formal mechanisms for regulating surveillance referring to the European Convention on Human Rights (ECHR) and the European Data Protection Directive; the fifth examines the European case law on surveillance. Specific surveillance categories are identified and analysed, namely: surveillance as listening; surveillance as watching; surveillance as collecting and storing; and surveillance as automated processing and profiling.
Surveillance is not only regulated through privacy and data protection instruments. On the contrary, there is an array of human rights and principles which contribute to set the legal framework that applies to surveillance. Nonetheless, the nature of these principles is not necessary legal. However, from a legal perspective, privacy and data protection can be considered as the main instruments for regulating surveillance. Article 8 ECHR represents the cornerstone of the protection of privacy, together with the jurisprudence of the European Court of Human Rights (ECtHR). Surveillance is not necessarily against privacy and data protection, nor does it constitute *per se* a violation of Art. 8 ECHR. Instead, Art. 8 ECHR is the synthesis of conflicting rights and interests that oppose each other when surveillance is at stake. This results especially from analysis of the principles of Art. 8.2 ECHR and from the case law of the ECtHR. There are gaps in privacy and data protection laws that regulate surveillance and they are only partially filled by the European case law.

Chapter 4 (on European national experiences and approaches in regulating surveillance) is composed of three main Sections. The first provides a general overview of the different privacy and data protection regimes that exist in Europe and emphasises their main features. The second compares different national experiences and legal traditions in regulating privacy and data protection with regards to surveillance, presenting the national cases of Belgium, Hungary, Spain, United Kingdom, and Norway. Finally, the third focuses on European Member States' national case law and presents some relevant decisions of national courts in cases relating to surveillance. In particular, cases concerning data retention, online surveillance and wiretapping are reported.
Privacy and data protection are broad, ambiguous and contentious concepts which are rooted in national constitutional values of European Member States. They encompass different dimensions that can be referred to as decisional privacy, informational privacy and local privacy. There is a rich tapestry of legal traditions and cultures at European level that generate in turn different privacy and data protection regimes. These differences are noticeable given the gap between the civil law and common law privacy regimes. In Western civil law countries privacy developed as a human rights demand and shaped the national constitutional framework from the late 1940s responding to the horrors of totalitarian regimes. By contrast, privacy protection in common law systems has been developed mainly in private law, as a legitimate interest protected by national tort law. Great efforts have been made at national level by Member States to implement European privacy and data protection laws in the last few decades and to regulate surveillance. However, remarkable differences still exist across Europe.

Key themes and emergent findings

The main themes of Task 2.3 can be summarised as follows:

A. analysis of the relationship between surveillance and democracy in different democratic settings, from an historical and legal perspective (Chapter 2, Sections 2-3);

B. analysis of the legal framework that applies to surveillance and its regulation, notably on the basis of legislation and case law on privacy and data protection (Chapter 3, Sections 1-6);

C. analysis of formal legal mechanisms and safeguards for regulating surveillance at European and national level (Chapter 3, Section 5 and Chapter 4, Sections 2-3),

D. analysis of different experiences and approaches in using and regulating surveillance in relation to the exercise of fundamental rights and liberties in Europe (Chapter 4, Sections 1-4).

The main findings of Task 2.3 can be summarised as follows:

A. privacy and data protection provide the legal framework for regulating surveillance. However, the legal framework that applies to surveillance is not clearly defined (Chapter 3, Section 2 and Chapter 4, Section 2);

B. the relationship between surveillance and democracy is usually explored from a public perspective, analysing the impacts of state surveillance on citizens' rights and liberties. However, private surveillance also plays an important role in shaping this relationship (Chapter 2, Section 3);

C. surveillance can affect the exercise of fundamental rights in democratic settings. It can challenge democracy and be non-democratic. However, the existence of specific legislation and/or regulations on the use of surveillance technologies does not necessarily prevent the spread of surveillance in our societies (Chapter 2, Section 3);

D. tensions between surveillance and democracy result from the effects and impacts of the former on fundamental rights. Indeed, the ECtHR recognises that secret surveillance can undermine or even destroy democracy on the grounds of defending it. However, the governance of surveillance often consists of balancing conflicting rights and interests, whose task is usually performed by Courts, on a case-by-case basis (Chapter 3, Sections 2-6 and Chapter 4, Section 4);

E. although the rights to privacy and data protection contain several significant safeguards against the spread of unfettered surveillance, surveillance is not only regulated through legal norms and principles, but also through values that are highly influenced by social and political values, such as accountability and transparency. In addition, remarkable differences exist at national level as to how privacy and data protection norms and principles are implemented (Chapter 4, Sections 1-4);

F. gaps and pitfalls can be found in legislation and case law on privacy and data protection with regards to surveillance. There is remarkable case law of the European Courts concerning surveillance which, however, contributes only partially to filling these gaps (Chapter 3, Sections 1-6).

Conclusion

IRISS Task 2.3 illustrates the legal framework which applies to surveillance, while raising key issues on the regulation of surveillance. It highlights the limits of legislation and case law in defining a clear set of norms and principles for regulating surveillance. As explained above, surveillance and its regulation are highly influenced by political and social variables that can be only partially explained through legal reasoning. Nevertheless, it is imperative to take these other aspects into account and so to consider IRISS Tasks 2.1 (the social perspective), 2.2 (the political perspective) and 2.3 (the legal perspective) in a systematic way. Similarly, the discourse about forms of resilience to surveillance in today's societies needs to consider these three perspectives. The themes and topics identified in Task 2.3 provide several inputs to the empirical research that will be developed in IRISS WPs 3, 4 and 5.

1. INTRODUCTION TO THE LEGAL PERSPECTIVE

Paul De Hert and Antonella Galetta, VUB

Surveillance has a certain impact on the exercise of fundamental rights. Privacy and data protection are the main human rights that are affected by surveillance practices, although, as argued in IRISS D.1, several other human rights may be infringed or at least influenced by surveillance. The relationship between surveillance and democracy in today's surveillance societies is based on social, political and legal safeguards that allow citizens to exercise their rights in a free and autonomous way, despite the growing surveillance trend. As a consequence, it is imperative to look for these guarantees and emphasise them not only to assess the legitimacy of certain surveillance practices but also understand if it makes sense to identify an acceptable level of surveillance in our societies.

Although their legal framework appears somehow vague and fragmented, privacy and data protection regulate surveillance to a certain extent and provide the legal basis for that purpose. Privacy in law, as we will see in Chapter 3 below, is a complex and contentious concept which is strongly linked to several legal values and principles such as legality, necessity, proportionality, foreseeability, accountability and transparency. Application of these principles answers the questions of why privacy matters, how it should be safeguarded and to what extent democratic states can add limitations to certain privacy practices. Given that the right to privacy is strongly linked and influenced by the aforementioned values and principles, it cannot be detached from them in the legal thinking and be regulated without taking these variables into account. Nonetheless, privacy and data protection are strongly influenced by principles and values whose nature is not only legal but also social and political. IRISS D.2.1 and D.2.2 analyse these two aspects respectively.

2. SURVEILLANCE AND DEMOCRACY: TOTALITARIAN AND CONTEMPORARY PRACTICES

Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)
Ivan Szekely and Beatrix Vissy, Eotvos Karoly Policy Institute (EKINT)
Anthony Amicelle, Peace Research Institute Oslo (PRIO)
Gemma Galdon Clavell, University of Barcelona (UB)
Richard Jones, University of Edinburgh (UEdin)

2.1 INTRODUCTION

This Chapter deals with the relationship between surveillance and democracy, focusing on how surveillance was deployed under totalitarian regimes and on contemporary surveillance practices. Recalling the main themes and findings of IRISS D.1 and in particular of Task 1.5 (on the impacts of surveillance on civil liberties and fundamental rights), this Chapter refers to the effects of surveillance and illustrates in particular how surveillance has changed over time.

This Chapter is composed of two main Sections. The first will look at surveillance practices adopted by totalitarian regimes and at how civil and political rights were exercised in dictatorships. We will start considering two understandings of surveillance, one negative (surveillance as repression); another less negative (surveillance as a tenet of modern bureaucracies). Both partly explain the experiences of form Communist Eastern European states. The experience of former Communist Hungary will be presented as a case example in this regard. The second Section will consider the exercise of fundamental rights and civil liberties in contemporary surveillance societies, focusing in particular on the impacts on human rights due to the use of CCTV in urban areas. Similarly, it will emphasise the widespread use of surveillance technologies for deterring and preventing crime and terrorism.

2.2 SURVEILLANCE, FUNDAMENTAL RIGHTS AND CIVIL LIBERTIES UNDER TOTALITARIAN REGIMES

As explained in IRISS D.1, several understandings of surveillance exist. Depending on these understandings, statements about the impact of surveillance on fundamental rights will differ.

A first understanding equates surveillance with totalitarianism. As Giddens has argued, "The expansion of surveillance in the hands of the state can support a class-based totalitarianism of the right (fascism); but it can also produce a strongly developed totalitarianism of the left (Stalinism)".[1] In connection with powerful metaphors such as Big Brother from Orwell's novel *1984*, surveillance is often interpreted as the manifestation of an authoritarian process.[2] The representation of surveillance is therefore also partly associated with European experiences such as Stalinist Russia and Nazi Germany. Academic works on totalitarian states highlight the critical role of surveillance measures to identify, classify, spy on and repress the

[1] Giddens, Anthony, "A Contemporary Critique of Historical Materialism", Vol.1: *Power, property and the state*, University of California Press, Berkeley, 1981, p. 175.
[2] Orwell, George, *1984*, Penguin Modern Classics, London, 2004.

"enemies of the regime".[3] These violently anti-liberal practices were usually based on a military and binary vision of the world reducing the social complexity to a dichotomy between friend and foe.[4] "The Nazi regime in Germany from the 1930s to 1945 offers one egregious example of state surveillance and classification in order to privilege 'Aryans' and to eliminate minorities such as 'Jews' and 'Gypsies'".[5] With regards to Mussolini's and Franco's fascist regimes and the Soviet Bloc, numerous authors describe how legal and extra-legal bodies enforced monitoring systems to target specific groups as well as to "prevent the spread of contagious ideas"[6] and to contain or eradicate any form of dissent.[7] Hence, surveillance can be framed as a central element of the historical manifestation of various forms of dictatorships. Nevertheless, echoing the famous depiction of surveillance as a Janus-face (i.e. protective and repressive),[8] scholars remind us that surveillance practices also play a key role regarding democratic processes.[9]

In a second understanding of surveillance, this is seen as an indispensable tenet of modern governance. "Surveillance has to do with the activity of governing".[10] According to this understanding, surveillance takes us away from the totalitarian and refers to the tools that any government needs to manage its own population, which entails both to care for and control. "These tools, such as the census, geographical survey, public health records, welfare rolls, voting register, national identity cards, passports, visas, etc., provide a statistical foundation of population management".[11] While these tools can facilitate authoritarian processes, they also support the implementation of rights and obligations that are related to the ideals of democracy.[12] Vital democratic practices such as open elections are based on electoral rolls as well as identification and registration systems to ensure equal rights of participation and to

[3] Los, Maria, "Looking into the Future: Globalization and the Totalitarian Potential", in David Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Willan, Cullompton UK, 2006, pp. 69-94. Los, Maria, "A Trans-systemic Surveillance: the Legacy of Communist Surveillance in the Digital Age", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, New York, 2010, pp. 173-194.

[4] Jarausch, Konrad, "Au-delà des condamnations morales et des fausses explications. Plaidoyer pour une histoire différenciée de la RDA", *Genèses*, Vol. 3, No. 52, Septembre 2003, pp. 80-95.

[5] Lyon, David, *Surveillance Studies*: An Overview, Polity Press, Cambridge, 2007, p. 32. Black, Edwin, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, Crown Publishing, New York, 2001.

[6] Los, Maria, "A Trans-systemic Surveillance: the Legacy of Communist Surveillance in the Digital Age", supra note 3, pp. 173-194.

[7] Dunnage, Jonathan, "Social control in Fascist Italy: the Role of the Police", in Clive Emsley, Eric Johnson and Pieter Spierenburg (eds.), *Social Control in Europe*. 1800-2000, Vol. 2, Ohio State University Press, Ohio State University, 2004, pp. 261-280. Dunnage, Jonathan, "Policing Right-Wing Dictatorships: Some preliminary comparisons of Fascist Italy, Nazi Germany and Franco's Spain", *Crime, History & Societies*, Vol. 10, No. 1, January 2006, pp. 2-28. Dunnage, Jonathan, "Surveillance and Denunciation in Fascist Siena, 1927-1943", *European History Quarterly*, No. 38, April 2008, pp. 244-265. Fonio, Chiara, "Surveillance under Mussolini's regime", *Surveillance & Society*, Vol. 9, No. 1/2, May 2011, pp. 80-92. Koehler, John O., *Stasi: The Untold Story of the East German Secret Police*, Westview Press, Boulder CO, 1999. Lindenberger, Thomas, "Secret et public: société et polices dans l'historiographie de la RDA", *Genèses*, Vol. 3, No. 52, Septembre 2003, pp. 33-57. Poppe, Ulrike, "Que lisons-nous lorsque nous lisons un dossier personnel de la Stasi", *Genèses*, Vol. 3, No. 52, September 2003, pp. 119-132.

[8] Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, Polity Press, Cambridge, 1994.

[9] See contributions to Haggerty, Kevin, and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, New York, 2010.

[10] Bellanova, Rocco, and Michael Friedewald (eds.), Deliverable 1.1: "Smart Surveillance – State of the Art", *SAPIENT project*, Brussels, 2012, p. 20.

[11] Salter, Mark B., "Surveillance", in J. Peter Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, p. 193.

[12] Brown, Felicity, "Rethinking the Role of Surveillance Studies in the Critical Political Economy of Communication", IAMCR Prize in Memory of Dallas W. Smythe, 2006, p. 1-32.

prevent voter frauds.[13] Moreover, citizens' protection and social welfare expectations are partly provided via various administrative forms of monitoring from health surveys to surveillance of tax regimes. Surveillance and policing practices are also required to mitigate illegalities that can challenge democratic principles.[14] Thus, the relationship between surveillance and democracy is nuanced and complex to the extent that the former can inhibit as well as contribute to the existence of the latter.[15]

This second understanding of surveillance explains why some make a strong connection between surveillance and the formation of the modern, bureaucratic state.[16] Modalities of identification, classification, record-keeping and monitoring are all key features of bureaucracies. Although bureaucracy and surveillance as routine practices of administration have been presented as modern means to ensure democracy, the accumulation of data and files have also drawn attention to possible misuses of considerable amounts of information.[17] Many academic and political debates are currently focused on the electronic processing of data (i.e. "dataveillance") and the growth of surveillance programmes that are technologically mediated.[18] There seems to be no difference with the surveillance practices implemented in former Eastern European states after World War II. However, it is worth remembering that "some of the most repressive and anti-democratic forms of state surveillance – such as was conducted by East Germany's notorious secret police, the Stasi – did not rely on cutting-edge technologies, but instead drew upon extensive networks of informers; common citizens who were either enticed or coerced into informing on others".[19]

Thanks to access to the archives of the Ministry for State Security, commonly known as the Stasi, and the development of a socio-historical perspective on surveillance, the case of East-Germany is regularly cited to emphasise how surveillance can operate in undemocratic contexts. The widespread networks of "unofficial collaborators" (*Inoffiziele Mitarbeiter*) were key components of the surveillance apparatus implemented by the East German State.[20] These collaborators reported information on relevant events, on informal conversations in public places, at work, and so on. Thus, they participated in the informative structure that aimed to keep up-to-date files on ordinary citizens. This system "saw 1/6th of the population employed

[13] Lyon, David, "Identification, Surveillance and Democracy", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, New York, 2010, pp. 34-50.

[14] Haggerty, Kevin, and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, New York, 2010.

[15] Bigo, Didier, "Security, Surveillance and Democracy", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *The International Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 277-284.

[16] Dandeker, Christopher, *Surveillance, Power and Modernity*, Polity Press, Cambridge, 1990. Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007. Salter, Mark B., "Surveillance", in J. Peter Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, pp. 187-196.

[17] Weber, Max, *Economie et Société*, Paris, Agora, 2003. Weber, Max, "Parlement et gouvernement dans l'Allemagne réorganisée", in Max Weber, *Oeuvres politiques*, Paris, Albin Michel, 2004, pp. 307-455.

[18] Amicelle, Anthony, "The Great (Data) Bank Robbery: The Terrorist Finance Tracking Program & the SWIFT Affair", *Research Questions*, CERI, No. 36, May 2011, pp. 1-27. Amoore, Louise, and Marieke De Goede, "Introduction. Data and the war by other means", *Journal of Cultural Economy*, Vol. 5, No. 1, February 2012, pp. 3-8. Clarke, Roger, *Introduction to Dataveillance and information privacy, and definition of terms*, 2006, http://www.rogerclarke.com/DV/Intro.html (last accessed 31 October 2012). Gutwirth, Serge, and Mireille Hildebrandt (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer science, Brussels, 2008.

[19] Haggerty, Kevin, and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, New York, 2010, p. 5. See also Schmeidel, John C., *Stasi*, Routledge, London, 2008.

[20] Dennis, Mike, and Peter Brown, *Stasi: Myth and Reality*, Pearson Education, Longman, Harlow, 2003. Miller, Barbara, *Narratives of Guilt and Compliance in Unified Germany: Stasi Informers and Their Impact on Society*, Routledge, London, 2000.

as informers in some capacity".[21] A wide web of anonymous informers was also a central element of the "dossier society" fostered by Mussolini's fascist regime to monitor "suspects", both inside and outside Italy.[22] Furthermore, denunciatory practices represent a common feature of surveillance exercised in European authoritarian regimes such as Fascist Italy, Vichy France, Nazi Germany and Stalinist Russia although forms of denunciations were slightly different. Mass organisations (youth groups, organisations for women and so on) were also a way both to obtain obedience and to implement informal surveillance.[23] With regards to East Germany, wire-tapping, face-to-face surveillance and correspondence control (i.e. interception and reading of letters and postal cards) were intensively used by the Stasi agents.[24] This enterprise of organised observation of behaviour and social control consisted of spying on political opponents, preparing so-called measures of "psychological destruction" and even trying to provide an overview of the opinions within the population.[25] While some authors question the Stasi's ability to really grasp social dynamics and to influence socio-political process[26], anti-democratic forms of surveillance devices such as in East Germany had tremendous consequences on citizens' personal lives.[27]

2.2.1 Fundamental rights and civil liberties under the Communist regime in Hungary

After the Second World War, the countries of Central and Eastern Europe became members of the Soviet Bloc and followed the Communist legal and political regime, until political changes in 1989. Hungary (at the time of the People's Republic of Hungary) was one of these countries. A common characteristic of Communist regimes, at least as viewed from the West, is that both the legal guarantees and the practical enforceability of civil and political rights are restricted or made practically impossible. It would be an oversimplified view to assume that until the fundamental changes of the political system these rights were restricted uniformly in all Communist countries, and after the political changes, every civil and political right became guaranteed and enforced. There were significant differences among the national Communist regimes and among the various historical periods of these regimes, too. In Hungary, in the years following the end of the Second World War these rights could be enforced relatively freely, then after the establishment of the one-party system a period of severe restrictions followed. Partly as a reaction to this situation the 1956 revolution broke out, after the suppression of which retaliation and restriction of rights were reintroduced. These years were followed by an era of *détente*, which can be characterised by its attempts to reach compromises in the domain of internal affairs.[28]

In this period relative improvements could be experienced in the treatment of those holding liberal opinions or fighting for civil and political rights in the Western sense, too. "He who is

[21] Wood, David, "Editorial. People Watching People", *Surveillance & Society*, Vol. 2, No. 4, April 2005, p. 474.
[22] Fonio, Chiara, "Surveillance under Mussolini's regime", *Surveillance & Society*, Vol. 9, No. 1/2, May 2011, pp. 80-92. Franzinelli, Mimmo, *I tentacoli dell'Ovra*, Bollati e Boringhieri, Torino, 1999.
[23] *Ibid*.
[24] Poppe, Ulrike, "Que lisons-nous lorsque nous lisons un dossier personnel de la Stasi", *Genèses*, Vol. 3, No. 52, Septembre 2003, pp. 119-132.
[25] Jarausch, Konrad, "Au-delà des condamnations morales et des fausses explications. Plaidoyer pour une histoire différenciée de la RDA", *Genèses*, Vol. 3, No. 52, Septembre 2003, pp. 80-95.
[26] Lindenberger, Thomas, "Secret et public: société et polices dans l'historiographie de la RDA", *Genèses*, Vol. 3, No. 52, Septembre 2003, pp. 33-57.
[27] Funder, Anna, *Stasiland*, Granta, London, 2004.
[28] This period was called by the Western media the Kadar Era, named after Janos Kadar, the leader of the Communist party who ruled the country for over three decades, or later as "goulash communism", referring to the relative wealth provided within the framework of the political system.

not against us is with us" declared Kadar in 1960, indicating that those who did not question the fundamental framework of the regime might enjoy a thriving economic and cultural life. The system gradually lifted the earlier draconian measures against free speech and movement, and also eased some restrictions on cultural activities. The system of "three T's" had been introduced, named after the Hungarian equivalents of "banned", "tolerated" and "supported" activities. The tolerated category had been gradually extending (although there were significant political and ideological fluctuations during the 1970s and 1980s), and consequently the sanctions imposed on members of the democratic opposition or those violating the written or unwritten rules of the regime had also been changed.

In general, in this post-War era laws virtually guaranteed a wide range of civil and political rights, without however, allowing citizens to enjoy these rights. This was partly due to the fact that the laws could be interpreted or "specified" in ministerial decrees and other norms, which also prescribed the detailed rules of enforcement (in Hungary, between two parliamentary sessions the Parliament was substituted by a Presidential Council which was authorised to enact statutory rules), and partly due to the formal and informal obligation of those enjoying these rights to follow the ideology of the one-party system.

Certain rights, however, could not be enjoyed even within these limits. In particular, after the introduction of the one-party system the right to establish parties and other political organisations was denied. It was also practically impossible to establish and operate civic organisations with any kind of political relevance, up until 1989. Qualifying of certain activities relating to the practical realisation of legally guaranteed rights was often arbitrary. This was notably the case of the right of assembly, which was always subordinated to the Communist ideology.

From the aspect of the influence exerted by the (non-Soviet) international community on Communist countries in the area of fundamental rights and freedoms, the signing of the Helsinki Accords in 1975 proved to have outstanding significance in the long run. The document, which was signed by almost all European states, the USA and Canada, was originally aimed at reducing the Cold War tensions and strengthening the inviolability of national frontiers – at the same time consolidating the Soviet Union's territorial gains in Eastern Europe following the Second World War – and developing cooperation in the fields of trade, industry, science and technology; however, it also included requirements for promoting fundamental rights and freedoms. Although the Communist countries did not intend to follow the latter requirements in practice, it turned out during the following decades that the Helsinki Final Act, which was first seen in the Communist countries as the diplomatic triumph of the Soviet Bloc, became a sort of manifesto and official reference for dissidents and liberal movements in these countries. The Soviet Union even felt the obligation to publish a volume under the name of Konstantin Chernenko, later to be leader of the country for a short period, on "Human Rights in Soviet Society", for which he received the Lenin Prize in 1982.

Independent non-governmental organisations were formed for monitoring compliance with the Helsinki Accords, such as the Moscow Helsinki Group in 1976, the pioneering work of which had inspired the formation of similar groups in other countries of the Soviet Bloc: Charter 77 in Czechoslovakia or the Polish Helsinki Watch Group in 1979. These non-governmental organisations initiated the establishment of the International Helsinki

Federation in 1982.[29] In Hungary an informal forum of opposition intellectuals, the "Flying University" – a discussion forum meeting in changing private locations – was formed in 1978, and the Committee to Help the Poor (SZETA), an illegal organisation formed by members of the democratic opposition was established in 1979. The most widely circulated illegal (Samizdat) periodical, *Beszélő,* in which editors and writers published their work under their real names, was first published in 1981.[30]

The most important (illegal) rights protecting organisations in this period was the Independent Legal Watch Agency. Its Founding Statement in 1988 identified activities in three areas: legal proceedings based on acts of legislation that violate human rights; legal proceedings based on acts which citizens are powerless to challenge in court; and decisions that discriminate against individuals or groups of individuals on the basis of their beliefs, social status or ethnicity.[31] Another important organisation was the Hungarian Helsinki Committee[32] formed in 1989, amidst the turbulent events of political changes. Founded in the new, democratic period of the country's history, the organization had and still has a lot to do in the areas of monitoring the respect for human rights protected by international human rights instruments, to inform the public about human rights violations, and to provide victims of human rights abuse with free legal assistance.

In this period in Hungary there were no harsh retaliations against the civilian population. Equally there was no state of emergency being declared unlike in Poland, so members of the democratic opposition who openly used their real names in the underground press did not face the direct risk of imprisonment. Instead, the government made continuous efforts to vex, distress and intimidate them. Naturally, these individuals and organisations were subject to regular – open and secret – surveillance, the basic attributes of which are summarised by Szekely as follows:

- "The basic informational regime was the exact reverse of expectations in the constitutional democracies. Whereas the Western political ideal was based on the autonomous, self-determining citizen and on the transparent, accountable state, the Communist ideal was based on self-determining party-state leadership and on the transparent, accountable citizen. [...]
- The overriding ideology was intolerant of any form of deviation, with the authorities and party organizations making a point not only of hoarding sensitive data pertaining to dissident behaviour and sentiment but also of publicizing them by way of "instruction" or retribution.
- When the early visions of the cybernetic state and the wired society first emerged, they did not spring from the efficiency principle, as they had in Western democracies, but arose in direct response to the need for a highly centralized administration and surveillance system. [...]
- By keeping the "internal enemies" of the system under surveillance, the secret services and their civilian collaborators perpetuated a situation in which no one could be sure just how much the next person knew about him or her. This constant sense of doubt

[29] The archives of the International Helsinki Federation (the organisation was liquidated in 2008) is in the custody of the Open Society Archives at Central European University (OSA Archivum), see the Open Society Archives, http://osaarchivum.org/db/fa/318.htm (last accessed 31 October 2012).
[30] *Beszélő* is still being published today as a political and cultural journal of liberal intellectuals.
[31] Mink, Andras, *The Defendant: the State. The Story of the Hungarian Helsinki Committee,* Hungarian Helsinki Committee, Budapest, 2005.
[32] The Hungarian Helsinki Committee, http://helsinki.hu/en/ (last accessed 31 October 2012).

and distrust massively disfigured human relationships on both the personal and the social levels."[33]

It is interesting to note that in this environment of fear and surveillance, civil rights protection regulation emerged relatively early in advance of changes to the system. The Statistical Act of 1973 prescribed that "individual data relating to private persons, his family or other circumstances shall only be used for statistical purposes".[34] A new provision of the Civil Code, which became effective in 1977, declared that "personal rights shall be respected by everyone. These rights shall be protected by law".[35] [...]"Computerized data processing shall not violate personal rights."[36] In 1981 the president of the John von Neumann Computer Society initiated the preparation of a "Law on Informatics" aiming at "modernizing the relationship between state and citizens", defining what kind of data may be requested from citizens and may be stored about them, thereby following the practice of democratic capitalist countries, and resulting in a favourable impact on international and home affairs.[37]

As we will see in Section 4.3, such provisions did not emerge in the framework of constitutional law, but were built in the system of civil law, where many of these provisions can still be found. However, the reasons for enacting such provisions were not only conscious intentions to democratise the political and legal system, but rather influences from Western political and professional forums in which Hungarian officials participated. Ironically enough, some of the initiatives were based on misunderstandings. For example, data protection was generally understood as data security (in the interest of the data controllers) therefore its legal regulation was supported by government branches. Even after the political changes and the enacting of the new combined data protection and freedom of information law, numerous "experts" were using the terms "data protection" and "data security" as synonyms, listed one after the other, to be on the safe side. There was a similar misunderstanding around the notion of freedom of information. In the Hungarian language the phrases "freedom of information" and "regulation of information" sounds very similar, and the new concepts could be "sold" by its supporters to the government under the latter name, which was much easier.[38]

In 1982 the Central Statistical Office (KSH) undertook the coordinating role of legislation in the area of information security.[39] On the official track, KSH proposed the preparation of an "Information Act" to the Council of Ministers in 1984,[40] and even in 1988 the title of the act the codification of which was proposed by the Minister of State, was about "handling of personal data and registration (!) of data of public interest".[41]

---

[33] Szekely, Ivan, "Changing attitudes in a changing society? Information privacy in Hungary 1989–2006", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan (eds.), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons,* McGill-Queen's University Press, Montreal & Kingston, London, Ithaca 2010.

[34] Act No. V of 1973 on Statistics, Section 15.

[35] Act IV of 1959 on the Civil Code, Section 75, para (1).

[36] Act IV of 1959 on the Civil Code, Section 83, para (1).

[37] Letter from the president of the John von Neumann Computer Society to the president of the Central Statistical Office, 29 December, 1981 (available in the archives of the Central Statistical Office, Budapest).

[38] For example, the official body coordinating the legislation was named as "Working Party on Regulation of Information".

[39] Letter of 14 January 1982 from the president of KSH to a competent leader of the Central Committee of the Hangarian Socialist Workers' Party (available in the archives of KSH).

[40] Letter of 22 May 1984 from the president of KSH to the president of the Council of Ministers (available in the archives of KSH).

[41] Annex to the verbal presentation of Imre Pozsgay, Minister of State, November 1988.

In the background, however, under the wings of KSH a multidisciplinary panel of experts began to gather and to analyse the available Western laws and practical experience in the area of information rights.[42] Their activity led to the drafting of the concept of the new data protection and freedom of information law, the principles of which had been accepted officially in 1989 (although still as a classified document).[43] The work of this multidisciplinary group resulted in the coherent conceptualisation of informational rights, which constituted the fundamentals of the informational-legal regime which is effective even today. In Section 4.3 we will examine the evolution of the Hungarian legislative system towards regulating state surveillance powers in the last thirty years.

2.3 FUNDAMENTAL RIGHTS AND CIVIL LIBERTIES IN CONTEMPORARY SURVEILLANCE SOCIETIES

It would be simplistic and inappropriate to say that surveillance is against democracy and fundamental rights. As the case law of the ECtHR shows,[44] surveillance may infringe human rights and it is very challenging to assess whether and to what extent surveillance technologies affect or infringe human rights. Violations due to the use and deployment of surveillance technologies may involve not only informational rights but also other fundamental rights, such as the freedom of expression. Surveillance may also have "chilling effects" on civil and political rights are they are worthy of note and consideration in the interest of keeping the democratic legal order and thus preventing the abuse of state powers.

This Section will elaborate on the relationship between surveillance and democracy, recalling some of the findings of IRISS D.1 (notably Task 1.5 on the impacts of surveillance on civil liberties and fundamental rights). It will present the main issues at stake in the relationship between surveillance and democracy focusing on some of the contemporary surveillance practices. In particular, the case of surveillance in urban areas and surveillance as a tool for detecting and preventing crime and terrorism will be dealt with.

2.3.1 How surveillance affects legal and democratic values

Surveillance may represent a threat to several human rights such as privacy, data protection, freedom of expression, freedom of association, freedom of movement,[45] due process and non-discrimination.[46] These freedoms aim to protect individual self-expression in the public sphere. Furthermore, they refer to the public value of privacy. In a liberal democratic society, human beings are free by definition to enjoy their rights and freedoms autonomously. In a surveillance society, the extensive monitoring of individuals does not necessarily imply a lack of freedom, and in principle individuals are still free to make their own choices without being

[42] Szekely, Ivan, "Central and Eastern Europe: Starting from Scratch", in Ann Florini (ed.), *The Right to Know. Transparency for an Open World*, Columbia University Press, 2007.
[43] Resolution 3022/1989 of the Council of Ministers, declassified in June 2005.
[44] This is discussed in Chapter 3 of this Deliverable.
[45] Council of Europe, European Commission for Democracy through Law (Venice Commission), *Opinion on Video Surveillance in Public Spaces by Public Authorities and the Protection of Human Rights*, 70th Plenary Session, 16-17 March 2007.
[46] Gellert, Raphaël, Katja de Vries, Paul De Hert, and Serge Gutwirth, "A Comparative Analysis of Anti-Discrimination and Data Protection Legislations", in Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky, *Discrimination and privacy in the information society. Data mining and profiling in large databases*, Springer, Heidelberg, 2012, pp. 61-89.

subject to state constraints.[47] However, the fact of being monitored may inhibit the individual's behaviour and thus affect the exercise of democratic rights. As Goold underlines, widespread forms of public surveillance risk undermining the public authorities' commitment to democratic government and to the protection of individual rights.[48] Democracy is safeguarded, as long as citizens are granted a space free of governmental oversight in order to engage in social and political action. As a consequence, the risk of surveillance being anti-democratic is actual.[49]

2.3.2 Surveillance technologies in urban areas

In most urban areas, CCTV is the most prominent and common surveillance technology, and has been so since the beginning of the relationship between cities and surveillance. Olean, in New York, is one of the first cities mentioned in the literature as deploying cameras to combat crime in 1968. In 1973, cameras were installed in Times Square, even if the system was quietly dismantled two years later because of little impact on the security of the area.[50] In the following years, the idea that cameras were cheaper than increasing the police force, together with the willingness to look for urban design solutions to social problems meant that CCTV continued to proliferate on both sides of the Atlantic, especially in public transport, social housing and schools.[51] By 1975, the London Underground had a CCTV system in one of its lines to fight against robberies and attacks on personnel, and that same year 145 cameras to control traffic were installed in the streets of the UK capital. In general, however, at that time the deployment of video surveillance by the police to monitor public order and public space was limited and tended to concentrate on hooliganism and political events.[52]

The proliferation of such technologies in urban areas has implications for the ways in which public space is perceived and used, as well as on the social interactions that occur. Generally speaking, the European legal framework for CCTV emphasises that while technical means substantially increase the protection of goods and freedoms, these must be regulated in order to introduce the necessary guarantees so that the exercise of constitutional rights and freedoms is fully protected.[53] This means that all public surveillance devices must go through an *a priori* process of authorisation and that all citizens have a right to access, modify and cancel the data that is kept on them. Spain has one of the strictest and more rights-based legal frameworks for surveillance in Europe, which explains why in 2003 a request to install a

[47] Jacobs, Bart, "Keeping our surveillance society non-totalitarian", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, p. 27.
[48] Goold, Benjamin J., "Technologies of surveillance and the erosion of institutional trust", in Franko Aas, Katja, Helene Oppen Gundhus, Heidi Mork Lomell (eds.), *Technologies of Insecurity. The Surveillance of Everyday Life*, Routledge-Cavendish, New York, 2009, pp. 208-218, p. 211.
[49] Haggerty, Kevin D. and Minas Samatas, "Surveillance and democracy: an unsettled relationship" and Monahan, Torin, "Surveillance as Governance. Social Inequalities and the Pursuit of Democratic Surveillance", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and democracy*, Routledge-Cavendish, New York, 2010, pp. 1-16, and 91-110 respectively. K. Haggerty and M. Samatas argue that surveillance is anti-democratic "to the extent that it prevents individuals from coming together to identify common interests, forge alliances and develop political strategies".
[50] Yesil, Bilge, "Watching ourselves: Video surveillance, urban space, and self responsibilization", *Cultural Studies*, 2006, p. 403.
[51] *Ibid*.
[52] McCahill, Michael and Clive Norris. *CCTV in Britain*, Urbaneye Working Paper no. 3, Berlin, Centre for technology and Society, Technical University of Berlin, 2002.
[53] This is the case of the Spanish Organic Law 4/1997, that regulates the use of video cameras in public spaces by the Spanish Police Forces.

camera in a well-known route for demonstrations in Barcelona was only accepted on the provision that it would be turned off whenever political events take place so as to not infringe upon people's right to assembly by creating a digital record of those participating.[54] While it is difficult to know whether or not this measure is actually implemented, the ruling acknowledges that surveillance does have an impact on the exercise of civil and political rights, and tries to find a compromise between these and the need to increase public safety.

Although a strict legal framework does not necessarily prevent the spread of CCTV and surveillance technologies in general, legal provisions can respond to some of people's concerns over surveillance. There are a myriad of externalities that affect civil and political rights that have so far not been properly addressed by the law, such as discrimination, exclusion, social sorting, profiling, privacy, ethics, empowerment and accountability. The sociological nature and political character of public space is altered when visualisation introduces new power relationships (the 'surveilled' over those doing the surveillance, those who can and cannot see). In their study of the night-time economy in Lancaster (UK), Dixon et al.[55] for instance, point to the possibility that video surveillance discourages feelings of social responsibility and that 'responsibility for the welfare of others is handed over to the CCTV cameras'. Also, other studies suggest that surveillance systems are often installed in places where young people meet, emphasising how the electronic eye is often directed at groups that are perceived to be problematic, thus contributing to reinforce discrimination and stigmatisation and making those groups subject to a double victimisation that affects their social position and limits their exercise of their civil rights.[56,57]

Cameras are not the only surveillance technology being deployed in urban areas. Smart cards, ANPR, RFID systems, biometrics, sensors and databases are increasingly permeating the urban experience and having a significant impact upon civil and political rights, but also on the way cities are run, and people relate to each other.[58] The fact that "smart cities" are still used more for public relations reasons than in response to real needs does not mean that these surveillance technologies should not be taken seriously by those trying to understand how surveillance impacts on civil and political rights in Europe. The generalisation of these and other devices, such as mobile phones that collect location data, means that the urban experience is increasingly becoming a surveillance experience, and that "dataveillance" practices are increasingly permeating public space, urban relations and urban policy. As addressed in Chapter 3 of this Deliverable, surveillance practices affect people's privacy (which includes notions of autonomy, dignity, liberty, personality, and self-determination), and fundamental freedoms such as freedom of association, assembly, expression and movement. As mentioned above, surveillance can sometimes weaken social responsibility and social bonds, which are key to the democratic and inclusive character of the public sphere.

---

[54] Galdon Clavell, G. "Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia", *Information Polity*, 16(4), 2011, pp. 319-338.

[55] Dixon, John, Mark Levine and Rob McAuley, *Street Drinking Legislation, CCTV and public space: exploring attitudes towards public order measures*, Home Office Report, London, 2003, p. 21.

[56] Galdon Clavell, Gemma, "Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia", *Information Polity*, Vol. 16, Issue 4, 2011, pp. 319-338.

[57] Norris, Clive and Gary Armstrong, *The maximum surveillance society: The rise of CCTV*, Berg, Oxford (England), 1999.

[58] Murakami Wood, D., Kirstie Ball, Lyon David, Clive Norris and Charles Raab, 'A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network', 2006. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdfhttp://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (last accessed 15 October 2012).

Surveillance can also affect some people's relationships to others and to the state, in the sense of introducing a "culture of suspicion" which affects mutual trust, social inclusion and the right to the presumption of innocence. This context of fear and distrust is what has sometimes been described as the "chilling effect" of the surveillance society, which can seriously affect people's exercising of their rights.

Another significant externality related to the proliferation of surveillance in urban areas is the effect of control on the freedom of movement. If everyone is traced through mobile devices, CCTV cameras, ANPR, smart cards, etc., the possibility to "escape" is increasingly limited. This can affect criminals and wrongdoers in general, but also those in irregular administrative situations (illegal aliens), those that are routinely perceived as "not belonging" and put under special scrutiny (young people, poor people, women with specific clothing) or those that become a "false positive". With the generalisation of surveillance, the whole city becomes a "checkpoint".[59]

Finally, as many authors have highlighted, surveillance is often at times discriminatory. Contemporary surveillance is based on the collection, storage, processing and retrieving of electronic personal information to manage and to influence populations' activities through social categorisation.[60] This classifying drive of surveillance constitutes what David Lyon calls "social sorting".[61] When such categories are implemented in public space, this results in increased police attention towards certain groups, "police profiling", which has an immense impact on the effective enjoyment of the rights derived from citizenship by those that are labelled as "criminal", "outsider" or "improper" by the category which they happen to fall in.

2.3.3 Surveillance systems for deterring and preventing crime and terrorism

For many reasons democratic states turn to surveillance devices for crime control purposes. The foregoing section illustrates this. It is not the object of this Chapter to identify the motives of states, nor the solidity of the policy arguments in favour of using surveillance, but it is clear that expectations about efficiency, technological availability *and* political opportunism, explain this turn to surveillance in crime control.[62] The events of 9/11 added a

[59] Graham, S. *Cities under siege*. London, Verso, 2010.
[60] Surveillance Studies Network, *A report on the surveillance society*, Office of the Information Commissioner, Wilmslow, 2006.
[61] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2008.
[62] The uneven trajectory of the development of the varied surveillance systems which are utilised today to deter and prevent crime and terrorism has been propelled by innovation, opportunity and coincidence. The now widespread practice of electronic monitoring of offenders, for instance, is largely credited to New Mexico's Judge Jack Love finding inspiration in a Spiderman comic (Nellis, Mike, "Out of this World: The Advent of the Satellite Tracking of Offenders in England and Wales", *The Howard Journal*, Vol. 44, Issue 2, 2005, pp. 125 – 150), while the UK's status as having more CCTV cameras per person than anywhere in the world (Norris, Clive and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999) is to some extent a reflection of a political desire by particular governments to be seen to be active in 'fighting crime' rather than driven by evidence-based research regarding cameras' deterrent effects (Webster, William, "CCTV policy in the UK: reconsidering the evidence base", *Surveillance & Society*, Vol. 6, Issue 1, 2009, p. 11). The rhetoric constructed around CCTV by the then UK Home Secretary Michael Howard in 1995 gives an impression of the forceful sentiment used to justify the expansion of UK city CCTV schemes: "CCTV catches criminals. It spots crimes, identifies lawbreakers and helps convict the guilty. The spread of this technology means that more town centres, shopping precincts, business centres and car parks around the country will become no-go areas for the criminal… CCTV is a wonderful technology supplement to the police". McCahill, Michael and Clive Norris, "On the Threshold to Urban Panopticon? Analysing the Employmeny of CCTV in European Cities and Assessing its Social and Political Impacts", *Working Paper No. 3 CCTV in Britain*, RTD-Project (September

national security dimension and ushered in a range of counter-terrorism surveillance measures and what Zedner and others have termed 'pre-crime' strategies, which would broaden their reach even further.[63] The lack of an over-arching normative approach to the development and use of surveillance technologies, along with the emerging technological possibility that previously separate surveillance systems might be linked into a larger, integrated 'assemblage' permitting data mining and data combining, have also resulted in concerns around the power of such a far-reaching web of data collection, raising the possibility of the erosion of civil liberties and potential 'function creep' as the supplementary outcomes of such a diffuse and persistent practice.

Today's 'surveillance societies'[64] could be said to have their origins in state bureaucracies, but in their high-tech form could be said to have developed out of the post-War advances in electronics made in the United States and elsewhere. Surveillance societies are as old as the deployment of surveillance practices for law enforcement purposes. Presidents Johnson and Ford's central database of personal information and the growing prominence of CIA, NSA and FBI use of wiretapping and monitoring served to put surveillance prominently onto the policy agenda and thereafter into the public imagination. However, as Murakami Wood notes, the 'surveillance society' was "a very American story, in which the fears of state actors, the wealthy and their responses, [were] largely in American contexts".[65] Similarly, the introduction and expansion of electronic tagging, as previously mentioned, where a New Mexico Judge built on 'behavioural electronics'[66] work from Harvard University, remained very much an American development until an electronic tag was piloted in the UK in 1989.[67] As Jones[68] notes, electronic tagging then became commonly used as a crime control measure in the UK as a result of various schemes introduced by the Conservative governments of the 1980s and 1990s which were further expanded by the Labour government elected in 1997, despite growing moral and ethical concerns. Throughout these years, the technology used in tagging has progressed considerably, beginning years ago as a simple and limited device with no tracking capability but more recently developing to incorporate sophisticated Global Positioning System (GPS) technology utilising satellite-based tracking systems.[69]

As technological advances continue, innovative new forms of surveillance are likely to emerge. For instance, Monmonier[70] argues that:

> "As more commercial applications for real-time positional data are found, and as more consumer devices become positionally locatable or positionally aware, it will become

---

2001 – February 2004) 5th Framework Programme of the European Commission, Contract No.: HPSE-CT2001-00094, 2002, p. 15.

[63] McCulloch, Jude and Sharon Pickering, "Pre-Crime and Counter-Terrorism: Imagining Future Crime in the 'War on Terror'", *British Journal of Criminology*, Vol. 49, Issue 5, 2009, pp. 628 – 645.

[64] Lyon, David, *Surveillance Society: Monitoring Everyday Life*, Buckingham, Open University Press, 2001.

[65] Murakami Wood, David, "The Surveillance Society: Questions of History, Place and Culture", *European Journal of Criminology*, Vol. 6, Issue 2, 2009, p. 185.

[66] Schwitzgebel, Ralph, "Behavioral Electronics Could Empty the World's Prisons", *The Futurist*, 1970, pp. 59-60.

[67] Lilly, J. Robert and Joan Himan, *The Electronic Monitoring of Offenders: Symposium Papers, Second Series.* De Montfort University Law School Monographs, Leicester, 1993.

[68] Jones, Richard, "Surveillance" in Hale, Chris, Keith Hayward, Azrini Wahidin and Emma Wincup, *Criminology 2nd Edition*, Oxford University Press, Oxford, 2009.

[69] Shute, Stephen, *Satellite Tracking of Offenders: A Study of the Pilots in England and Wales (Research Summary 4)*, Ministry of Justice, London, 2007.

[70] Monmonier, Mark, *Spying with Maps: Surveillance technologies and the future of privacy.* Chicago University Press, Chicago, 2002.

> increasingly possible for surveillance of the locations of individuals, vehicles, and goods to be conducted for commercial or crime control purposes".[71]

Automatic Number [i.e. vehicle license] Plate Recognition (ANPR) systems offer a powerful if actually rather crude way of identifying passing vehicles. Geographic Information System technologies, which perform computerised mapping, can be used along with GPS to "offer a convenient and powerful way of storing, manipulating and visualizing positioning data".[72] As a result, advancing technologies have ensured that the potential spread of the 'surveillance society' has grown beyond being heavily monitored by CCTV, beyond a crime control measure and into our personal use of the Internet and wireless devices.

In recent years, a political or policy justification that has often been used to justify further expansion of forms of surveillance has been the prevention of terrorism (colloquially, and more rhetorically still, the domestic 'war on terror'). Zedner suggests we may be witnessing a shift towards 'a pre-crime society', "in which the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done".[73] McCulloch and Pickering[74] also argue that post-9/11 measures have moved the focus away from criminal justice to national security, which broadens the scope of such measures significantly. Surveillance has played a prominent role in this shifting jurisdiction, which has further fuelled concerns over a growing 'surveillance society'. Lyon notes that the legislation passed by the USA and other countries post-9/11, including the controversial 'Patriot Act' allowed greater freedom for wiretapping, including extending the legality of email interception and Internet clickstream monitoring.[75] The UK also attempted to enhance its anti-terrorism procedures with an unpopular and largely protested national identity card scheme, which would be linked to a database called the 'National Identity Register'. The Identity Cards Act 2006 was, however, immediately repealed by the new Conservative and Liberal Democrat coalition government of 2010.[76] Many other highly personal surveillance measures have been implemented as part of airport security, such as iris-scans[77], full-body scanners, and schemes such as Canada's 'Advanced Passenger Information/ Passenger Name Record Program' (API/PNR), which "requires commercial carriers to provide Citizen and Immigration Canada (CIC) with passenger and crew information for analysis, so that any who appear to pose concerns may be identified and intercepted".[78]

At the same time, the recent rise of surveillance measures cannot be explained by reference to 9/11 alone. As Garland points out, a long-term shift towards a 'culture of control' had been

---

[71] Jones, Richard, "Surveillance" in Hale, Chris, Keith Hayward, Azrini Wahidin and Emma Wincup, *Criminology 2nd Edition*, Oxford University Press, Oxford, 2009, p. 538.
[72] *Ibid*.
[73] Zedner, Lucia, "Pre-Crime and Post-Criminology?", *Theoretical Criminology*, Vol. 11. 2007, p. 261.
[74] McCulloch, Jude and Sharon Pickering, "Pre-Crime and Counter-Terrorism: Imagining Future Crime in the 'War on Terror'", *British Journal of Criminology*, Vol. 49, Issue 5, 2009, pp. 628 – 645.
[75] Lyon, David, *Terrorism and Surveillance: Security, Freedom and Justice after September 11 2001*, Paper given at the Privacy Lecture Series <http://privacy.openflows.org> on November 12, 2001, available at http://privacy.openflows.org/pdf/lyon_paper.pdf (last accessed 31 October 2012).
[76] The Guardian, *ID card scheme to be scrapped within 100 days*, 27 May 2010, http://www.guardian.co.uk/politics/2010/may/27/theresa-may-scrapping-id-cards (last accessed 31 October 2012).
[77] Lyon, David, *Terrorism and Surveillance: Security, Freedom and Justice after September 11 2001*, Paper given at the Privacy Lecture Series <http://privacy.openflows.org> on November 12, 2001, available at http://privacy.openflows.org/pdf/lyon_paper.pdf (last accessed 31 October 2012).
[78] Lyon, David, "Airport screening, surveillance and social sorting: Canadian responses to 9/11 in context", *Canadian Journal of Criminology and Criminal Justice*, Vol. 48, Issue 3, p. 404.

underway for some decades prior.[79] With such undeniably fast-paced and broad-ranging surveillance expansion in response to unforeseen terrorist and criminal acts, many commentators have warned against the potential for what has been termed 'function creep' (the subsequent re-appropriation of surveillance technologies or the information they generate for means for which they were not originally intended).[80] Gary Marx's 1988 study of data-collection in policing highlighted this insidious sense of function creep, "marked by subtle, invisible, involuntary forms of social control";[81] while Nelken and Andrews also argue that the potential for abuse of data such as of DNA held by government databases for criminal identification programmes, will become of increasing interest to corporate bodies as behavioural genetics become more commonly used for predictive information in the military or in criminal justice.[82] Therefore, the somewhat random and ambiguously-motivated development of today's various surveillance technologies and the gradually eroding moral safeguards surrounding their use in deterring and preventing crime and terrorism may have arguably resulted in a somewhat uncertain future for our civil liberties.

[79] Garland, David, *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford University Press, Oxford, 2001.
[80] Marx, Gary T., *Undercover: Police Surveillance in America.* University of California Press, Berkeley, 1988, p. 2.
[81] Nelken, Dorothy and Lori Andrews, "Surveillance Creep in the Genetic Age", in Lyon, David (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination,* Routledge, London, 2005, p. 95.
[82] *Ibid*.

3. SURVEILLANCE AND THE EUROPEAN PRIVACY AND DATA PROTECTION FRAMEWORK

Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)

3.1 INTRODUCTION

The use of surveillance technologies is most likely to interfere with the right to privacy and the protection of personal data.[83] Although there is a widespread perception that privacy is continuously eroding and fading in our surveillance societies, privacy provides the strongest legal safeguards against the pervasiveness of surveillance powers. As Loader says, "[p]rivacy must and should remain an important part of our conversation when we think about surveillance … because the capacity to control information about your life … seems to me an important part of what it means to have … a sphere of autonomy within which to operate that the state cannot encroach upon".[84]

Legislation and case law on privacy and data protection will come under examination in this Chapter in order to assess how surveillance is regulated. Chapter 3 is composed of six main Sections. Section 3.2 will deal with the right to privacy; Section 3.3 will focus on the right to data protection; Section 3.4 will look at the relationship between privacy, data protection and surveillance; Section 3.5 will investigate the legislative safeguards and formal mechanisms for regulating surveillance referring to the ECHR and the European Data Protection Directive[85]; Section 3.6 will examine the European case law on surveillance. Specific surveillance categories will be identified and analysed, namely: surveillance as listening; surveillance as watching; surveillance as collecting and storing and surveillance as automated processing and profiling.

Of course this Chapter has neither the ambition to present a comprehensive analysis of the theoretical framework of privacy and data protection, nor to provide answers to key questions around privacy and data protection issues. Instead, its purpose is to consider surveillance from a legal perspective on the basis of European legislation and case law.

[83] Vermeulen, Matias, Rocco Bellanova and Serge Gutwirth "A fundamental rights analysis of smart surveillance", *SAPIENT project*, D. 1.1, Chapter 3, p. 85, January 2012.

[84] Loader, Ian, cited by: House of Lords, *Surveillance: Citizens and the State*, Select Committee on the Constitution, 2nd report of Session 2008-09, London, 2009, p. 26.

[85] 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, *Official Journal of the European Communities* L 281, 23 November 1995.

3.2 THE RIGHT TO PRIVACY

Privacy is an ambiguous and contentious concept. It is a value that encompasses several values and principles. Its significance lies in the distinction between the public and the private. Originally considered as the 'right to be let alone',[86] privacy was meant first and foremost to create barriers between public authorities and citizens, thus framing spheres of exclusive dominium and influence. Nevertheless, the modern claim to privacy refers also to the relationship between the individual and other individuals and so the public sphere represents more generally an area in which the individual interacts with society.

The meaning of privacy is rooted in the history, culture and tradition of a community and a country. It varies according to time, space and peoples and is strictly linked to the constitutional origins of a state. Nonetheless, privacy is a subjective value. This denotes that it varies on an individual basis, not only between communities but also within communities. It follows that privacy can be considered as a sensitive value and issue which, in turn, originates "very different sensitivity levels in different contexts".[87] Privacy has different inflections and can be understood in different ways. In Bennett and Raab's words, there are manifold paradigms of privacy[88] and all of them are worthy of attention to realise what privacy is. Referred to as the "limitation of others' access to an individual"[89] or as the "ability to control who has access to us and to information about us",[90] privacy is rather an idea which is often surrounded by an aura of vagueness and contestability. Indeed, *privacy* "is a broad, amorphous concept".[91] The concept of privacy has developed over time to include several aspects and components. It is far broader than the 'right to be let alone', and instead can be taken to refer to "the claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others".[92] The realm of intimacy and wish for solitude that underlies the definition of the 'right to be let alone' is part mainly of the concept of physical privacy. Actually, privacy encompasses several other aspects that are not restricted to this component.[93] Privacy can be referred to six main dimensions, namely: the right to be let alone (1); limited access to the self (2); secrecy (3); control of personal information (4); personhood (5); and intimacy (6) and be distilled into seven different categories.[94] Rössler identifies three different dimensions of privacy, namely:

---

[86] Warren, Samuel and Louis Brandeis, "The Right to Privacy", Harvard Law Review, Vol. 4, No. 5, 15 December 1980.

[87] Bennett, Colin J. and Charles Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, Ashgate, Burlington, 2003, p. 17.

[88] *Ibid*. According to the authors, as a consequence of the ambiguity of the meaning of privacy, legislation and regulations on privacy can address privacy concerns merely from a procedural perspective and they can neither shape nor affect the substantive nature of privacy.

[89] Gavison, Ruth, "Privacy and the Limits of the Law", *Yale Law Journal*, Vol. 89, 1980, pp. 421-471, p. 421.

[90] Rachels, James, "Why privacy is important", *Philosophy and Public Affairs*, Vol. 4, No. 4, 1975, pp. 323-333, pp. 326. Here the author adds that "privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have, and this is why it is important to us".

[91] Moreham, Nicole, "Privacy Rights", in Tugendhat Michael and Christie Iain (eds.), *The Law of Privacy and the Media*, Oxford, Oxford University Press, 2002, pp. 59-88.

[92] Westin, Alan F., *Privacy and Freedom*, New York, Atheneum, 1967.

[93] Rössler, Beate, *The Value of Privacy* (translated by R .D. V. Glasgow), Cambridge, Polity Press, 2005, p. 9.

[94] Zureik, Elia, Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, London, Ithaca, 2010. Finn et al. identify the following seven types of privacy: privacy of the person (1); privacy of behavior and action (2); privacy of communication (3); privacy of data and image (4); privacy of thoughts and feelings (5); privacy of location and space (6); privacy of association (7). Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy" in Serge Gutwirth, Yves Poullet et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013 (forthcoming). See

decisional privacy (right to protection from unwanted interference or heteronomy in our decisions); informational privacy (right to protection against unwanted interference in personal data) and local privacy (right to protection against the admission of other people to spaces or areas). On the basis of this distinction he claims that violations of privacy can consist in an illicit interference in one's actions (1), an illicit surveillance (2) and illicit intrusions in private spaces (3). Informational privacy will be the main dimension at stake in the framework of this Task.

Given the broad meaning of privacy, it is widely recognised that the right to privacy embraces several other rights. Flaherty identified thirteen of them: the right to individual autonomy; the right to be left alone; the right to a private life; the right to control information about oneself; the right to limit accessibility; the right to exclusive control of access to private realms; the right to minimise intrusiveness; the right to expect confidentiality; the right to enjoy solitude; the right to enjoy intimacy; the right to enjoy anonymity; the right to enjoy reserve; the right to secrecy.[95]

The right to privacy is endorsed by Art. 8 ECHR.[96] This article does not mention privacy explicitly. Still, it does not define its meaning and content. From a textual interpretation of the provision of Art. 8.1 ECHR it follows that the definition of privacy here refers only to private and family life, home and correspondence. However, the right to privacy is neither restricted nor limited to these four areas. Instead, as confirmed by a consolidated jurisprudence of the ECtHR, privacy "is a broad term not susceptible to exhaustive definition".[97] Although the ECtHR has never pronounced itself on the exact meaning of the right to privacy, it has partially qualified its content by defining the right to private life. In fact, in *Niemietz v. Germany* the Court, having recognised that it is neither possible nor necessary to "attempt an exhaustive definition of the notion of "private life"", argued that it would be too restrictive to limit its notion "to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings".[98] Thus, the ECtHR recognises that the content of the right to privacy is broad, neither defined nor definable and that its interpretation is dependent upon several variables. Nonetheless it also true that the ECtHR considers the Convention as a living instrument which must be interpreted in the light of existing conditions

---

also Friedewald Michael, Van Lieshout M, Wright David and Gutwirth Serge, "Reconciling privacy and security". *Innovation. The European Journal of Social Science Research*, 2013, pp. 1-14.

[95] Flaherty, David, H., *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada & the United States*, Chapel Hill, The University of North Carolina Press, 1989, p. 8.

[96] Art. 8 ECHR reads as follows:

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.

[97] ECHR, *Peck v. United Kingdom*, application no. 44647/98, judgement of 28 January 2003, para 57; *Niemietz v. Germany*, application no. 13710/88, judgement of 16 December 1992, para 29; *Pretty v. United Kingdom*, application no. 2346/02, judgement of 29 April 2002, para 61; *P.G. and J.H. v. United Kingdom*, application no. 44787/98, judgement of 25 September 2001, para 56.

[98] ECtHR, *Niemietz v. Germany*, supra note 97, para 29.

and European living law.[99] As a consequence, it would make sense to affirm that the ECtHR promotes a 'living interpretation' of the right to privacy.

Two different obligations originate from Art. 8 ECHR. On the one hand, the Convention establishes a negative obligation on member states not to interfere with the rights specified in Art. 8 ECHR, unless the conditions stated in Art. 8.2 are satisfied. On the other, member states have the (positive) obligation to adopt measures to protect the right declared at Art. 8 ECHR in order to avoid interferences by other individuals. The enforcement of this double approach enshrined in Art. 8 ECHR was also confirmed by the ECtHR. As pointed out in *Van Kück v. Germany*, "the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities". Secondly, "in addition to this negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[100] In order to assess violations of Art. 8 ECHR, the ECtHR has been developing and using a three-step analysis which is based on evaluating if there is a legal basis for the supposed infringement of Art. 8 ECHR (1); if the supposed violation of Art. 8 ECHR is meant to attain a legal aim (2); if the violation is necessary or proportionate in a democratic society (3). These criteria will be further analysed below (Section 3.5).

3.3 THE RIGHT TO DATA PROTECTION

Data protection can be defined as a relatively new individual right in European legislation. It has been gradually developed in EU law through public international law instruments, such as the OECD Guidelines of 1980[101] and Convention No. 108.[102] Furthermore, it has been developed in European law under the auspices of member states' legislations and through the jurisprudence of the ECJ and ECtHR.

Despite the fact that personal data is now considered as a human right in European law, it is important to note that data protection has been developed, first and foremost, in member states' legislations since the late 1960s, marking the rise of the information age. The first ever data protection law was adopted by the German state of Hesse in 1970.[103] However, Germany has not been the first European country to pass a national data protection law. Instead, this achievement was made by Sweden in 1973.[104] As Burkert underlines, at that time Sweden was a special case given that it was the most computerised country in the world. In addition, it had a personal identification number system since the late 1940s and used national centralised

[99] ECtHR, *Tyrer v. the United Kingdom*, application no. 5856/75 judgement of 25 April 1978, para 31; *Loizidou v.Turkey*, application no. 15318/89 judgement of 23 March 1995, para 71; *Mamatkulov and Askarov v. Turkey*, application no. 46827/99 and 46951/99, judgement of 4 February 2005, para 121.

[100] ECtHR, *Van Kück v. Germany*, application no. 35968/97, judgement of 12 June 2003, para 70.

[101] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, in OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 9-12, 1980 (1981) *International Legal Materials*, I., 317.

[102] Council of Europe, Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series, No. 108 (1981), *International Legal Materials*, 422.

[103] *Hessisches Datensch*utz, Gesetz, 7 October 1970 – *GVBI (Gesetz und Verordnungsblatt) I*, 1970.

[104] The Swedish Data Protection Act, *Datalag SFS*, 1973. The first German data protection act was issued in 1977, *Bundesdatenschutzgesetz, BDSG*.

registers that urged the need for data security.[105] Although the Swedish data protection system is considered as the basis for the development of the German model, the Hesse Act set important principles and laid the foundation for the growth of a European wide tradition for the protection of personal data.[106] Later on, other European countries started to implement the same models and somehow to conform to the legal traditions inaugurated by Sweden and Germany.[107] The development of data protection rights in Europe and the adoption of European Convention No. 108 in 1981 further encouraged the implementation of data protection norms in Europe, particularly in countries reluctant to regulating privacy and data protection, such as the United Kingdom.[108]

Born within the framework of member states' national legislations, the right to data protection has gradually found its way in European law. However, this process has been uneven and slow. The 1950 ECHR does not contain any provision referring to personal data, nor is this right explicitly protected by the Convention. The European Charter of Fundamental Rights (hereafter 'the EU Charter') has been the first European formal act to endorse the right to the protection of personal data.[109] Following the entry into force of the Lisbon Treaty in 2009, the Charter has acquired a legally binding force in EU law as well as a formal autonomy as a fundamental right. Art. 8 of the Charter recognises unequivocally and officially the right to the protection of personal data.[110] As a consequence, for a long time data protection has been referred to as an uncharted right in European legislation and to a certain extent it is still considered alike.[111] Although it is unquestionable that the right to data protection has been granted a new legal source of legitimacy in European legislation since the entry into force of the Lisbon Treaty, it is important to highlight that until 2009 the main legal basis for the protection of this right was the 1995 European Data Protection Directive[112] which shaped the

[105] Burkert, Herbert, "Privacy – Data protection. A German/European Perspective", in Christoph Engel and Kenneth H. Keller (eds.), *Governance of Global Networks in the Light of Differing Local Values*, Nomos, 2000, pp. 44-69.

[106] These principles were enforced through the following provisions: the negative default rule (1); the legitimisation of the processing of personal data (2); the rights of the data subject (3); the right of access to information (4); the establishing of a privacy protection institution (5); the omnibus approach (6). Indeed, the German approach to data protection was referred to as '"omnibus', given that its rules had a global and comprehensive scope and concerned both the private and public sectors. By contrast, the Swedish approach was more targeted and it contained more specific regulations.

[107] The Swedish tradition was soon followed by other Scandinavian countries. Denmark and Norway adopted their first data protection acts in 1978, Finland in 1988. France passed the first data protection act in 1978 (*Loi no. 78-17* of 6 January 1978 *relative à l'informatique, aux fichiers et aux libertés*), Luxembourg in 1979, the Netherlands in 1988, Portugal in 1991, Belgium and Spain in 1992.

[108] The UK Data Protection Act dates back to 1984. It was then amended by the second data protection act in 1998 which introduced significant changes to the regulation of 1984.

[109] Solemnly proclaimed by the European Parliament on 7 December 2000 during the European Council meeting of Nice, the Charter was then proclaimed a second time on occasion of the approval of the Lisbon Treaty in December 2007.

[110] Art. 8 of the European Charter (Protection of personal data) 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 acccess 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.

[111] González Fuster, Gloria and Raphaël Gellert, "The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right", *International Review of Law, Computers & Technology*, Vol. 26, No. 1, pp. 73-82, 2012.

[112] 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, *Official Journal of the European Communities* L 281, 23 November 1995, 31-50.

legislative framework for data protection together with Directive 97/66.[113] A detailed analysis of the provisions of Directive 95/46/EC would fall outside the scope of this contribution. What is important here is to highlight the goal of the Directive and its main purposes. On the one hand, Directive 95/46 was part of the Community's internal market legislation under Art. 114 TFEU (ex Art. 100A of the Treaty of Rome) and was meant to enhance the creation of a European internal market. Accordingly, the Directive was considered as the legislative tool to allow for a free flow of data within Europe, in order to prevent member states from blocking inter-EU data flows on data protection grounds.[114] On the other hand, the Directive had the aim to achieve a minimum level of data protection throughout Europe, setting harmonised European standards for data protection. Directive 95/46 was built upon six main principles (namely, legitimacy (1); purpose limitation (2); transparency (3); proportionality (4); security (5) and control (6))[115] which will be dealt with in the Sections and Paragraphs that follow. Being considered for a long time as a corollary of the right to privacy, data protection has been gradually acknowledged as an autonomous right by member states' and European legislators. Since 1995 data protection has become part of European law, despite the fact that it was introduced mainly for harmonisation and internal market purposes. It is apparent that Directive 95/46 was neither meant to introduce a new fundamental right in European law, nor to devote personal data an autonomous protection.[116] However, Directive 95/46 raised awareness over the protection of personal data while moving data protection "from an abstract intellectual concern to a contentious political issue".[117]

Although between 1995 and 2009 the protection of personal data was mainly framed around Directive 95/46, it is important to stress that the case law of the ECtHR and the ECJ have greatly contributed to the development of data protection as an autonomous fundamental right. In *Österreichischer Rundfunk* and in *Lindqvist* the ECJ affirmed that the fact that Directive 95/46 is meant to reach internal market purposes "does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that basis".[118] Furthermore, in *Lindqvist* the ECJ underlined that the scope of Directive 95/46 is that to "ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate" and so to maintain a "balance between the free movement of personal data and the

[113] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, *Official Journal of the European Communities* L024, 30 January 1998, 0001-0008. Directive 97/66/EC was replaced by Directive 2002/58 then amended by Directive 2006/24. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic telecommunications sector (Directive on privacy and electronic communications), *Official Journal* L 201/37, 31 July 2002 37-47. Directive 2006/24 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, *Official Journal* L 105 of 13 April 2006, 54-63.

[114] In fact, Art. 1.2 of Directive 95/46 ('Object of the Directive') stresses that "Member states shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1".

[115] Kuner, Christopher, *European Data Protection Law. Corporate Compliance and Regulation*, Oxford University Press, Brussels, 2007, pp. 20-21.

[116] Indeed, Art. 1.1 of Directive 95/46 states that "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

[117] Bennett, Colin J., *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Victoria, British Columbia, 1992, p. 45.

[118] ECJ, C-101/01, *Bodil Lindqvist*, judgement of 6 November 2003, para 40. Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgement of 20 May 2003, para 41.

protection of private life".[119] In 2008 the ECJ took the chance to explicitly refer to personal data as a fundamental right in the *Promusicae v. Telefónica de España* case,[120] while interpreting the preamble of Directive 2002/58.[121] This judgment is worthy of particular note given that in this circumstance the ECJ urged the need to "reconcile the requirements of the protection of different fundamental rights",[122] in European law, namely the right to respect for data protection with the other rights guaranteed by European treaties. A step forward was made by the ECJ in the case *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* of 2009.[123] Making reference to the provisions of Directive 95/46 and in particular to its Art. 6, the Court ruled that the right to privacy implies the right to protection of personal data which, in turn, requires that data are processed in a correct and lawful manner and in particular that personal data are accurate and disclosed to authorised recipients.[124] While in its earlier judgements the Court referred to Directive 94/46 as the main legal instrument for the protection of personal data, it is noteworthy that the ECJ refers also to the Charter of Fundamental Rights of the EU in recent case law. In *Volker und Markus Schecke GBR and Hartmut Eifert v. Land Hessen* the ECJ stated that the right to the protection of personal data is a fundamental right,[125] as recognised by Art. 8 of the Charter and that it is connected to the right to respect of private life expressed in Art. 7 of the Charter.[126] The ECJ recalled Art. 8 of the Charter also in *Deutsche Telekom AG v. Bundesrepublik Deutschland.*[127] Furthermore, it must be highlighted that the ECJ has now a clear preference for a systematic interpretation of the European law on data protection, so reading the provisions of Directive 95/46 in light of the Charter. Indeed, in *Deutsche Telekom AG v. Bundesrepublik Deutschland* the Court said that Directive 95/46 "is designed to ensure, in the Member States, observance of the right to protection of personal data".[128] On the one hand, this statement reflects the consolidated case law of the ECJ on data protection. On the other, it shows the significant efforts made in order to consider data protection as an autonomous fundamental right in

[119] ECJ, C-101/01, *Bodil Lindqvist*, supra note 118, para 96-97.

[120] ECJ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, judgement of 29 January 2008, para 63.

[121] Directive 2002/58/CE of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal* L 201 of 31 July 2002, 37-47. The preamble of Directive 2002/58 recalls Art. 7 and 8 of the European Charter saying at point (2) that the Directive "seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union". In particular, the Directive "seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter".

[122] ECJ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU,* supra note 120, para 65.

[123] ECJ, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, judgement of 7 May 2009.

[124] ECJ, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, supra note 123, par. 49. In addition, at para 70 of the judgement the Court argued that "Article 12(a) of Directive 95/46 requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller".

[125] ECJ, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GBR and Hartmut Eifert v. Land Hessen*, judgement of 9 November 2010, para 30 and ss.

[126] ECJ, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GBR and Hartmut Eifert v. Land Hessen*, supra note 125, para 47.

[127] ECJ, C-262/06, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, judgement of 22 November 2007, para 49 and ss.

[128] ECJ, C-262/06, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, supra note 127, para 50.

European law. It is important to note in this regard that data protection was designed neither as a right, nor as a fundamental right in the framework of Directive 1995/46. Instead, it was originally aimed to protect the "right to privacy with respect to the processing of personal data" (Art. 1.1 of the Directive) and to meet internal market expectations and interests.

While the recent jurisprudence of the ECJ concerning data protection has leaned to somehow eclipse the internal market purposes underlying Directive 95/46, it is also imperative to refer to the developments of the jurisprudence of the ECtHR. From a human rights perspective, the protection of data is conventionally referred to Art. 8 ECHR and, most of all, it is anchored to the interpretations of its provisions given by the Court of Strasbourg. Although data are not expressly protected by Art. 8 ECHR, there is a constant jurisprudence of the ECtHR which associates data protection with the respect for private and family life. In particular, data protection is considered as part of the legislative compound of Art. 8.1 ECHR.[129] In *Z. v. Finland* the ECtHR argued that "the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention"[130] and applied the proportionality test of Art. 8 to assess whether the measures at stake were proportionate to the legitimate aim they pursued. Moreover, the Court did not consider proportionate and necessary in a democratic society the use of documents from medical records used without the consent of the data controller.[131] Recalling the need to respect the confidentiality of health data, in *Biriuk v. Lithuania* the Court said that the disclosure of such data may dramatically affect a person's private and family life (as well as the individual's social situation) "by exposing that person to opprobrium and the risk of ostracism".[132] In *S. and Marper v. the United Kingdom*, the ECtHR, while insisting that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, pointed out that domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of Art. 8 ECHR.[133] Finally, in *Peck v. United Kingdom* the Court recognised that the disclosure of data got from relevant CCTV footage constituted "a serious interference with the applicant's right to respect for his private life".[134] Nonetheless, the trend of the ECJ to consider data protection as an autonomous right can also be found in the case law of the ECtHR.[135] As Boehm confirms, "whereas in the past the ECtHR focused on the private nature of the data at issue by examining whether the content of the data was related to the right to private life, the analysis of the data very closely connected to private life is less common nowadays".[136]

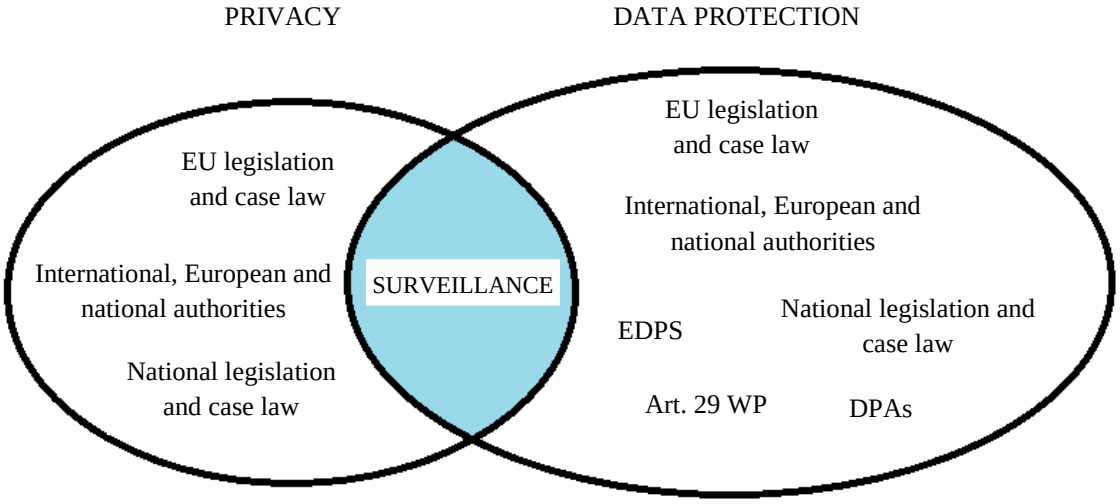
[129] In addition to the cases mentioned above, see also ECtHR, *I. v. Finland*, application n. 20511/03 of 17 July 2008, para 38 and *C.C. v. Spain*, application n. 1425/06, judgement of 6 October 2009, para 31.
[130] ECtHR, *Z. v. Finland*, application no. 22009/93, judgement of 25 February 1997, para 95.
[131] ECtHR, *L.L. v. France*, application n. 7508/02, judgement of 10 October 2006, para 43 and ss.
[132] ECtHR, *Biriuk v. Lithuania*, application n. 23373/03, judgement of 25 November 2008, para 39.
[133] ECtHR, *S. and Marper v. the United Kingdom*, application n. 30562/04 and 30566/04 judgement of 4 December 2008, para 103.
[134] ECtHR, *Peck v. United Kingdom*, application no.44647/98, judgement of 28 January 2003, para 63.
[135] *Reyntjens v. Belgium,* application n. 16810/90, admissibility decision of 9 September 1992; *S. and Marper v. the United Kingdom*, application n. 30562/04 and 30566/04 judgement of 4 December 2008. 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*, Berlin, Springer, 2012, p. 32.
[136] Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice,* supra note 135, Berlin, Springer, 2012, p. 32.

3.4 PRIVACY, DATA PROTECTION AND SURVEILLANCE

As explained at Section 3.2, there is a tight relationship between privacy and data protection. According to the jurisprudence of the ECtHR and ECJ, the protection of personal data serves the purpose of the enforcement of the right to privacy. Thus, the infringement of the individual's right to data protection leads to a violation of the right to privacy. However, a privacy infringement does not necessarily result in a violation of the right to data protection. It follows that although these two fundamental rights are intertwined and tend to overlap, it is imperative to keep them separate and consider them as autonomous human rights. Data protection applies every time personal data are processed and so it is more specific than privacy.

Surveillance can be considered as one of those issues that trigger both privacy and data protection reactions. Of course, it does more and privacy and data protection regulations do not constitute the only tools that regulate and govern it. We already saw that other fundamental rights like the right to non-discrimination and the right to freedom of expression also come into play. Moreover, surveillance is also regulated through other hard-law and soft-law instruments that need to be mentioned here. Apart from European law and case law, surveillance is regulated and enforced at national level. Every national (and European) legal act that makes surveillance possible, in general also contains a list of guarantees and limitations that have to keep the surveillance act within the acceptable boundaries.
Surveillance guarantees are often to be found in surveillance bills that allow for certain surveillance practices.

Turning to the question of agency, one consequently needs to open the horizon. National (and European) authorities, other than judges, (in particular governments, parliaments, judges and national data protection authorities) play a crucial role in governing surveillance. Furthermore, there are many other legal actors that contribute to regulate surveillance (through data protection), such as the European Data Protection Supervisor and the Article 29 Working Party, both issuing legal opinions with great impact. Also noteworthy is the contribution of international organisations (such as the OECD and the UN) and NGOs in this regard.
This complex interplay of privacy and data protection regulations and of actors is represented in the following picture:



3.5 LEGISLATIVE SAFEGUARDS AND FORMAL MECHANISMS FOR REGULATING SURVEILLANCE

After having given an overview of national and European legislation on privacy and data protection and on how surveillance is regulated, this Section will focus on the issue of forms of resilience to surveillance. In particular, it will look for legal forms of resilience in legislation and case law, mainly at European level and in a supranational perspective. A caveat in this regard is necessary. Legislation and case law do not and cannot provide sufficient safeguards to cope with the effects of surveillance. From a legal perspective, privacy can be considered as the main form of resilience to surveillance. However, as explained in this Chapter, privacy is an ambiguous and contentious concept that encompasses several other aspects that relate also to the social and political domains. Thus, a comprehensive analysis on resilience to surveillance must take these aspects into account and have a holistic approach. As a consequence, IRISS Tasks 2.1, 2.2 and 2.3 need to be considered in a systematic way. The following Paragraphs will deal with forms of resilience to surveillance in European law and having regard of Art. 8.2 ECHR and Directive 95/46.

3.5.1 The European Convention on Human Rights

Lawfulness

Art. 8.2 ECHR states a negative obligation for public authorities not to interfere with the right to respect for private and family life, home and correspondence while allowing exceptions for interferences that are "in accordance with the law". As explained at Section 8 of Deliverable 2.2, the rule of law is one of the pillars of democracy and constitutionalism. Furthermore, it is one of the crucial requirements to ascertain the boundaries between surveillance and democracy in the framework of Art. 8 ECHR. The lawfulness criterion represents the first step in the reasoning of the ECtHR to assess whether surveillance measures infringe Art. 8.1 ECHR.

The consistent jurisprudence of the Court prescribes that in order for a surveillance measure to be in accordance with law, it is necessary first of all that the concerned measure has a legal basis in national legislation. As argued in *Malone*, the expression 'in accordance with the law' means firstly that any interference must have some basis in the law of the country concerned.[137] Accordingly, there must be a measure of legal protection in domestic law against the arbitrary power of public authorities in resorting to surveillance. However, the criterion of lawfulness does not prescribe the mere existence of a specific law at national level regulating the exercise of surveillance powers. On the contrary, the core of the lawfulness principle relates to the content of the law, its substantive nature and 'quality'.[138] In order for the surveillance measure to be lawful, the concerned national law has to be particularly clear, precise and detailed. Given that surveillance measures may cause serious interferences with the individual's private life and correspondence, the ECtHR requires national laws to be particularly detailed, in order to prevent possible abuses. In *Malone* and *Silver* the Court pointed out that national laws must indicate the scope of the discretion conferred on the

[137] ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, judgement of 2 August 1984, para 66-67.
[138] In fact, the Court understands the term 'law' in its substantive sense (and not in its formal one). ECtHR, *Malone v. the United Kingdom*, supra note 137, para 67. ECtHR, *Huvig v. France*, application no. 11105/84, judgement of 24 April 1990, para 28. ECtHR, *Kruslin v. France*, application no. 11801/85, judgement of 24 April 1990, para 27 and 30-36. ECtHR, *Khan v. the United Kingdom*, application no. 35394/97, judgement of 12 May 2000, para 26.

competent public authorities and the "manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference".[139] In *Huvig* and *Kruslin* the ECtHR was even more explicit on this point stating that national laws must indicate "with reasonable clarity the scope and manner of exercise of the relevant discretion" of public authorities in exercising surveillance powers.[140] Assessing the violation of Art. 8 ECHR by telephone tapping measures, the ECtHR has been developing specific requirements that national legislation have to ensure in order for a surveillance measure to be lawful. In particular, national laws need to define the following:

- categories of people liable to have their communications monitored;
- nature of the offences which may give rise to an interception order;
- limits on the duration of such monitoring;
- procedure to be followed for examining, using and storing the data obtained;
- precautions to be taken when communicating the data to other parties;
- circumstances in which data obtained may or must be erased or the tapes destroyed.[141]

Thus, the ECtHR requires national legislation to meet specific criteria and to be particularly detailed in regulating surveillance measures such as telephone tapping. These six requirements represent, in turn, legal safeguards established at national level against the indiscriminate use of surveillance measures. However, it is noteworthy that in the Court's view the lawfulness test is not necessarily grounded on these six criteria. On the contrary, it must be carried out on a case-by-case basis. The level of detail prescribed by the lawfulness principle depends on the surveillance measure or technology at stake. The Court distinguishes between cases in which surveillance interferes more with the person's private life (such as wiretapping and surveillance of telecommunications) and cases in which interferences have a lower intensity (such as GPS surveillance). In the first situation, national legislation must guarantee a high level of detail specifying the above-mentioned six criteria. In the latter case, the threshold to be met to comply with the lawfulness principle is lower, as well as the level of detail required by domestic legislation. In *Uzun v. Germany* the ECtHR made clear this distinction arguing that the use of GPS does not constitute either visual or acoustical surveillance and is less susceptible of interfering with Art. 8.1 ECHR through the disclosure of a person's conduct, opinions or feelings.[142] As a consequence, domestic laws on GPS surveillance do not need to meet the six criteria mentioned above and for them it is sufficient to ensure a general "protection against arbitrary interference".[143] As the Court underlined, this more general lawfulness test "depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law".[144]

[139] ECtHR, *Silver and Others v. the United Kingdom*, judgement of 25 March 1983, para 88-89. ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, judgement of 2 August 1984, para 68.
[140] ECtHR, *Huvig v. France*, application no. 11105/84, judgement of 24 April 1990, para 35. ECtHR, *Kruslin v. France*, application no. 11801/85, judgement of 24 April 1990, para 36.
[141] ECtHR, *Huvig v. France*, supra note 140, para 34 and ECtHR, *Kruslin v. France*, supra note 140, para 35. ECtHR, *Uzun v. Germany*, application no. 35623/05, judgement of 2 September 2010, para 65.
[142] ECtHR, *Uzun v. Germany*, supra note 141, para 52.
[143] ECtHR, *Uzun v. Germany*, supra note 141, para 66.
[144] ECtHR, *Uzun v. Germany*, supra note 141, para 63.

Although the lawfulness principle is applied on a case-by-case basis, it prescribes that the lack of any express legal basis at national level for using covert surveillance constitutes a violation of Art. 8 ECHR, as well as the lack of clarity, scope and legitimate aim of that basis.[145]

Accessibility

Art. 8.2 ECHR does not only require the existence of a legal basis at national level to legitimise the exercise of surveillance powers. On the contrary, it implies a positive obligation on public authorities to make the national legal basis accessible. As a consequence, Art. 8.2 "requires firstly that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law".[146] Thus, the condition of accessibility is embedded in the expression 'in accordance with law' and is part of the reasoning of the ECtHR in the context of Art. 8 ECHR.

Foreseeability

Foreseeability is another requirement that contributes to the judgement on the lawfulness of a surveillance measure. The ECtHR has been particularly detailed in explaining the claim that any domestic law that legitimises the exercise of surveillance powers must be foreseeable. In the Court's reasoning, foreseeability implies that the law must be "sufficiently clear in its term 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 to respect for private life and correspondence".[147] However, foreseeability does not mean that individuals should be able to foresee when public authorities are likely to adopt surveillance measures targeting them so that they can adapt their conduct accordingly.[148]

In more practical terms, the accessibility and foreseeability requirements have the final aim to ensure transparency between public authorities and citizens, so preventing the exercise of unfettered and arbitrary powers and the implementation of secret surveillance measures. Thus, they are meant to make individuals aware of the likelihood of them being the target of surveillance measures. Of course, both conditions can be considered as requirements from the point of view of public authorities, whereas they constitute safeguards from the perspective of the citizen.

---

[145] ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, judgement of 2 August 1984. ECtHR, *Khan v. the United Kingdom*, application no. 35394/97, judgement of 12 May 2000. ECtHR, *Halford v. the United Kingdom*, application no. 20605/92, judgement of 25 June 1997. ECtHR, *P.G. and J.H. v. United Kingdom*, application no. 44787/98, judgement of 25 September 2001.

[146] ECtHR, *Huvig v. France*, application no. 11105/84, judgement of 24 April 1990, para 26. ECtHR, *Kruslin v. France*, application no. 11801/85, judgment of 24 April 1990, para 27. ECtHR, *Khan v. the United Kingdom*, application no. 35394/97, judgement of 12 May 2000, para 29. ECtHR, *P.G. and J.H. v. United Kingdom*, application no. 44787/98, judgement of 25 September 2001, para 44. ECtHR, *Perry v. the United Kingom*, application no. 63737/00, judgement of 17 July 2003, para 45. ECtHR, *Liberty and other organisations v. the United Kingdom*, application no. 58234/00, judgement of 1 July 2008, para 59.

[147] ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, judgement of 2 August 1984, para 67.

[148] ECtHR, *Malone v. the United Kingdom*, supra note 147, para 67. ECtHR, *Liberty and other organisations v. the United Kingdom*, application no. 58234/00, judgement of 1 July 2008, para 93. ECtHR, *Weber and Saravia v. Germany*, application no. 54934/00 admissibility decision, para 93 of 29 June 2006.

Necessity

According to Art. 8.2 ECHR, exceptions to the right of private and family life, home and correspondence must be necessary in a democratic society. From a legal point of view, the balance between surveillance and democracy is enshrined in this provision of Art. 8 ECHR which is a synthesis of conflicting interests. Art. 8 does neither provide a definition of 'democratic society', nor specifies what its necessities are. However, exceptions to Art. 8.1 are allowed both to prevent "disorder or crime" and to protect the "rights and freedoms of others", thus ensuring security while safeguarding fundamental rights.

In the 1978 *Klass* case the ECtHR recognised that highly sophisticated forms of espionage and terrorism represented serious threats to democracy and thus justified the resort to "secret surveillance of subversive elements".[149] In addition, the Court admitted that that "the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime".[150] The Court acknowledges that public authorities have a leading and crucial role in defining their necessities in a democratic society and have a certain discretion as regards to the fixing of the conditions for the operation of surveillance systems. Nonetheless, the ECtHR is aware of the threats that can result from secret surveillance and of the dangers of such measures of "undermining or even destroying democracy on the ground of defending it".[151] As a consequence, public authorities cannot enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. Instead, the Court is particularly keen in requiring the contracting states to set up "adequate and effective guarantees against abuse" in resorting to secret surveillance.[152] Furthermore, the margin of appreciation given to national authorities in striking a fair balance between public and private interests is subject to European supervision.[153] In *Peck* the ECtHR argued that the disclosure of relevant CCTV footage can be considered as necessary in a democratic society if the reasons adduced to justify the disclosure are "relevant and sufficient" and the measures are proportionate to the legitimate aims pursued.[154]

Proportionality

Proportionality is part of the necessity requirement test of the ECtHR. The Court has been developing specific criteria to assess whether a surveillance measure can be considered proportionate in a democratic society. As explained in *Klass*, proportionality of the surveillance measure concerned must be assessed taking into account "all circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such

[149] ECtHR, *Klass v. Germany*, application no. 15473/89, judgment of 6 September 1978, para 48.
[150] ECtHR, *Klass v. Germany*, supra note 149, para 48.
[151] ECtHR, *Klass v. Germany*, supra note 149, para 49.
[152] ECtHR, *Klass v. Germany*, supra note 149, para 50. ECtHR, *Malone v. the United Kingdom*, supra note 147, para 81.
[153] ECtHR, *Funke v. France*, application no. 10828/84, judgement of 23 February 1993, para 55. ECtHR, *Peck v. United Kingdom*, application no. 44647/98, judgement of 28 January 2003, para 77.
[154] ECtHR, *Peck v. United Kingdom*, supra note 153, para 76.

measures, and the kind of remedy provided by the national law".[155] In *Leander* the Court underlined that the scope of the state's margin of appreciation is related not only to the nature of the legitimate aim pursued but also to the particular nature of the interference involved.[156] Therefore, the ECtHR recognised that the interest of the state in protecting its national security must also be balanced against the "seriousness of the interference with the applicant's right to respect for his private life".[157] This finding was further confirmed in the *Peck* case in which the Court said that the margin of appreciation enjoyed by national authorities in the exercise of surveillance powers depends on the nature and seriousness of the interests at stake and the gravity of the interference.[158]

Thus, the ECtHR has provided useful guidelines for explaining the broad meaning of the proportionality requirement which underlies Art. 8.1 ECHR and so for balancing the conflicting interests that are enshrined therein. However, it is necessary to refer to the practical enforcement of the proportionality principle in the ECtHR case law to see how it operates on the ground. In *Peck* the Court found that the disclosure of CCTV footage related to an attempted suicide was not proportionate given that the objective of crime prevention could have been achieved through more proportionate means and options. In particular, this aim could have been attained identifying the applicant beforehand and obtaining his consent prior to the disclosure of film footage. Furthermore, images could have been masked in order to safeguard the applicant's right to respect for his private life or measures could have been taken to ensure that media, to which the disclosure was made, masked those images.[159]

From a more empirical perspective, the core of the proportionality requirement consists in balancing conflicting rights and interests, whose task is typically performed by judges. The ECtHR stressed this point in the *Marper* case. The Court highlighted that the protection of Art. 8 ECHR would be "unacceptably weakened" if the use of modern surveillance 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".[160] The ECtHR found that the "*blanket and indiscriminate*" retention of fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences "failed to strike a fair balance between competing public and private interests" and thus the retention at issue constituted a disproportionate interference with Art. 8 ECHR.[161]
In the Court's view, the proportionality requirement has to be ensured also by domestic law that regulate the use of surveillance. As a consequence, the six requirements prescribed by the lawfulness principle (see Section 3.5) must comply with the proportionality criterion.[162]

[155] ECtHR, *Klass v. Germany*, supra note 149, para 50. See also ECtHR, *Malone v. the United Kingdom*, supra note 147, para 66-68 and *Liberty and other organisations v. the United Kingdom*, application no. 58234/00, judgement of 1 July 2008, para 93-94.
[156] ECtHR, *Leander v. Sweden*, application No. 9248/81, judgement of 26 March 1987, para 59.
[157] ECtHR, *Leander v. Sweden*, supra note 156, para 59.
[158] ECtHR, *Peck v. United Kingdom*, supra note 153, para 77.
[159] ECtHR, *Peck v. United Kingdom*, supra note 153, para 80.
[160] ECtHR, *S. and Marper v. the United Kingdom*, application n. 30562/04 and 30566/04 judgement of 4 December 2008, para 112.
[161] ECtHR, *S. and Marper v. the United Kingdom*, supra note 160, para 125.
[162] 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*, Berlin, Springer, 2012, p. 50.

3.5.2 The European data protection directive

Forms of legal resilience against the unfretted surveillance powers of state authorities result also from European legislation on data protection and particularly from Directive 95/46.[163] These safeguards are based on the Council of Europe Convention for the Protection of individuals with regard to Automatic Processing of Personal Data[164] and are laid down in the European Charter of Fundamental Rights.[165] Art. 8 of the Charter states that "everyone has the right to the protection of personal data concerning him or her" and that 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 established 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. Nonetheless, the Charter requires independent authorities to verify compliance of these rules.

Art. 6 of Directive 95/46 states that personal data must be processed fairly and lawfully (1); should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (2); should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (3); accurate, up to date (4) and; kept for no longer than is necessary for the purposes for which they were collected or further processed (5). Art. 7 sets specific conditions under which personal data may be processed and says that this circumstance occurs only if the data subject has given his consent or if the processing is necessary for the performance of a contract to which the data subject is party.[166] Member States have to prohibit the processing of 'special categories of data', notably personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.[167] However, this prohibition does not apply if the data subject has given his explicit consent to the processing of these data or the processing relates to data which are

---

[163] 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, *Official Journal of the European Communities* L 281, 23 November 1995.

[164] According to Art. 5 of the Convention that personal data shall be:

a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

[165] Council of Europe, Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series, No. 108 (1981), *International Legal Materials*, 422.

[166] Art. 7 of Directive 95/46/EC requires member states to process personal data only if:

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

[167] Art. 8.1 of Directive 95/46/EC.

"manifestly made public by the data subject".[168] Finally, Directive 95/46 requires that information should be provided in case of collection of data from the data subject[169] and guarantees the right to access to data and to object.[170]

The case law of the ECJ on the interpretation of Art. 6 and 7 of the Directive seems to be strongly influenced by the jurisprudence of the ECtHR on Art. 8 ECHR. In *Eugen Schmidberger, Internationale Transporte und Planzüge and Republik Österreich*, the ECJ ruled that unlike the absolute fundamental rights enshrined in the ECHR (such as the right to life or the prohibition of torture and inhuman or degrading treatment or punishment, which admit of no restriction), there are other rights that are not absolute in the framework of the Convention (such as the freedom of expression and the freedom of assembly) and that need to be viewed in relation to their social purpose.[171] More specifically, in *Volker and Markus Schecke GBR und Hartmut Eifert v. Land Hessen* the ECJ admitted that the right to data protection is not an absolute right. Instead, it must be considered in relation to its function in society[172] and thus balanced against other eventual conflicting interests and rights. Nonetheless, like the ECtHR, the ECJ recognises that member states have a certain margin of appreciation in balancing public and private interests.[173]

Consent

Consent is one of the main pillars of the European data protection legislation and can be considered as one of the most important legal safeguards against data protection violations and the unlawful exercise of surveillance powers. It guarantees transparency and enables the data subject to become aware of its own position and adapt its behaviour to a given situation. Personal data are released only if consent is given accepting specific terms of agreement or conditions. The practice of giving one's consent is a reality, well developed in our everyday life. However, despite this matter of fact, there is not a coherent legal framework at European level for regulating consent. Indeed, consent is not a human right, nor does it have a clear legal status.

Similarly, the legal value of consent is crucial in regulating surveillance and represents one of the most contentious issues. From a legal perspective, the mere fact of agreeing with a surveillance practice does not necessarily justify that surveillance practice. In order to be valid, consent should be explicit, full and free.[174] However, when considering CCTV for example, we notice that consent is not explicit but implicit (when entering public places it is assumed that consent is given implicitly given that in such circumstance surveillance is unavoidable). In addition, it is hard to admit that consent is truly free when being subject to surveillance is the price to pay to have access to goods and services.[175]

[168] Art. 8.2 (e) of Directive 95/46/EC.
[169] Art. 10 of Directive 95/46/EC.
[170] Art. 12 of Directive 95/46/EC.
[171] ECJ, C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge and Republik Österreich*, judgement of 12 June 2003, para 79-80.
[172] ECJ, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GBR and Hartmut Eifert v. Land Hessen*, judgement of 9 November 2010, para 48.
[173] ECJ, *Keegan v. Ireland*, C-16969/90, judgement of 26 May 1994. ECJ, *B. v. France*, C-13343/87, judgement of 25 March 1992, para 44. ECJ, *Mikulic v. Croatia*, C-53176/99, judgement of 7 Febrary 2002, para 57. ECJ, *Van Kück v. Germany*, judgement of 12 June 2003, para 71.
[174] Alexander, Larry, "The Moral Magic of Consent", *Legal Theory*, Vol. II, 1996, pp. 165-174.
[175] Gras, Marianne L., "The legal regulation of CCTV in Europe", *Surveillance & Society*, Vol. 2, No. 3, 2004, pp. 216-229.

The ambiguous legal nature of the principle of consent explains why it is often associated with other principles, such as dignity and proportionality.

3.6 SURVEILLANCE AND THE EUROPEAN CASE LAW

The European legal framework on surveillance (and on the implantation of surveillance measures) is based on privacy and data protection, whose protection is ensured firstly by Art. 8 ECHR. There is a substantial case of law of the ECtHR on surveillance. Conventionally, it can be ascribed to three different categories, namely: unwanted listening to individuals (1); unwanted watching of individuals (2), and unwanted publishing of personal information (3).[176] The aim of this Section is to provide an overview of relevant ECtHR jurisprudence on surveillance and to get a general picture of how surveillance is regulated at European level, making reference to the first two categories of cases.

3.6.1 Surveillance as listening

The ECtHR case law on violation of Art. 8 ECHR due to secret listening is rich and has been growing increasingly since the 1970s. There are manifold surveillance measures that can give rise to an 'interference' with the right to respect for private and family life, home and correspondence. The Court has recognised that a breach of Art. 8.1 may occur in case of interception of mail, post and telecommunications (*Klass v. Germany*);[177] interception of telephone calls (*Kopp v. Switzerland*);[178] release of records of metering to the police (*Malone v. the United Kingdom* and *P.G. and J.H. v. the United Kingdom*);[179] tapping and interception of telephone conversations (*Huvig v. France, Valenzuela Contreras v. Spain, Khan v. the United Kingdom, Armstrong v. the United Kingdom, Chalkley v. the United Kingdom* and *Hewitson v. the United Kingdom*).[180] Furthermore, a breach of Art. 8.1 can originate from the interception or monitoring of paper messages (*Taylor-Sabori v. United Kingdom*)[181] and Internet usage (*Copland v. the United Kingdom*)[182].

However, an interference with Art. 8 ECHR can result not only from the implementation of a surveillance measure by state authorities but also from the existence of a national law which contravenes Art. 8.1 ECHR. This circumstance occurred in the case *Klass v. Germany* of

[176] 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*, supra note 162, p. 33.
[177] ECtHR, *Klass v. Germany*, application no. 5029/71, judgement of 6 September 1978, para 41.
[178] ECtHR, *Kopp v. Switzerland*, application no. 23224/94, judgement of 25 March 1998, para 53.
[179] ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, judgement of 2 August 1984, para 64. ECtHR, *P.G. and J.H. v. the United Kingdom*, application no. 44787/98, judgement of 25 September 2001, para 39 and 42.
[180] ECtHR, *Huvig v. France*, application no. 11105/84, judgement of 24 April 1990, para 32. ECtHR, *Valenzuela Contreras v. Spain*, application no. 27671/95, judgement of 30 July 1998, para 46. ECtHR, *Khan v. the United Kingdom*, application no. 35394/97, judgement of 12 May 2000, para 25-28. ECtHR, *Armstrong v. the United Kingdom*, application no. 48521/99, judgement of 16 July 2002, para 19. ECtHR, *Chalkley v. the United Kingdom*, application no. 63831/00, judgement of 12 June 2003, para 24. *Hewitson v. the United Kingdom*, application no. 50015/99, judgement of 27 May 2003, para 20.
[181] ECtHR, *Taylor-Sabori v. the United Kingdom*, application no. 47114/99, judgement of 22 October 2002, para 19.
[182] ECtHR, *Copland v. the United Kingdom*, application no. 62617/00, judgement of 3 April 2007, para 42.

1978.[183] In the aftermath of the terrorist threats of 1970s, Germany introduced national laws[184] restricting the right to secrecy of mail, post and telecommunications, so authorising in certain circumstances secret surveillance without the need to inform the person concerned. Though the applicants had not been subject to state secret surveillance, the ECtHR said that they were anyway entitled to claim a violation of Art. 8 ECHR on the basis of the fact that the contested legislation resulted in the potential interference with their right to respect for private and family life and correspondence.[185] Thus, the ECtHR recognised that secret telephone surveillance and recording is against Art. 8 ECHR and that the mere existence of secret surveillance legislation created the danger of surveillance. Then, the Court went on to analyse whether or not the interference was justified under Art. 8.2 ECHR. This stance was reiterated by the ECtHR in its more recent judgement *Liberty and other organisations v. the United Kingdom.*[186] Here the Court confirmed that "the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied" which, in turn, constitutes an interference with Art. 8 ECHR.[187] In order to contend that a violation of Art. 8 ECHR has occurred, the Court must assess that the surveillance measure at stake does not fall within the exceptions mentioned at Art. 8.2 ECHR. Nonetheless, there is also a burden of proof on the applicants to demonstrate at least a "reasonable likelihood" that the surveillance measure adopted was meant to produce effects on themselves.[188]

3.6.2 Surveillance as watching

As explained in IRISS Deliverables 2.1 and 2.2, secret or unwanted watching represents a threat to privacy and data protection which is exacerbated by the increasing use of surveillance systems such as CCTV. The widespread deployment of surveillance technologies is reflected in the case law of the ECtHR. The relevant jurisprudence of Court of Strasbourg has been aimed particularly to set specific criteria and conditions to assess whether the surveillant gaze in private or public places leads to an infringement of Art. 8 ECHR.

Although the protection granted by Art. 8 ECHR recalls primarily a private dimension, it is necessary to underline that the ECtHR does not consider the term 'private life' as limited to the intimate sphere of the individual. Instead, the Court recognises the existence of a sort of private dimension of the individual in the public sphere which needs to be safeguarded under the terms of Art. 8 ECHR. This interpretation results from the case law of the Court, as explained above at Section 3.2 of this Deliverable. Moreover, in *P.G. and J.H. v. the United Kingdom*, the Court noted that the private dimension of the individual in the public sphere corresponds to the "zone of interaction of a person with others".[189] In this judgement the ECtHR admitted explicitly that people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner and that in such a circumstance a "person's reasonable expectations as to privacy" may be called into

[183] ECtHR, *Klass v. Germany*, supra note 177.
[184] In particular, in 1968 Germany passed an amendment to Article 10§2 of the Basic Law and Act of 13August 1968. In addition to the exception to the freedom of communications, the new legislation excluded legal remedy before national courts for contesting the surveillance measures concerned.
[185] ECtHR, *Klass v. Germany*, supra note 177, para 33-38.
[186] ECtHR, *Liberty and other organisations v. the United Kingdom*, application no. 58234/00, judgement of 1 July 2008.
[187] ECtHR, *Liberty and other organisations v. the United Kingdom*, supra note 186, para 56.
[188] ECtHR, *Halford v. the United Kingdom*, application no. 20605/92, judgement of 25 June 1997, para 48.
[189] ECtHR, *P.G. and J.H. v. the United Kingdom*, supra note 179, para 56.

question.[190] Still, the Court compared surveillance which a person who "walks down the street" could be subject and monitoring by technological means through CCTV realising that these two situations have the same character.[191] Accordingly, the Court admits that files gathered by security services on a particular individual fall within the scope of Art. 8 ECHR no matter if the information is gathered by an intrusive or covert method.[192] As for the legal implications of these surveillance practices, the ECtHR stated that "private-life considerations may arise, however, once a systematic or permanent record comes into existence of such material from the public domain".[193] A clearer definition of the idea of the private dimension of individuals in public places was given in *Peck v. the United Kingdom*.[194] Here the Court found that the disclosure of CCTV footage to the media of the applicant's suicide attempt for further broadcast and publication purposes amounted to an interference with Art. 8.1 ECHR. The ECtHR stipulated that such a wide disclosure "exceeded any exposure to a passer-by or to security observation and to a degree surpassing that which the applicant could possibly have foreseen".[195]

Nonetheless, it is important to highlight that the ECtHR perceives a clear distinction in the use of different surveillance systems and tools. In *Perry v. the United Kingdom*,[196] the Court distinguished between the monitoring of actions of an individual in a public place by the use of photographic equipment (which does not record the visual data) and the recording of data and the systematic or permanent nature of the record. The ECtHR claims that only the latter may give rise to a violation of Art. 8 ECHR.[197] The Court does not consider that the mere and normal use of CCTV *per se* (whether in public streets or on premises) challenge Art. 8.1 ECHR. On the contrary, these surveillance systems serve "a legitimate and foreseeable purpose".[198] Thus, the systematic and permanent recoding of data through CCTV does not violate Art. 8 ECHR, on condition that the surveillance measures at stake are in accordance with law and necessary in a democratic society.

3.6.3 Surveillance as collecting and storing

According to a consolidated jurisprudence of the ECtHR the mere storing of information relating to an individual's private life by a public authority amounts to interference within the meaning of Art. 8 ECHR. In addition, the subsequent use of the stored information has no bearing on that finding.[199] In the more recent *Copland* case the ECtHR pointed out that the collection and storage of personal information relating to the applicant's telephone (especially the numbers dialled), as well as email and Internet usage constitute an interference with Art. 8.1 ECHR if handled without the consent of the person concerned.[200] The fact that personal

[190] ECtHR, *P.G. and J.H. v. the United Kingdom*, supra note 179, para 57.
[191] ECtHR, *P.G. and J.H. v. the United Kingdom*, supra note 179, para 57.
[192] ECtHR, *Rotaru v. Romania*, application no. 28341/95, judgement of 4 May 2000 and ECtHR, *P.G. and J.H. v. the United Kingdom*, supra note 179, para 57.
[193] ECtHR, *P.G. and J.H. v. the United Kingdom*, supra note 179, para 57.
[194] ECtHR, *Peck v. the United Kingdom*, application no. 44647/98, judgement of 28 January 2003.
[195] ECtHR, *Peck v. the United Kingdom*, supra note 194, para 62.
[196] ECtHR, *Perry v. the United Kingom*, application no. 63737/00, judgement of 17 July 2003, para 38.
[197] ECtHR, *Perry v. the United Kingom*, supra note 196, para 38.
[198] ECtHR, *Perry v. the United Kingom*, supra note 196, para 40.
[199] ECtHR, *Leander v. Sweden*, application No. 9248/81, judgement of 26 March 1987, para 48, ECtHR, *Kopp v. Switzerland*, application No. 23224/94, judgement of 25 March 1998, para 53, ECtHR, *Amann v. Switzerland*, application No. 27798/95, judgement of 16 February 2000, para 69.
[200] ECtHR, *Copland v. the United Kingdom*, application No. 62617/00, judgement of 3 April 2007, para 44.

information may be gathered without the use of intrusive or secret means is not sufficient to exclude the applicability of Art. 8 and thus violations may occur also in these situations.[201]

As the ECtHR underlined in *Marper* both the retention of cellular samples and DNA profiles on one hand and the retention of fingerprints in connection with an identified or identifiable person on the other, constitute an interference with Art. 8.1 ECHR.[202] In particular, the Court stressed that the collection and retention of fingerprints may raise private life concerns considering that they contain unique information about individuals and allow identification. As the Court pointed out, the retention of fingerprints cannot be considered as "neutral or insignificant".[203]

3.6.4 Surveillance as automated processing and profiling

While modern surveillance practices and techniques are very effective in fighting crime, they can be particularly intrusive because of the way personal data are treated and processed. This risk was clearly assessed by the ECtHR in the *Marper* case. The applicants claimed a violation of Art. 8 ECHR on the grounds that British authorities retained their DNA and fingerprint data taken during a previous investigation despite the acquittal of one of them and the discontinuance of the criminal proceedings against the other. In this case the Court found that the blanket and indiscriminate retention of fingerprints, cellular samples and DNA profiles constituted a disproportionate interference with the applicants' rights to respect for private life and could not be considered as necessary in a democratic society.[204] Most of all, it is noteworthy that the Court recognised that DNA profiles contain sensitive data and that their automated processing allows public authorities to get 'sensitive information' such as ethnic origin.[205] Further, it stated that the possibility the DNA profiles create for interferences to be drawn "makes their retention all the more sensitive and susceptible of affecting the right to private life".[206] Thus, in this circumstance the Court met the claim of the UK civil society organisation Liberty which asked the UK government to delete the DNA samples and fingerprints of two individuals who were arrested but never convicted of a crime. The Court stressed in this regard that state authorities have the responsibility for striking a right balance between private-life interests and law enforcement purposes when profiling.[207] Nonetheless, this balance must be reflected in national legislation. The risks linked to automated data processing were highlighted also in the *Friedl* case in which the ECHR Commission assessed that the retention of anonymous photographs (taken at a public demonstration) did not violate Art. 8 ECHR because they had not been entered in a data-processing system.[208]

Art. 15 of Directive 95/46 grants the right to every person "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating

[201] ECtHR, *P.G. and J.H. v. United Kingdom*, application no. 44787/98, judgement of 25 September 2001, para 57.
[202] ECtHR, *S. and Marper v. the United Kingdom*, application n. 30562/04 and 30566/04 judgement of 4 December 2008, para 77 and 85.
[203] ECtHR, *S. and Marper v. the United Kingdom*, supra note 202, para 84-85.
[204] ECtHR, *S. and Marper v. the United Kingdom*, supra note 202, para 125.
[205] ECtHR, *S. and Marper v. the United Kingdom*, supra note 202, para 75-76.
[206] ECtHR, *S. and Marper v. the United Kingdom*, supra note 202, para 76.
[207] ECtHR, *S. and Marper v. the United Kingdom*, supra note 202, para 112.
[208] ECHR, *Friedl v. Austria*, application No. 15225/89, judgement of 31 January 1995, para 49-51.

to him, such as his performance at work, creditworthiness, reliability, conduct, etc.".[209] However, as explained in IRISS D.2.1 (Chapter 1, Section 1.6), this provision, which is intended to prohibit automated profiling, is weak and ambiguous and the data protection reform does only partially address the legal concerns originated by Art. 15 of the Directive.

[209] Art. 15 of Directive 95/46, supra note 114.

4. REGULATING SURVEILLANCE: COMPARATIVE ANALYSIS OF EUROPEAN NATIONAL EXPERIENCES

Paul De Hert and Antonella Galetta, Vrije Universiteit Brussel (VUB)
Gertjan Boulet, Vrije Universiteit Brussel (VUB)
Ivan Szekely and Beatrix Vissy, Eotvos Karoly Policy Institute (EKINT)
Charles Raab and Richard Jones, University of Edinburgh (UEdin)
Anthony Amicelle and Marit Moe-Price, Peace Research Institute Oslo (PRIO)
Gemma Galdon Clavell University of Barcelona (UB)

4.1 INTRODUCTION

National authorities play a crucial role in regulating and governing surveillance. As a consequence, national legislation and case law contribute to define the legal framework that applies to surveillance.

Chapter 4 consists of four main Sections. Section 4.2 provides a general overview of the different privacy and data protection regimes that exist in Europe and emphasises their main features. Section 4.3 compares different national experiences and legal traditions in regulating privacy and data protection with regards to surveillance, presenting the national cases of Belgium, Hungary, Spain, and Norway. Finally, Section 4.4 focuses on European Member States' national case law and presents some relevant decisions of national courts in cases relating to surveillance. In particular, cases concerning data retention, online surveillance and wiretapping are reported.

4.2 PRIVACY AND DATA PROTECTION: TRADITIONS, PRINCIPLES AND VALUES

Contemporary legal systems both within and beyond the European legal space form a rich tapestry of various legal traditions and cultures. These traditional and cultural contrasts have historically resulted in stark differences in the attributes of modern privacy and data protection regimes. Although there is a significant degree of consensus among contemporary democracies about recognising privacy as a democratic right that shall be granted to individuals by way of qualified protection, the different legal traditions and cultures have elaborated clearly differing approaches in terms of actual formulation and implementation of privacy and data protection laws.

While there is no overall agreement on the way and scope of protecting privacy, not even under the umbrella of the EU, the recent technological developments as well as the globalised social and political processes have sparked a significant increase in transborder data flow, and thereby escalated the conflicts between diverging privacy regimes.[210] From a human rights perspective, handling the tension between the increasing need for global attitudes towards increasingly globalised surveillance[211] and the existing traditional and cultural diversity on the international stage is one of the greatest challenges Europe faces in the twenty-first century's

[210] Salbu, Steven R., "The European Union Data Privacy Directive and International Relations", *35 Vand. J. Transnat'l L.* (2002), p. 688. See also Blume, Peter, "Transborder data flow: Is there a solution in sight?" *8 Int'l J,L & Info Tech (2000),* pp. 65-86.

[211] For theoretical considerations of qualifying surveillance as a global phenomenon see Lyon, David, *Surveillance Studies, An overview*, Polity Press, 2007. pp. 119-136. Mattelart, Armand, *The Globalization of Surveillance*, Polity Press, 2007.

surveillance era. Recognising and understanding the core differences of legal traditions and cultures may not only facilitate the harmonic political coexistence of sovereign powers in multiple international dimensions,[212] but do also contribute to the deliberations on the potential and limits of harmonising legal attitudes to surveillance concerns at the European or even global level. Such considerations may ultimately also crystallise into a clear position on whether the idea of a common European legal privacy culture is a fallacy or not.

4.2.1 'Legal tradition', 'legal culture', 'legal system'

Tradition means, in the words of Goldman, "to have a history and a framework for the future".[213] In terms of law, the term 'tradition' has gained an autonomous meaning in the legal literature that has inspired several scholars to develop detailed and sophisticated theoretical concepts of what is supposed to be meant by this idea.[214] Without entering these far-reaching considerations, 'legal tradition' is allowed to be defined, although simplified, as a set of deep-seated, historically-conditioned attitudes about the role and nature of law in society and polity, about the proper organisation and operation of a legal system, and about the way law is or should be made, applied, perfected, and taught.[215] Legal tradition, legal culture, and legal system are, in theory, three relatively separable but empirically closely intertwined notions that are supposed to describe three different superimposed dimensions, or rather superimposed levels of law.[216] Accordingly, a legal system corresponds to the surface level of law comprised of a set of operating legal rules, institutions, and mechanisms related to a sovereign nation or community of nations;[217] 'below' the surface i.e. behind the rules and their application there is a particular legal culture which is reflected in the matrix of specific legal concepts, principles, values, moral convictions etc.; and, finally, most deeply, there is the legal tradition manifested in the main structure and idea of law, as explained above. These relatively distinguishable levels of law are in a closely tied, interdependent relationship,[218] meaning that legal rules are normally embedded in and determined by their legal culture which is also organically linked to the legal tradition in which it was born. What makes the harmonisation of different national legal standards quite difficult is that although the surface

[212] As Steven Salbu remarked, in the era of global surveillance, sovereign powers can be expected to press their own legal doctrines and philosophies in the global marketplace of laws and customs, which can lead to international strife. He argues that approaches being consistent with cultural identity are highly valued but aggressive approaches that neglect the existence of cultural diversity are threatening and may increase the potential for international discord. Salbu, (2002), *ibid*., pp. 688-689.

[213] Goldman, David B., *Globalisation and the Western Legal Tradition, Recurring Patterns of Law and Authority*, Cambridge University Press, 2008, p. 6.

[214] There is a remarkable literature on what is supposed to be meant by the notion of legal tradition (legal culture). See for instance: Glenn, H. Patrick, "A Concept of Legal Tradition", *Queen's L. J.*, Vol. 34, 2008-2009, pp. 427-445; Glenn, H. Patrick, *Legal Tradition of the Worlds: Sustainable Diversity in Law*, Oxford, 2007, Goldman (2008) *ibid*.

[215] Marryman, John and Perez Perdomo Rogelio: *The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America*, Stanford University Press, 2007, p. 2.

[216] The three-level concept put down here is developed from the concept of Kaarlo Tuori Finnish legal philosopher. See Tuori, Karlo, "EC Law: An Independent Legal Order or a Post-Modern Jack-in-the-Box?", in Eriksson, Lars D. et al. (eds.), *Dialectic of Law and Reality: Readings in Finnish Legal Theory*, University of Helsinki, 1999, p. 403. See also Lopez-Rodriguez, Ana M., "Towards a European Civil Code Without a Common European Legal Culture? The Link Between Law, Language and Culture", *Brook J. Int'l L*, Vol. 29, 2003-2004, p. 1206.

[217] Marryman, John and Perez Perdomo Rogelio: *The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America*, supra note 215, p. 1.

[218] Lopez-Rodriguez, Ana M., "Towards a European Civil Code Without a Common European Legal Culture? The Link Between Law, Language and Culture", supra note 216, p. 1206.

level of law is quite dynamic (lawmakers should be able to meet mainly the socio-political and economical demands and adjust the rules to them accordingly), the traditional and cultural settings, which determine the substantive, applicable law, are more static and rigid, and as key identity-determining factors, particularly resistant to external forces.

4.2.2 Core differences among privacy regimes

As suggested above, the legal protection of privacy may and actually does take significantly divergent forms among legal systems, and this fact is largely attributed to differences in historical and cultural conditions which are quite difficult to change. Although there are considerable differences in the legal environment of privacy protection among each legal regime, the most profound concerns over the differing national attitudes and the chance of harmonisation are primarily related to the gap between the common law and the various (Western and Post-Communist) civil law privacy regimes. It is often argued, basically with regard to the situation of the UK that in contrast to the continental-style regimes, the UK privacy law is underdeveloped and national authorities fail to show willingness to provide adequate safeguards for individual privacy in today's digital surveillance era.[219]

It is broadly admitted that the common law system consists of a cohesive set of structural and procedural components that prevent the UK from following the civil law pattern of developing the right to privacy and data protection. Although the ECHR was incorporated into the UK domestic law in 1998, the implementation of fundamental rights in statute was likely to create problems for the operation of a legal system which did not inherently recognise positive rights.[220] Taking affirmative measures including the drafting of appropriate legislation in order to prevent privacy violations as well as enforcing the right to privacy are also strange, out of place elements to the common law in which rights are conceived as 'negative liberties' (i.e. whatever is not prohibited by statute is permitted).[221] Although suitable cases could open the way for the judiciary to design voluminous legal changes, the competence to make law through case by case jurisdiction is very limited by the system of checks and balances between the parliament and the courts.[222] These differences certainly cannot be seen as technicalities that can be easily overridden for the sake of guaranteeing the proper level to right to privacy. Yet, it can be assumed that the reasons behind the lack of willingness to pose wholesale changes in the field of the protection of privacy go beyond to the structural and procedural features of the common law tradition.

A key difference between the two dominant European traditions is that in contrast to the common law community, in the Western civil law countries the protection of privacy was a real human right demand in the late 1940s which responded directly to the horrors of totalitarian surveillance regimes, and has been predominantly developed in the framework of constitutional law (notwithstanding, the same is true of the post-Communist regimes analysed

[219] See for instance, Press release issued by the EC on the infringement proceeding launched against the UK, Brussels, 29 October 2009, available at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626; Memorandum of the Ministry of Justice of the UK, available at http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/8020603.htm (last accessed 31 October 2012).

[220] Collins, Val, "Privacy in the United Kingdom: a Right Conferred by Europe?" *Int'l J.L. & Info. Tech.*, Vol. 1, 1993-1994, p. 291.

[221] Memorandum of the Ministry of Justice.

[222] Masterman, Roger, *The Separation of Powers in the Contemporary Constitution, Judicial Competence and Independence in the United Kingdom*, Cambridge, 2011, p. 182.

above at Section 1.2). However, privacy protection in common law countries, which did not share these experiences, has been developed mainly in private law as a legitimate interest that is to be protected predominantly by tort law. According to Westin, the effect of this different historical past is reflected today in the difference of the balance between privacy and government in the two regimes. He argued that while Germany exhibits an 'authoritarian democratic balance', meaning that "respect for the privacy of person, home, office, press, still gives a way to the claims of official surveillance and disclosure", England exhibits a 'deferential democratic balance', in which there is "greater personal reserve between Englishmen, high personal privacy in home and private associations, and a faith in government that bestows major areas of privacy for government operations".[223]

The second wave of legal recognition of privacy protection was hallmarked by the recognition of the right to data protection in the 1970s and 1980s, and triggered by the technological developments, also prompted considerably by developments in Western-type constitutional democracies (data protection principles, generic laws on data protection etc.). However, these dynamics did not trigger the European common law regimes to identify personal data as something to be protected as a value. Although the UK adopted a Data Protection Act in 1984, the real catalyst for introducing the law was not a concern for individuals and their privacy right, rather the fear that the transborder data flow was likely to pose problems without legislation.[224] Otherwise, in the European Union, the introduction of data protection rules at this level was also not a normative moral demand for protecting fundamental rights, rather balancing the asymmetry of national data protection systems, which may distort competition and may be disadvantageous for the common market.

4.2.3 The right to privacy: universalism v. cultural diversity

As human rights are universal values, and privacy is recognised as such a right both in the ECHR and the Charter of Fundamental Rights of the EU, the question seems legitimate whether the discrepancy between the levels of the protection of privacy ensured by different legal regimes is consistent with the claim of the universality of human rights.
Although the diverging conceptions in literature of how to handle the anomalies generated by the tension between universalism and cultural relativism with regard to human rights can hardly be synthesised,[225] it can be maintained today that the axiomatic universality of human rights do not impose a uniform cultural standard, nor even a uniform legal standard for the sake of safeguarding these rights in general and the right to privacy in particular. What the ECHR provides for is 'only' a minimum legal standard that must be met by every member state. Therefore, even though the protection of the ECHR overarches every democratic legal system in Europe, the Convention cannot be interpreted as reflecting, or orienting towards, one preferred legal tradition or culture to the exclusion of others.[226] Indeed, even the universal aspiration of the ECHR to guarantee a minimum legal standard at regional level is

[223] Westin, Alan, *Privacy and Freedom*, 1967, New York: Atheneum, pp, 26-27, For a summary of the argumentation, see Bennett, Colin and Raab, Charles, "The privacy paradigm", in Hear, Sean P. and Greenberg, Josh (ed.) *The Surveillance Studies Reader*, Open University Press, 2009, p. 338.
[224] Collins, Val, "Privacy in the United Kingdom: a Right Conferred by Europe?" supra note 222, p. 293.
[225] Donnelly, Jack, *Universal Human Rights in Theory & and Practise*, Cornell University, 2003, pp. 89-105.
[226] So explicit in relation to the UN Charter, see Anyton-Schenker, Diana, *The Challenge of Human Rights and Cultural Diversity*, UN Background Note, United Nations Department of Public Information, DPI/1627/HR-March, 1995, available at http://www.un.org/rights/dpi1627e.htm (last accessed 31 October 2012).

compromised.[227] The development of the doctrine of 'margin of appreciation' under the ECHR has been unquestionably motivated by the aim of allowing the Court leeway to take into consideration the cultural and historical diversity of the Council of Europe's community of nations when adjudicating breaches of human rights obligations.[228] Since both the initial transplantation and the greatest extensions of the room for manoeuvre provided by the 'margin' doctrine were related to the concerns of national governments that international obligations could threaten the interest of national security,[229] the doctrine has become a major role in the jurisdiction of the ECtHR relative to the right to private life violated by state surveillance practices. Two examples will help clarify this point. In the well-known *Klass* case[230] (West) Germany was granted a wide margin to establish the conditions of the national secret wiretap system combating terrorism. Later, in the *Leander* case,[231] which challenged Sweden's secret police register, the ECtHR also invoked this doctrine and recognised that national authorities enjoy a wide discretion in choosing the means for achieving the legitimate aim of protecting national security.[232] Even though the ECtHR systematically emphasises that the wide margin permitted member states to arrange their national surveillance systems, the evaluation of the margin of appreciation is subject to its scrutiny so that to enforce adequate and effective national guarantees against abuses, and thus set forms of controls against arbitrary power-wielding. Furthermore, on the other hand the application of the 'margin' doctrine undoubtedly supports the maintenance of divergence between privacy regimes.

4.3 NATIONAL EXPERIENCES

4.3.1 The Belgian case[233]

The constitutional right to privacy (Article 22 of the Belgian Constitution) protects against secret surveillance, monitoring and searching computer data. Private communications are also protected by the constitutional right of secrecy of communications (Article 29 Constitution). An important instrument in privacy and personal data protection law is the Privacy Act (hereinafter 'the Act') which imposes obligations on data controllers in the public and private sectors, with some exemptions e.g. for police purposes.[234] The Act contains rights for the data

[227] Benvenisti, Eyal, "Margin of Appreciation, Consensus, and Universal Standards". *N.Y.U. J. Int'l L. & Pol.*, Vol. 31, 1998-1999, p. 843. Aolain, Fionnuala, Emergence of Diversity: Differences in Human Rights Jurisprudence, *19 Fordham Int'l L.J.* (1995-1996), p. 115-117.

[228] Yourow, Howard C, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence*, Martinus Nijhoff Publisher, 1996, pp. 4-6; Bakircioglu, Onder, The Application of the Margin of Appreciation Doctrine in Freedom of Expression and Public Morality Cases, *8 German L.J. (2007)* p. 717.

[229] In more details see Bakircioglu, (2007), *ibid.*, pp. 713-717., Yourow (1996), *ibid*., p. 21.

[230] ECtHR, *Klass v. Germany*, application No. 15473/89, judgment of 6 September 1978.

[231] ECtHR, *Leander v. Sweden*, application No. 9248/81, judgement of 26 March 1987.

[232] A detailed examination of the relevant case law greatly exceeds the limited scope of this paper. For a proper analysis on the application of the margin of appreciation doctrine see: Yourow (1996) *ibid*; Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Intersentia, 2001.

[233] VUB thanks Gertjan Boulet for his kind contribution to this report on Belgium. It refers to relevant legislation and case law which differentiates the faces of surveillance and surveillance technologies in Belgium. This report is partly based on an earlier country report on cybercrime legislation: De Hert, Paul, and Frédéric Van Leeuw, "Cybercrime Legislation in Belgium", in Eric Dirix & Yves-Henri Leleu (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Bruylant, Brussels, 2011, pp. 867-956.

[234] The Act of December 8, 1992 concerning the protection of privacy in relation to the processing of personal data, *Belgian Official Journal,* March 18th, 1993; The Constitutional Court has recently been asked whether the Privacy Act violates the Constitution because it does not provide a similar exception for private detectives: see

subject and duties for data processors, and established a Data Protection Authority.[235] The key principle of proportionality[236] has been translated to both the workplace for camera and e-mail monitoring,[237] and to the investigation and intelligence phase.[238] The Constitutional Court of Belgium guarantees the civil liberties, and recently judged that the Belgian Secret Service Act violated the Constitution for the lack of active notification duty after the end of surveillance.[239]

The criminal sanctions in the Act provide in theory a very suitable instrument to combat secret surveillance. Furthermore, the Criminal Code (CC) criminalises identity theft, hacking and wiretapping (Articles 231, 550*bis*, 314*bis* CC and 259*bis* CC). Although the prohibition of wiretapping leaves no possibility for employers to listen without an employee's consent to telephone conversations,[240] it does not apply to the control by an employer of e-mails stored on an employee's hard disc.[241] Yet, e-mail content is generally protected by the criminal provisions in Article 124 §1 and §3 of the Act of June 13th 2005 on electronic communications (hereinafter 'Electronic Communications Act'). The Electronic Communications Act also contains a special provision (Article 145 § 3, 1°) that could be used to prosecute hacking on the basis of fraudulent electronic communications through an

---

the Avis Officiels [Official Notices] in the *Belgian Official Journal*, November 25th, 2011, No. 2011/205887, p. 70044, http://www.ejustice.just.fgov.be/mopdf/2011/11/25_3.pdf#Page128

[235] The Data Protection Authority issued many opinions and recommendations, for instance: Data Protection Authority, Opinion No.10/2000 of April 3, 2000 on the supervision by the employer of the use of computer systems at work, http://www.privacycommission.be; Data Protection Authority, Opinion No. 34/99 on image processing carried out in particular through systems of video surveillance.

[236] The Supreme Court has recognised the horizontal effect of article 8§2 ECHR which contains the criteria (legality, proportionality and legitimacy) under which limitations of privacy are deemed possible: Supreme Court, January 27th, 2001: Kindt, Els, Eva Lievens, Eleni Kosta, Thomas Leys and Paul De Hert, "Constitutional Rights and New Technologies in Belgium", in Ronald Leenes, Bert-Jaap Koops and Paul De Hert (eds.), *Constitutional Rights and New Technologies*, T.M.C. Asser Press, The Hague, 2008, pp. 11-15 [pp. 20, 29 and 49].

[237] The proportionality has been found to be violated by the employer, by controlling e-mails merely based on rumours that the employee used his communication methods for concurring activities: Court of Appeal of Ghent, June 16th, 2011, cited by Saelens, Ronny, and Paul De Hert, "Gents hof hekelt e-mailcontrole op de werkplaats" [Court of Appeal of Ghent criticises secret e-mail control at work], *De Juristenkrant*, No. 250, May 2012, p. 3; The proportionality principle had been found to be blatantly violated by the employer, by, amongst other things, controlling e-mails sent to the employee in the evening or at night or while she was on leave without salary. It was reasonable to expect the employer to have known that such e-mails were of a private nature, with the result that an unlimited control as regards content was illegal: Labour Court of Appeal of Antwerp (Hasselt Division), November 15th, 2005, *Sociaalrechtelijke Kronieken*, No. 03, 2006, pp. 153-157.

[238] Two intelligence and security services exist: The Intelligence Services Act of November 30th, 1998, *Belgian Official Journal*, December 18th, 1998, see: http://www.comiteri.be/index.php?option=com_content&task=view&id=2&Itemid=53&lang=EN (last accessed 31 October 2012); De Hert, Paul, and Ann Jacobs, "Mesures de procédure spéciales et respect des droits de l'homme: rapport national belge" [Special procedural methods and respect for human rights], *Revue Internationale De Droit Pénal / International Review Of Penal Law*, issue (CD-ROM Annexe), Vol. 80, No. 1-2, 2009, pp. 29-66 [33-34].

[239] Constitutional Court, September 22th, 2011, No. 145/2011, cited by: De Hert, Paul, and Franziska Boehm, "The Rights of Notification after Surveillance is over: Ready for Recognition", in Jacques Bus, Malcolm Crompton, Mireille Hildebrandt and George Metakides (eds.), *Digital Enlightenment Yearbook 2012*, Amsterdam, IOS Press, 2012, 332 p. [pp. 20, 27 and 38].

[240] De Hert, Paul, "De wet van 30 juni 1994 en het afluisteren. Een sociaalrechtelijke toets" [Implications of the Belgian Tapping Act for Workplace activities], *Oriëntatie*, No. 4, April 1995, pp. 106-111.

[241] Belgian Data Protection Authority, Recommendation no 08/2012 of May 2, 2012 on the control by the employer of the use of electronic communication instruments at work, p. 11.

electronic communication network. Finally, the law on surveillance cameras also contains criminal provisions.[242]

Surveillance in Belgium has different faces. Security services include surveillance and monitoring but are strictly regulated, just as private detectives are.[243] The Federal Police controls the border and uses surveillance technology, among others, X-ray, heartbeat detection, passive millimetric wave detectors and biometric visas.[244] Noteworthy is the debated grey zone between general police powers and investigation methods for which stricter rules and prior authorisation by the Public Prosecutor or Investigative Judge apply.[245] As the constitutional right to inviolability of the home (Article 15 Constitution) does not protect against visual intrusion by the police when the door is open, a similar logic might apply to proactive investigation on the Internet. Investigatory powers include a network search, wiretapping (Article 88ter of the Code of Criminal Procedure (CCP) and Article 90ter §1CCP), and special and other investigation methods.[246] Belgian law enforcement agencies also cooperate with the private sector: Internet service providers can be asked to supply specific information or a temporarily surveillance period.[247] Production and preservation orders can be given to electronic communication providers (Article 46*bis* and 88*bis* CCP; Article 126 of the Electronic Communications Act) and to notaries, bailiffs and accountants.[248] Wiretapping support can be required from (tele)communication providers (Article 90quater §2 CCP).

In the workplace, secret camera monitoring (without prior notice) is forbidden,[249] unlike permanent Internet and e-mail monitoring.[250] Although no privacy violation would follow

[242] Act of March 21th, 2007 on the installation and use of surveillance cameras, *Belgian Official Journal*, May 31th, 2007.

[243] Law Organizing the Profession of Private Detectives: Law of 19 July, 1991, *Belgian Official Journal,* October 2nd, 1991; See: Reiter-Korkmaz, Axelle, "Belgian National report on Private Military and Security Companies", PRIV-WAR *National Reports Series*, No. 06/09, pp. 9-12, http://priv-war.eu/wordpress/wp-content/uploads/2009/05/nr-06-09-bel.pdf; Law regulating private security: Law of April 10th, 1990, *Belgian Official Journal, 29 May, 1990;* See Reiter-Korkmaz, Axelle, *o.c.*

[244] Perrin, Nathalie, "Practical Measures for Reducing Irregular Migration in Belgium", Report for the European Migration Network (EMN) Belgium National Contact Point, Brussels, 2012, 62 p. [p.25], http://www.emnbelgium.be/nl/node/1082 (last accessed 31 October 2012).

[245] Conings, Charlotte, and Philippe Van Linthout, "Sociale media. Een nieuwe uitdaging voor politie en justitie" [Social media. A new challenge for police and justice], *Panopticon*, Vol. 33, No. 3, 2012, pp. 217-224; Vermeulen, Mathias, and Paul De Hert, "Toegang tot sociale media en controle door politie. Een eerste juridische verkenning vanuit mensenrechtelijk perspectief" [Access to social media and control by police. A first legal exploration from the human rights perspective], *Panopticon*, Vol. 33, No. 3, 2012, pp. 258-272.

[246] The Act of January 6th 2003 concerning special investigation methods and any other methods of investigation, *Belgian Official Journal*, May 12th, 2003: observation, infiltration, direct monitoring, looking-in operations and data collection regarding bank accounts and –transactions.

[247] Act on Certain Legal Aspects of Services in the Information Society Service: Act of March 11th, 2003, *Belgian Official Journal*, March 17th, 2003.

[248] Law of 11 January 1993 on preventing use of the financial system for purposes of laundering money and terrorism financing, *Belgian Official Journal* , February 9th, 2005, http://www.imolin.org/doc/amlid/Belgium_law_11_January_1993.pdf (last accessed 31 October 2012).

[249] National Labour Council, *Collective Labour Agreement no. 68 of June 16th, 1998 concerning the protection of the privacy with regard to video monitoring at the workplace*, declared legally binding by royal decree of September 20th, 1998, *Belgian Official Journal*, February 2nd, 1998. The Agreement also applies to camera-surveillance that is not covered by the Belgian Privacy Law.

[250] National Labour Council, *National collective agreement no. 81 of April, 26th, 2002 on the protection of the private lives of employees with respect to controls on electronic on-line communications data*, declared legally binding by Royal Decree of June 12th, 2002, *Belgian Official Journal*, June 29th, 2002. The agreement covers all on-line technologies such as the Internet, e-mail and WAP, but has been drafted sufficiently wide so as it will also cover future developments; See De Hert, Paul, and Mieke Loncke, "Camera Surveillance and Workplace

from the inspection by the employer of documents with a professional character and stored on a company computer, the search of private documents by the employer still seems to require the employee's consent or the involvement of the investigative authorities, even if the employer explicitly prohibited to store those documents on a company computer or network.[251] Acting to the contrary is punishable for usurpation of authority by the employer (Article 227 CC).

4.3.2 The Hungarian case

Hungary is one of the so-called new democracies of Europe, a country which belonged to the Soviet Bloc from the end of the Second World War until the political changes in 1989. As explained at Chapter 2 of this Deliverable, Hungary was among the first to build a legal and institutional system and the accompanying practice of treating informational rights and freedoms not as separate entities but as organic elements of a new and comprehensive system. This historical advantage was mainly due to an informal multidisciplinary group that had grown up under the wing of the Central Statistical Office (KSH) in the 1980s, collected and analysed Western debates, publications, laws, and legal practice, and fashioned a comprehensive concept for the new information regime (the group later gave Hungary, among others, the first president of its new Constitutional Court, who also became President of the Republic, and the first and second parliamentary commissioners for data protection and freedom of information).[252]

From the aspects of the legislation and case law on privacy, data protection and surveillance, as well as the enforcement of mechanisms of legal resilience to counter the development of surveillance systems the historical period from 1989 until today can be divided into two parts. The first part can be counted from the proclaiming of the Third Republic of the country in 1989, the second part from the profound changes in legislation introduced by the new parliamentary majority in the 2010s.

The Hungarian model, similarly to the early models in several other countries of the CEE region, drew a dichotomy between state and non-state information, signalling that the prime objective of the new system was to break the state's monopoly on information.[253] The model, which is still applicable – although refined in the course of enacting of detailed legal provisions on processing information – defined two fundamental categories of information/data: personal data and data of public interest. For the former the fundamental rule is informational self-determination, for the latter it is openness. Surveillance (similarly to secrecy) is regarded as an exception from the main rule.

Privacy in Belgium", in Sjaak Nouwt, Berend R. De Vries and Corien Prins (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, The Hague, 2005, pp. 167-209 [p. 189], http://www.vub.ac.be/LSTS/pub/Dehert/017.pdf

[251] Labour Court of Antwerp, April 3rd, 1998, cited by De Bie, Bart, Leen Cornil and Stijn De Meulenaer, "Interne fraude en privacy: hoe ver kan (mag) een werkgever gaan? [Internal fraud and privacy: how far can (may) an employer go?]", in X (ed.), *Handboek Security – Beheersing van criminele risico's [Handbook Security – Control of criminal risks]*, Vol. 8, No. 3.8.5/58, September 2003, pp. 107-166, p. 130.

[252] For more on this, see Szekely, Ivan, "Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation*, Edward Elgar Publishing Ltd., November 2008.

[253] Szekely, Ivan, "Central and Eastern Europe: Starting from Scratch", in Ann Florini (ed.), *The Right to Know. Transparency for an Open World*, Columbia University Press, 2007.

The system follows the European general Act – sectorial Acts model. The general Act was the combined data protection and freedom of information Act of 1992 (DP&FOIA) encompassing both the public and private sectors. However, as opposed to new democracies where legislation on informational rights and freedoms remained a unique, exotic piece of law, in Hungary nearly 1,000 sector-specific acts and regulations contain provisions on the processing of personal data,[254] including the exceptions, such as surveillance. In other words, the system of newly established informational rights has penetrated the whole legal corpus. This situation gave the country a historical advantage over other countries of the CEE region and in the first decade after the political changes, Hungary became a sort of a model country regarding informational rights and freedoms.

Provisions regarding surveillance can be found, among others, in the Police Act, the National Security Act, or in the Act on Security Services and the Activities of Private Investigators. Provisions relating to workplace privacy and the special informational relationship between the employer and the employee (including the possibilities of the employer to openly or secretly monitoring the employee's activities), can be derived mostly from the general rules of handling personal data (although the new labour code specifies some of these provisions). As discussed elsewhere, the process of lustration also has an indirect relationship to surveillance, in the sense that the information relating to former agents who performed unlawful surveillance activities and former victims of such surveillance may become accessible to the persons concerned or the general public. Hungary opted for a model in which former secret service agents and other persons involved in unlawful surveillance were asked to leave their positions in public or political life on the quiet, but they were not obliged to leave: if they wanted to stay, as the greatest sanction under the new law, their pasts were simply made public.[255]

The most successful institution in this regard was the newly established Parliamentary Commissioner for Data Protection and Freedom of Information, first elected in 1995. The independent Commissioner was responsible for the supervision of both the protection of personal data and the freedom of information, and, besides the obvious economic considerations, the joint interpretation of the two rights had a significant advantage of ensuring consistent positions on the borderlines between the two informational rights. The success of this model had a positive impact on other European countries, which later opted for introducing such a combined supervisory function.[256] In general, the Commissioner's powers were "weak," such as those associated with an Ombudsman: he possessed broad investigative powers but could only make formally nonbinding recommendations. In the majority of the cases, however, the data controllers followed the Commissioner's recommendations even if they disagreed with his arguments.[257]

After a decade of enthusiastic building of informational rights and establishing institutional guarantees, however, both the social and political environments have changed. Rights and freedoms became less important for the new generation, while government and business

[254] Szekely (2008), *ibid*.
[255] In order to avoid the trap of retroactive legislation, the only way of sanctioning these persons was to prove the unlawfulness of such surveillance activities even under the laws which had been formally in force at that time.
[256] See for example: Dix, Alexander, "The influence of Hungarian freedom of information legislation abroad – the Brandenburg example and experience", in Laszlo Majtenyi (ed.), *The Door Onto the Other Side: A report on information rights,* Office of the Parliamentary Commissioner for Data Protection and Freedom of Information, Budapest, 2001 [bilingual edition].
[257] See the annual reports of the Commissioner, both in printed and electronic formats. See also Szekely, Ivan, "Central and Eastern Europe: Starting from Scratch", supra note 253.

entities gained momentum in restricting the newly established information rights in the name of efficiency and security. As Szekely analysed,[258] the knowledge of the Hungarian population about information laws and institutions significantly decreased between 1989 and 2006, and the acceptance of various surveillance practices was the highest among the countries surveyed in the Globalization of Personal Data project.[259]

After the coming into power of the new parliamentary majority in 2010, significant changes have been introduced both in legal and institutional terms. The most critical observers even reported on the fall of the Third Republic and heavily criticised the weakening of the system of constitutional rights and the violations of the rule of law.[260] Civic and professional organisations, such as the Eotvos Karoly Policy Institute, have monitored the changes and published evaluative reports on the constitutional changes, the curtailment of individual rights and freedoms, the restrictions on the free media, and the limitations of judicial independence.[261] The Constitution has been replaced by a Basic Act, the DP&FOIA by the so-called Act on informational self-determination and freedom of information, and the institution of the parliamentary commissioner has been abolished and replaced by a government authority, the National Authority for Data Protection and Freedom of Information. The new authority can issue binding resolutions and impose fines on data controllers, however, the authority's real independence is questionable, with special regard to cases relating to surveillance activities of the Government of which it is part. In October 2011 three civil organisations sent a letter to José Manuel Barroso, President of the European Commission, asking him to investigate the case of replacement of the institution of the Commissioner.[262] The dismissal of the Commissioner served as one of the three main reasons why the European Commission started an infringement action against Hungary in early 2012.[263]

The recent history of Hungary in the area of information rights and legal resilience against surveillance has high and low tides in the sense of legal and institutional guarantees. The former forerunner of information rights has become a warning signal by now. Although legal guarantees have been weakened, the fundamental system of rights and freedoms is still strong, however the practical realisation of the guarantees have now less chances than in the first period after 1989. This scenario well demonstrates the importance of the period of fundamental political changes in establishing legal and institutional guarantees in the area of informational rights. These phenomena are accompanied by "jumping into postmodernism" – as discussed higher at Section 2.2 of this Deliverable –, the partial lack of historical

[258] Szekely, Ivan, "Changing attitudes in a changing society? Information privacy in Hungary 1989–2006", in Zureik, Elia, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan (eds.), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, London, Ithaca, 2010.

[259] Queen's University, Surveillance Studies Centre, *The Globalization of Personal Data Project (2003-2007)*, see http://www.sscqueens.org/projects/gpd (last accessed 31 October 2012).

[260] The Eötvös Károly Institute (EKINT), *Hungarian NGOs assess the new Constitution of Hu*ngary, http://www.ekint.org/ekint/ekint_angol.news.page?nodeid=454 (last accessed 31 October 2012).

[261] The Eötvös Károly Policy Institute, *Analysis on the Constitutional Changes in Hungary*, http://alaptorveny.eu (last accessed 31 October 2012).

[262] The Eötvös Károly Policy Institute, *Letter on the Independence of the Data Protection Authority*, http://alaptorveny.eu, also available at http://www.ekint.org/ekint_files/File/barroso_dpa_independence_20111106_printed.pdf (last accessed 31 October 2012).

[263] European Commission, Economic and Financial Affairs, *European Commission launches accelerated infringement proceedings against Hungary*, http://ec.europa.eu/economy_finance/articles/governance/2012-01-18-hungary_en.htm (last accessed 31 October 2012).

experience in practicing democratic rights, and the legacy of surveillance practice of the past political system. All this can serve as lessons for other European (and non-European) new democracies too.

4.3.3 The Spanish case

In relation to the legal framework regarding privacy and data protection, Article 18 of the Spanish Constitution establishes: 1) The right to one's honour, personal and family privacy [*intimidad*] and one's own image is hereby guaranteed; 2) One's home address is inviolable. No entrance or search can be carried out without the consent of the owner or judicial authorisation, unless a flagrant crime or offence has been committed; 3) The confidentiality of communications, whether they are postal, telegraphic or via phone, unless there is judicial authorisation, and 4) The law will limit the use of informatics in order to protect the honour and personal and family privacy of citizens and their full enjoyment of their Rights. Article 10 of the Spanish Constitution also establishes the recognition of the related right to one's dignity. The right to personal data protection stems from Articles 10 and 18.4 and is developed in the Organic Law[264] 15/1999 of Personal Data Protection (*Ley Orgánica de Protección de Datos*, LOPD, in Spanish). The LOPD specifically recognises the right to be informed when data-gathering involving personal information takes place, the right to access, rectify and cancel personal data found at the General Registry of Data Protection, where information on all declared files is kept, and the right to oppose the gathering of personal data.[265]

The Spanish Data Protection Agency (Agencia Española de Protección de Datos, AEPD, in Spanish) was created in 1993 and is the control body responsible for the fulfilment of the Spanish Organic Law of Personal Data Protection. It has its headquarters in Madrid and its scope of action comprises the whole country. It is a body of public law with its own legal status and full public and private capacity that act independently of the public administration in the exercise of its functions. AEPD oversees the compliance with data protection legislation by people in charge of files that include personal data (public entities, private companies and other organisations).[266] Due to the decentralised nature of the Spanish state, there are also regional DPAs.[267] The Spanish DPAs main function is to oversee and control the implementation of the legal framework regarding data protection, especially in relation to the rights of information, access, rectification, opposition and cancellation of personal information gathered by any authority, private body or individual. In order to do so, the Agency can issue sanctions and authorisations as stated in the legal framework, to establish measures of correction when a breach of rights is detected, to determine the unlawfulness of specific data-gathering processes and procedures, to provide information and to authorise the international transfer of information. Faced with specific demands by Spanish citizens, the Spanish DPA must provide any information required, to inform of the rights recognised,

[264] In the Spanish legal framework constitutional matters relating to fundamental rights and freedoms are regulated by Organic Laws, which require a parliamentary debate and an absolute majority to be approved.
[265] Agencia Española de Protección de Datos (AEPD), *Guía del derecho fundamental a la protección de datos de carácter personal*, 2004, available at http://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf (last accessed 31 October 2012).
[266] Agencia Española de Protección de Datos, http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (last accessed 31 October 2012).
[267] See for example the Autoritat Catalana de Protecció de Dades (APDCAT), www.apd.cat (last accessed 31 October 2012).

attend to all claims and complaints, and to promote the dissemination of the activities of the agency and data protection issues in general.

Spain has recently seen many controversies in relation to data protection. One of the most relevant is that around the issue of the so-called 'right to be forgotten' or 'right to oblivion' [*derecho al olvido*]. While the Spanish DPA does not recognise the right to be forgotten as a right *per se*, it does recognise the possibility for individuals to demand that one's stored information is erased if there are good grounds for it – but these must be considered case by case.[268] [269] This has generated a debate around the limits of such a right, and its impact on 'data veracity' and the individualistic nature of a right that only exists once an individual demands it, and so is dependent on a person's responsibility and needs to be acted upon.

A specific example of this controversy is the case of Google. In 2011 the AEPD filed 90 court orders against Google at the request of individuals who wanted the search engine to remove specific links that, they felt, shed a dim and untruthful light on their past. In one of the cases, the court heard arguments from both sides. Google argued that the search engine is just an intermediary platform for content, and that it is publishers that should be responsible for the content. According to the AEDP, the original publishers cannot legally be ordered to take content down, and Google, with its cookies and continued collection of personal information, is the one violating Spanish citizens' privacy rights.[270] Therefore, Google is responsible for the elimination of personal information, and this can be requested directly to the search engine even if the relevant information remains in pages of third parties. The issue of the right to be forgotten continues to be controversial, however, and each case is being analysed independently.

Another controversial case has been CCTV and the EU Directive on services in the internal market. This represents a clear example of national and supranational disparities and lack of consensus, as the adaptation of the EU directive to the Spanish legal framework has resulted in less legal control on private CCTV devices. Spain has a clear imbalance between public and private CCTV regulations, in the sense that while public CCTV systems are highly regulated, private CCTV schemes are only subject to a minor data protection directive - therefore, a greater control of private schemes would be desirable, even if just to avoid the grey areas that emerge in such an imbalanced context.[271] However, the Spanish 'Omnibus law' that adapts the Bolkerstein Directive, established the "exclusion of companies providing technical equipment for security purposes. Private security service providers or their subsidiary companies selling, installing or maintaining technical security equipment, as long as they do not provide a connection to a central alarm system, are excluded from that established in the private security law".[272] So while before 2009 all CCTV cameras had to be

[268] Romero, Pablo, "The limits of the right to oblivion", *El Mundo*, 27 February 2012, http://www.elmundo.es/elmundo/2012/02/22/navegante/1329915513.html (last accessed 31 October 2012).

[269] Zaplana, José Guerrero, "Aproximación al derecho de olvido en el nuevo reglamento de protección de datos", *Foro Público*, 17 July 2012, available at http://publico.blogs.lexnova.es/2012/07/17/aproximacion-al-derecho-al-olvido-en-el-nuevo-reglamento-de-proteccion-de-datos/ (last accessed 31 October 2012).

[270] Boyd Myers, Courtney, "In the first case of its kind, Spain takes Google to court over privacy issues", *TNW online magazine* 19 January 2011, http://thenextweb.com/google/2011/01/19/is-your-past-etched-in-the-internet-spain-takes-google-to-court-over-it/ (last accessed 31 October 2012).

[271] Galdon Clavell, Gemma, Zuloaga, L. and Romero, A., "CCTV in Spain: an empirical account of the deployment of video-surveillance in a Southern-European country", *Information Polity*, 17(1), 2012.

[272] Galdon Clavell, Gemma, "La videovigilancia va en Ómnibus", *Público,* Madrid, 2010, available at http://blogs.publico.es/civismos-incivicos/2010/07/06/la-videovigilancia-va-en-omnibus/ (last accessed 31 October 2012).

connected to a central alarm system and their existence (and that of files with personal information) be communicated to the Spanish DPA, as a result of adapting EU law to the national legal framework those CCTV systems that are not connected to an alarm system do not need to declare to the AEPD the fact that files with personal information are being created. The liberalisation of service provision is thus damaging legal protection in the fields of data protection, privacy and CCTV.

A third example of a controversy regarding privacy and data protection is the law of transparency and access to information, which is currently being drafted in Spain -the only major EU country without a similar text. The Organization for Security and Cooperation in Europe (OSCE) recently pointed out that "the draft did not comply with principles and standards already set by the Human Rights Tribunals".[273] The draft has ignored civil society groups' suggestions, such as the need to recognise access to information as a fundamental right. It also excludes the right of the public to request access to government emails, draft reports, notes and internal communications, thus making accountability difficult and moving the focus on transparency away from government activity.
These three examples show how in Spain, privacy and data protection are highly controversial and problematic issues. Besides the need to revise a 13-year old data protection law, several issues need urgent attention, such as the need to explore the problems linked to the adaptation of EU legislation into the local legal framework, the need to strengthen the legal control over the proliferation of privately-managed surveillance systems and the need to revise the relationship between central and regional legislation when it comes to privacy, data protection and surveillance. Perhaps one of the most crucial and urgent issues, however, is the transparency law, as accountability and civil-society control and activism could be a good antidote to ineffective legal protection. However, as Access Info Europe recently stated in relation to Spain's Action Plan for Open Government, 'Spain still has a long way to go in catching up with the democratic standards regarded as the norm in most of Western Europe'[274] in terms of public participation and understanding of what transparency, accountability and legal protection means.

4.3.4 The UK case

Legislation and other measures to limit and regulate surveillance in the United Kingdom (UK) is a patchwork quilt with many holes.[275] The current UK approach is a hybrid of Nissenbaum's 'omnibus' and 'sectoral' approaches to privacy law and regulation,[276] and as such the resultant inconsistency and complexity obscures many fundamental privacy principles that safeguard individuals and groups against the excesses of surveillance practice. There is no single privacy statute or comprehensive 'privacy law': information privacy is

[273] Goldman, Lisa "Spain's Draft Law on Transparency and Access to Information Disappoints Civil Society NGOs", *Techpresident*, 15 August 2012, available at http://techpresident.com/news/wegov/22724/spains-draft-law-transparency-and-access-information-disappoints-civil-society-ngos (last accessed 31 October 2012).
[274] Access Info Europe, *Spain's action plan for the open government partnership is weak and vague, and has not been subject to a public consultation*, available at http://www.access-info.org/en/spain-coalicion-pro-acceso/237-spain-in-ogp (last accessed 31 October 2012).
[275] This subtask draws upon Raab, Charles and Benjamin Goold, *Protecting Information Privacy*, Research Report 69, Equality and Human Rights Commission, London, 2011. It also reflects some of the discussion in House of Lords Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-I, The Stationery Office, London, 2009.
[276] Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010, pp. 237-238.

protected through a mix of statutes, legal regulations, common law rules, and systems of informal regulation ('soft law'). Guidance by regulators and codes of practice play an important part: for example, there are codes for CCTV, data-sharing, policing, data-matching practices, online privacy, employment, and the fair processing of telecommunications directory information, and other domains in which surveillance is practiced. Beyond that, there are other instruments for information privacy protection that play a role in conjunction with law or codes.

The Human Rights Act (HRA) of 1998[277] inscribes the provisions of the European Convention on Human Rights (ECHR) into UK law; thus Article 8 (1) declares that "[e]veryone has the right to respect for his private and family life, his home and his correspondence", with the familiar ECHR statutory override in Article 8 (2). The HRA makes it possible to seek remedies in UK courts, without requiring plaintiffs to resort to the European Court of Human Rights (ECtHR).

Data protection legislation precedes the HRA: first in 1984 with the Data Protection Act (DPA) 1984,[278] which developed statutory protections for information privacy, the DPA, 1984 was replaced by the DPA, 1998,[279] which transposed the EU Data Protection Directive 95/46/EC[280] into UK law, although as in the 1984 Act but unlike the Directive – the term 'privacy' was eschewed.[281] The DPA 1998, like its predecessor, establishes a regulatory regime. It is centred on the Office of the Information Commissioner (ICO), which plays a number of roles aimed at amplifying the formal enforcement powers by means of guidance, codes, exhortation, and the promotion of public awareness and education. However, the powers of the ICO to enforce the Act and to apply fines and other penalties are restricted by statute, although they have recently been somewhat expanded, and the DPA itself is not regarded as an example of a stronger privacy or data protection statute. Moreover, 'data protection' does not encompass the range of privacy values or rights that are involved when surveillance is practiced.[282]

A further, and controversial, statute of great significance is the Regulation of Investigatory Powers Act (RIPA) 2000.[283] RIPA replaced the Interception of Communications Act 1985[284] and governs the exercise of surveillance powers by the police and a large number of other

[277] Human Rights Act 1998 (1998 Chapter 42).
[278] Data Protection Act 1884 (1984 Chapter 35).
[279] Data Protection Act 1998 (1998 Chapter 29).
[280] *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*, No L 281/31, 23.11.95.
[281] See Gillian Black, "Data Protection", in *The Laws of Scotland – Stair Memorial Encyclopaedia*, The Law Society of Scotland, Edinburgh 2011, para. 12: "The tension between these two approaches [privacy and data protection] is becoming increasingly clear in a number of English cases, where the judiciary has turned to the Directive for guidance on the interpretation of the Act, with the consequence that a privacy emphasis is read into the purpose of the Act. …One possible cause for this divergence is the lack of a clear, prior right to privacy in Scots (and English) law. If there were a right to privacy in the United Kingdom as a whole, then the Act could focus on the protection of personal data, as it does, leaving the privacy aspects of the Directive to the prior right of privacy. Since this is not the case, the silence in the Act on privacy per se arguably means that the United Kingdom has failed to implement its obligations under the Directive". See the further discussion, including cases, in paras. 410-416. The conceptual distinction between privacy and data protection is referred to in the subsection on 'Surveillance and the Rule of Law' in IRISS Task 1.5, Deliverable D.1.
[282] See the earlier discussion of privacy and other values in IRISS Task 1.5.
[283] Regulation of Investigatory Powers Act 2000 (2000 Chapter 23). Its counterpart in Scotland is the Regulation of Investigatory Powers (Scotland) Act 2000.
[284] Interception of Communications Act 1985 (1985 Chapter 56).

public bodies. An exceptionally complex and unclear statute, it was enacted in the light of HRA Article 8, and covers a range of activities that include wiretapping, the interception of communications, 'directed'[285] and 'intrusive'[286] surveillance, and the surveillance of public, semi-private and private spaces. RIPA provides a framework for the authorisation and review of surveillance activities, establishing the Office of the Surveillance Commissioner (OSC), but the bulk of authorisations are internal to the surveillant organisation in question, and – given the lack of provision for judicial authorisation – difficulties have been experienced in interpreting the Act regarding when, and by whom, approvals must be provided.[287]

The OSC and the ICO is part of a surveillance regulatory regime operating under these laws, that also includes the Interception of Communications Commissioner (ICC). This can be a confusing and fragmentary approach to responsibility and to disparities in the extent of oversight and enforcement provided in the different domains in which regulators operate. Arguments for merger or, instead, better co-ordination, are frequently made. Less commonly discussed is the need for a more anticipatory, proactive approach by regulators as changes occur in the personal-data activities of individuals and organisations, and as new technologies as well as new trends and technologies emerge in surveillance and data collection.

A few of the most prominent cases in, or involving, the UK in the surveillance field – mainly involving data protection – can be mentioned briefly in terms of the issues involved. *Durant v. Financial Services Authority*[288] concerned the meaning of 'relevant filing system' and served to narrow the definition of 'personal data' – a definition that is heavily contested and of crucial importance in determining the scope of application of the DPA and of the Directive. *S and Marper v. The United Kingdom*,[289] a decision of the ECtHR that concerned the retention of DNA samples of persons who were not charged with a crime or who were acquitted, ruled that ECHR Article 8 rights were violated by the indiscriminate and sweeping powers of retention in England (but not in Scotland) that did not strike a 'fair balance' between the private and public interests.

In *Wainwright v. Home Office*[290], the Home Office won their appeal against the lower court's judgment that Wainwright's right to privacy was invaded when strip-searched upon visiting a prison. The Court rejected the claim that was made under ECHR Article 8, and denied that inhuman and degrading treatment had been involved (ECHR, Article 3); also, any tort of privacy invasion was too uncertain. Unlawful covert surveillance by a private investigator

[285] Defined as comprising covert observation or monitoring by whatever means, for the purpose of a specific investigation or operation, and which will or is likely to gather information about any person, not just the targeted individual.

[286] Defined as covert, carried out on any residential property or in any privacy vehicle, and involving the presence of an agent on the premises or in the vehicle or the use of a surveillance device. In practice, the distinction between 'directed' and 'intrusive' surveillance is not clear-cut.

[287] For further discussion, see Raab, Charles and Benjamin Goold, *Protecting Information Privacy*, Research Report 69, Equality and Human Rights Commission, London, 2011, pp. 35-41, where some relevant cases are cited. Criticism of RIPA can be found in House of Lords Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-I, The Stationery Office, London, 2009, and in HL Paper 18-II, which contains the written and oral evidence for the Report.

[288] *Durant v. Financial Services Authority* [2003] EWCA Civ 1746, [2004] FSR 28. See the discussion in Gillian Black, "Data Protection", in *The Laws of Scotland – Stair Memorial Encyclopaedia*, The Law Society of Scotland, Edinburgh 2011, paras. 64-66.

[289] ECtHR, *S. and Marper v. the United Kingdom*, application n. 30562/04 and 30566/04 judgement of 4 December 2008.

[290] *Wainwright v. Home Office*, [2003] UKHL 53, [2004] 2 AC 406. See also Boghal, Monica, "United Kingdom Privacy Update 2003", http://www.law.ed.ac.uk/ahrc/script-ed/docs/privacy_comment.asp#Peck (last accessed 24 October 2012).

was alleged in *Martin v. McGuiness*[291], a Scottish case that was brought under ECHR Article 8, but was rejected on the grounds that the surveillance was reasonable and proportionate. *Peck v. United Kingdom*[292] involved the disclosure to a television station of CCTV footage of an unmasked person who was recognised when the footage was broadcast. The case, which was prior to the enactment of the HRA, went to the ECtHR, which decided that his Article 8 rights had been breached by the disclosure. There have also been prominent UK privacy cases involving 'celebrities'.

A degree of judicial activism has led to the piecemeal and circumstantial development of common law jurisprudence in the privacy field concerning breaches of confidence, which are sometimes involved in privacy infringements. This development could lead to a widening of disparities across the component legal jurisdictions of the UK, in which decisions in one part do not bind the courts in other parts. In addition, common law litigation is costly and could lead to wider distinction between the 'haves' and 'have-nots' in terms of privacy and remedies for excessive surveillance.

In sum, while many forms of surveillance pose threats to privacy and other human rights and values, in the UK it has not been easy to regulate these or for individuals to achieve success in the courts owing to the lack of a single privacy law or a coherent and powerful system of regulatory controls and limits.

4.3.5 The Norwegian case[293]

In the early 1970s two reports[294] were solicited by the Norwegian Parliament to address concerns regarding personal information in relation to the introduction of computers and digital solutions. Based on these reports the Person Register Act (*Personregistreringsloven*) was adopted by the Parliament in 1978.[295] The act has been revised several times and was eventually replaced by the Personal Data Act (*Personopplysningsloven*) 1 January 2001. The ambition of the new act was to ensure legal durability by making it independent of technological advancement.[296] The Personal Data Act now constitutes the legal foundation for all matters related to personal privacy, and supports the implementation of the EU Data Protection Directive in Norway.[297] According to plan, the EU Data Retention Directive (DLD

[291] *Martin v. McGuiness*, 2003 SLT 1424. See http://www.shrlg.org.uk/2009/03/29/martin-v-mcguiness/ (last accessed 24 October 2012).
[292] *Peck v. United Kingdom*, [2003] EMLR 15. See also Boghal, Monica, "United Kingdom Privacy Update 2003", http://www.law.ed.ac.uk/ahrc/script-ed/docs/privacy_comment.asp#Peck, (last accessed 24 October 2012).
[293] PRIO thanks Marit Moe-Price as the author of this paragraph for her kind contribution to the IRISS project.
[294] Norges offentlige utredninger, *Personal data and personal privacy*, Norway, 1974. Norges offentlige utredninger, *Public person-data system and personal privacy*, Norway, 1975.
[295] Justis og beredskapsdepartementet, *Official report on improving personal privacy*, Norges offentlige utredninger, Norway, 1997, p. 32. Available at http://www.regjeringen.no/nb/dep/jd/dok/nouer/1997/nou-1997-19/6.html?id=140976 (last accessed 31 October 2012).
[296] Fornyings og administrasjonsdepartementet, *Official report on the individual and integrity. Privacy in the digital society*, Norges offentlige utredninger, Norway, 2009, p. 61, available at http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/8/1.html?id=542111 (last accessed 31 October 2012).
[297] *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*, No L 281/31, 23.11.95.

2006/24/EF, hereafter DLD)[298], adopted by the Norwegian parliament 4 April 2011, will also be implemented under the same legislation in 2013. Together these two regulations constitute the main legal framework for personal privacy in Norway.

The Data Inspectorate (*Datatilsynet*) oversees the implementation and monitors the practice of the above mentioned acts and regulations in Norwegian society. Additionally it serves as an *ombudsman* for private citizens on data protection and surveillance. It is also a watchdog for new, particularly technological, innovations which surveil or otherwise potentially infringe on the individual's right to privacy. It is a small, independent administrative body under the Ministry of Government and Reform (*Fornyings-og administrasjonsdepartementet*) with approximately 40 employees. It was established on 1 January 1980 following the implementation of the 1978 Person Register Act (Datatilsynet, Om datatilsynet n.d). As a non-EU member the Data Inspectorate only has a limited association to the important European bodies on personal privacy; it is an observer of Schengen's Joint Supervisory Authority (JSA); the European Data Protection Supervisor (EDPS), and the Article 29 group. It is not taking part in the work of EUROJUST's Joint Supervisory Body (JSB)[299], and is very unlikely to be included in the new European Data Protection Board.[300]

In accordance with the introduction of the Personal Data Act, an independent *Personvernsnemnd* (Personal Privacy Committee) was established 1 January 2001 which handles appeals against decisions made by the Data Inspectorate. Appeals had previously been processed by the Ministry of Justice and Police, with the new body being created in order to strengthen the independence of the Data Inspectorate and the position of personal privacy in society.[301] Norway's participation in the Schengen's cooperation, and Schengen following EU integration in 2001, stands as a milestone with regards to surveillance in Norway. As a result, Norway also became fully involved with European surveillance databases (SIS, Eurodac, VIS, Prüm), but as noted above, Norway is only partially involved in the controlling mechanisms.

The introduction of the DLD has been the single most important issue in the Norwegian debate in recent years. The Conservative party were divided in their position on the directive, but decided to support it in March 2011. Shortly thereafter they struck an agreement with the Labour party and secured a parliamentary majority sufficient to pass the directive. It was adopted 4 April 2011 with a majority of 9 votes (89 / 80).[302] The primary concerns in the Norwegian debate centred around if, and to what extent, the DLD was in breach with Article 8 of the European Convention of Human Rights (ECHR) which determines the right to

[298] Directive 2006/24EC 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, No L 105/54, 13.04.2006.
[299] Interview with an official of Datatilsynet, Oslo, November 2008.
[300] Datatilsynet, *Annual Report 2011*, Norway, February 2012, p. 5. Available at: http://www.datatilsynet.no/Om-Datatilsynet/Planer-rapporter/Arsmeldinger/Arsmelding-20111/ (last accessed 31 October 2012).
[301] Justis og beredskapsdepartementet, *Official report on improving personal privacy*, Norges offentlige utredninger, Norway, 1997, p. 5, available at http://www.regjeringen.no/nb/dep/jd/dok/nouer/1997/nou-1997-19/6.html?id=140976 (last accessed 31 October 2012).
[302] *Datalagring vedtatt etter maratondebatt i stortinget*, Aftenposten, 4 April 2011, available at http://www.aftenposten.no/nyheter/iriks/Datalagring-vedtatt-etter-maratondebatt-i-Stortinget-5115213.html (last accessed 31 October 2012).

personal privacy.[303] Supporters of the DLD argued that article 8.2 in ECHR provided the necessary clarifications for the DLD to be sanctioned. The Data Inspectorate and others pointed out that *collection* of information (ECHR 8.2), and *storage* of the same, as the DLD requires, are two different issues, but the DLD was nonetheless adopted.[304]

The second and related point in the public debate was how, for how long, and by whom data is to be stored. The National Criminal Investigation Service (KRIPOS), the *Politiets fellesforbund, Norsk Narkotikapolitiforening* (Police Union) supported a centralised database for storage.[305] Telenor, Netcom ('ecom providers'), *IKT-Norge* (Interest organisation for information technology) and the Norwegian Board of Technology were opposed to a centralised database, favouring smaller localised databases run by providers. Their concerns related to 'leaking' of information, for easier misuse of information, or that new purposes for legitimate use of the information might be introduced later with unforeseen consequences.[306] Prop. 49 L (2010-2011)[307], adopted by the Parliament, and effectuating the DLD, makes the providers responsible for localised storage and for finding technical solutions to securely store required information. Norwegian society was deeply split in their opinions on the DLD. Of those heard in the public hearing, these central institutions/organisations supported the implementation: The Norwegian Labour party; the Conservative party of Norway; KRIPOS; The Academics (trade union); Finance Norway (interest organisation for financial institutions); Stine Sofies Stiftelse (interest organisation fighting violence against children), and VG (Main tabloid paper). Central institutions/organisations against the implementation included: All the other political parties, all youth wings of the parties (including those of Labour, the Conservatives and the pro-EU movement). *Nei til EU* (Interest org against Norwegian participation in EU), *Norsk Pressforbund, Norsk redaktørforening, Norsk journalistlag* (trade unions for media employees), LO, YS (major trade unions), *Advokatforeningen* (Lawyers/Solicitors' union), *Barneombudet* (Ombudsman for children). Major newspapers: *Aftenposten, Adresseavisen, Bergens Tidene, Stavanger Aftenblad*.[308]

Implementation of the directive originally planned for 1 April 2012, was delayed with no new firm date confirmed. The delay is due to difficulties placing/distributing the costs. A 'høring' (public hearing) on the legal amendments required for the cost-models was due to be initiated summer 2012.[309]

4.4 CASE LAW EXAMPLES

In the offline world, governments generally need a judicial warrant to implant a wire-tap, and this is also the case for a physical search of property. In the online world, most "traffic" data –

[303] Transport og kommunikasjons kommiteen, *Innst. 275 L (2010–2011)*, Norway, 30.03.2011, p. 2, available at http://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2010-2011/inns-201011-275/?lvl=0 (last accessed 31 October 2012).
[304] Justis og beredskapsdepartementet, *Changes in the ekom act, criminal procedure act mv.* (implementing the EU DLD in Norwegian law), Prop. 49L 2010-2011, Norway, 10 December 2010, p. 14, available at http://www.regjeringen.no/nb/dep/jd/dok/regpubl/prop/2010-2011/prop-49-l-20102011.html?id=627826 (last accessed 31 October 2012).
[305] *Ibid*., p. 86-87.
[306] *Ibid*., p. 113.
[307] *Ibid*.
[308] The list is not exhaustive; it is a selection of key organisations/institutions in key sectors of the Norwegian society. Full list available at *Ibid*., p. 11.
[309] Samferdselsdepartementet Brev, *Høring om kostnadsdelingsmodeller for datalagringsdirektivet*, Norway, 21 March 2012. Available at: http://www.regjeringen.no/upload/SD/Hoeringsbrev_DLD.pdf

concerning who called or e-mailed whom, or visited what website, though not the content of a communication – is handed over without any such judicial authorisation. This is an issue of great concern as European states often find reasons to override their citizens' privacy. The EU's Data Retention Directive[310] – discussed in Chapter 7 of IRISS D.2.2 – requires telecoms firms to store vast amounts of data about their customers' activities, which may then be provided to law enforcement agencies. For example, in the UK, a 2012 draft Communications Data Bill, if enacted, would give intelligence agencies even wider powers to intercept and store such data.[311]

On the other hand, there has been a legal response to these and other challenges. Mass surveillance forces the redefinition of national fundamental rights, legal responses to unconstitutional practices, and the development of new rights. On a national level, some court rulings have developed important changes in order to maintain the balance between surveillance and privacy.

In the following examples, these will illustrate how some legal systems have reacted to problems arising in the information society that result in threats to fundamental rights and freedoms of citizens. In particular, the following discussion focuses on case law and presents some relevant decisions and the reasoning of national courts in cases relating to surveillance. The analysis will point out that the information status of citizens is determined not only by the scope and enforceability of their informational rights, such as data protection and freedom of information, but also by the whole range of their freedoms. National cases on data retention; online surveillance and wiretapping will be presented. A detailed analysis of data retention as a policy-making tool can be found in Chapter 7 of IRISS D.2.2.

4.4.1 Bulgaria: data retention

On 11 December 2008, the Bulgarian Supreme Administrative Court (SAC) annulled Article 5 of the national legislation that implements the Data Retention Directive, following a lawsuit initiated by Access to Information Program (AIP).[312] Article 5 of the Bulgarian Regulation that was issued by the State Agency on Information Technologies and Communication and the Ministry of Interior provided for a "passive access through a computer terminal" by the Ministry of Interior, as well as access without court permission by security services and other law enforcement bodies, to all retained data by Internet and mobile communication providers. The SAC annulled this article because the provision did not set any limitations with regard to data access by a computer terminal, and did not provide any guarantees for the protection of the right to privacy stipulated by Article 32 of the Bulgarian Constitution. No mechanism was established for respect of the constitutionally granted right of protection against unlawful interference in one's private or family affairs and against encroachments on one's honour, dignity and reputation. Moreover, the court also found that the text of Article 5 providing that the investigative bodies, prosecutor's office and the court shall be granted access to retained

[310] *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*, L 105/54, 13.4.2006.

[311] Draft Communications Data Bill. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty. June, 2012, available at http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf (last accessed 31 October 2012).

[312] Markovski, Veni, "Bulgarian Court Annuls A Vague Article Of The Data Retention Law", Digital Civil Rights in Europe, European Digital Rights (EDRI), 17 December 2008, available at http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention (last accessed 31 October 2012).

data "for the needs of the criminal process", and the security services "for the needs of the national security", does not provide limits against violations of constitutionally granted rights. Furthermore, the court held that Article 5 contradicts the provision of Article 8 of the ECHR. The court emphasised that national legal norms must comply with the established principle and must introduce comprehensible and well-formulated grounds for both access to the personal data of citizens and the procedures for their retention.

4.4.2 Ireland: data retention

On 10 February 2009, the Grand Chamber of the European Court of Justice (ECJ) ruled in *Ireland v. Parliament and Council* (Case C-301/06), that the Data Retention Directive had been correctly adopted on the basis of the first pillar (European Community – EC Treaty), as it relates predominantly to the functioning of the internal market.[313] Ireland sought annulment of the Directive on the ground that it should have been based on the EU's third pillar (relating to police and judicial co-operation in criminal matters) and was therefore not founded on the appropriate legal basis.

4.4.3 Romania: data retention

On 9 October 2009, the Romanian Constitutional Court (CCR) pronounced against data retention law.[314] The motivation of the court shows an interesting argument, coming from a court with no prior jurisprudence in the field of privacy protection. Thus, the court not only criticised several aspects of the legal text, but declared the whole law unconstitutional because it breaches the right to the privacy of correspondence. Even though only several articles were mentioned in the motion of unconstitutionality, the Court went further and examined Article 20 of the law, which could have been interpreted as an open door for the secret services to access retained data under any circumstances and without judicial approval. This issue had been raised by EDRi-member APTI starting with public consultations in 2007. The CCR noted that the principle of limited collection of personal data is emptied through this new regulation that obliges continuous retention of traffic data for at least 6 months. The court said that retention turned the exception from the principle of effective protection of the rights of privacy and freedom of expression into an absolute rule: "The right appears as being regulated in a negative manner, its positive role losing its prevailing character". The court underlining the point – already made by European civil-society organisations during the adoption of the Directive, that the law considers all citizens as potential criminals "regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform *a priori* all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes".

[313] Burton, Cédric, Christopher Kuner, Jörg Hladjk and Olivier Proust, "ECJ: Data Retention Directive has appropriate legal basis", *Lexology*, 16 March 2009, available at http://www.lexology.com/library/detail.aspx?g=aa3e4fbf-826a-416b-9c34-cbf631d27801 (last accessed 31 October 2012).

[314] European Digital Rights (EDRI), "Romanian Constitutional Court Decision Against Data Retention. Digital Rights", Digital Civil Rights in Europe, 2 December 2009, available at http://www.edri.org/edrigram/number7.23/romania-decision-data-retention (last accessed 31 October 2012).

4.4.4 Germany: online surveillance

On 27 February 2008, the German Federal Constitutional Court (*Bundesverfassungsgericht*) annulled provisions of the North Rhine-Westphalian Act on the Protection of the Constitution, which allowed the government to conduct online surveillance of personal computers.[315] The court ruled that the provisions were unconstitutional as they did not sufficiently respect the individual's right to confidentiality of data stored on IT systems and the integrity of these systems themselves. The new right could be termed the "IT Privacy" right. The court held that the right to confidential communication as granted by Article 10 of the German Constitution (*Grundgesetz*) also applies to online communications such as e-mail. In addition, the court found that accessing data on IT systems constituted an invasion of an individual's privacy as protected by Articles 1 and 2 of the *Grundgesetz*. The Court therefore decided that unjustified online surveillance violated the right to a "guarantee of confidentiality and integrity of information technology systems", which the court considered to be part of the fundamental right to privacy. The legitimate grounds for justification need to be defined by the legislator. However, the court put high demands in this respect: it ruled that, to be justified, there would have to be factual evidence indicating a specific threat to an outstanding and overriding legal interest such as threats to the life or freedom of an individual, or threats concerning the fundamentals or existence of the state. Additionally, to ensure that fundamental rights are protected, any and all online surveillance can only be conducted upon a judge's prior authorisation.

4.4.5 Spain: wiretapping

In Spain, there have been several scandals over illegal wiretapping by the intelligence services. In 2004, the National Police Corps and the Civil Guard reportedly started using a new software programme, SINTEL, that enabled them to tap directly into telephonic communications without the need to get prior court authorisation.[316] In addition to recording the content of the communication, the software also provided the identity of both callers and the places from which they are calling. SINTEL has generated a controversial debate about the necessity of some of the tools used to fight crime in Spain while defending citizens' fundamental rights. The Spanish Internet Users Association filed a motion before the court of the National Audience in order to assess whether the police may get access to the SINTEL database of personal data without a judge's consent and without sufficient evidence of wrongdoing. The motion was rejected.

[315] Bird & Bird, "German Constitutional Court creates a new fundamental 'IT Privacy' Right", 9 September 2008, http://www.twobirds.com/English/News/Articles/Pages/German_Constitutional_Court_creates_a_new_fundamental_IT_Privacy_Right.Aspx (last accessed 31 October 2012).

[316] Privacy International, "CHAPTER: II. Surveillance policies. National security, government surveillance and law enforcement", 1 January 2011, available at https://www.privacyinternational.org/reports/spain (last accessed 31 October 2012).

5. CONCLUSIONS

This Deliverable discusses the legal framework which applies to surveillance, while raising key issues on the regulation of surveillance. It highlighted the limits of legislation and case law in defining a clear set of norms and principles for regulating surveillance. As explained above, surveillance and its regulation are highly influenced by political and social variables that can be only partially explained through legal reasoning. Nevertheless, it is imperative to take these other aspects into account and so to consider IRISS D.2.1 (the social perspective), D.2.2 (the political perspective) and D.2.3 (the legal perspective) in a systematic way. Similarly, the discourse about forms of resilience to surveillance in today's societies needs to consider these three perspectives.

There is not a clear set of legal norms that regulate surveillance at European and national level. Privacy and data protection provide significant safeguards for regulating surveillance through specific norms and principles such as lawfulness, necessity, proportionality and consent. However, gaps and pitfalls can be found in legislation on privacy and data protection with regards to surveillance and case law contributes to fill these gaps only partially. It is unclear for example, which surveillance measures can be considered as 'necessary in a democratic society'. Similarly, the meaning of the expression 'a person's reasonable expectation of privacy' is not apparent in European legislation and case law. Nevertheless, the legal framework that relates to the regulation of a certain surveillance practice depends also on the capability of legislation and case law to accommodate developments in surveillance technologies, which represents a challenge in itself given that legislation has as a side-effect, the fact of being anachronistic when dealing with new technologies.

Surveillance can affect the exercise of fundamental rights in democratic settings. It can challenge democracy and be non-democratic. Tensions between surveillance and democracy result from the effects and impacts of the former on fundamental rights. Indeed, the ECtHR recognises that surveillance can undermine or even destroy democracy on the grounds of defending it. However, the governance of surveillance often consists of balancing conflicting rights and interests, whose task is usually performed by Courts, on a case-by-case basis. In turn, this case-by-case approach generates concerns as regards the enforcement of fundamental rights and democracy.

There is unanimous consensus on the fact that surveillance practices such as the interception of communications, wiretapping, bugging of apartments, recording of voices, disclosure to the media of footage filmed in a street by CCTV, monitoring of emails and GPS monitoring may result in illegal practices. However, there are remarkable differences in the way legislation regulates specific surveillance practices. If we look at wiretapping for example, we notice that it is better regulated and its provisions are more detailed than in the case of GPS monitoring. On the other hand, if we turn to case law, we see that is provides additional guarantees to counter possible infringements. However, as explained above, the ECtHR tends also to distinguish between hard surveillance (such as wiretapping) and soft surveillance (such as GPS monitoring) and requires a higher-intensity legal safeguards in the first case than in the second one.

Finally, although an almost equivalent level of constitutional protection of freedoms against excessive surveillance powers can be found at national level, remarkable differences exist across Europe. There are different privacy cultures and differences as to how different legal systems consider and regulate surveillance. These differences are rooted in the constitutional

traditions of European Member States and the European legislator should take them into account when regulating surveillance.

6. REFERENCES

Agencia Española de Protección de Datos (AEPD), *Guía del derecho fundamental a la protección de datos de carácter personal*, 2004, available at http://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf (last accessed 31 October 2012).

Alexander, Larry, "The Moral Magic of Consent", *Legal Theory*, Vol. II, 1996.

Amicelle, Anthony, "The Great (Data) Bank Robbery: The Terrorist Finance Tracking Program & the SWIFT Affair", *Research Questions*, CERI, No. 36, May 2011.

Amoore, Louise, and Marieke De Goede, "Introduction. Data and the war by other means", *Journal of Cultural Economy*, Vol. 5, No. 1, February 2012.

Ann Florini (ed.), *The Right to Know. Transparency for an Open World*, Columbia University Press, 2007.

Anyton-Schenker, Diana, *The Challenge of Human Rights and Cultural Diversity*, UN Background Note, United Nations Department of Public Information, DPI/1627/HR-March, 1995, available at http://www.un.org/rights/dpi1627e.htm (last accessed 31 October 2012).

Aolain, Fionnuala, Emergence of Diversity: Differences in Human Rights Jurisprudence, *19 Fordham Int'l L.J.*, 1995-1996.

Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Intersentia, 2001.

Bakircioglu, Onder, The Application of the Margin of Appreciation Doctrine in Freedom of Expression and Public Morality Cases, *8 German L.J.*, 2007.

Ball, Kirstie Kevin Haggerty and David Lyon (eds.), *The International Handbook of Surveillance Studies*, Routledge, London, 2012.

Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky, *Discrimination and privacy in the information society. Data mining and profiling in large databases*, Springer, Heidelberg, 2012.

Bellanova, Rocco, and Michael Friedewald (eds.), Deliverable 1.1: "Smart Surveillance – State of the Art", *SAPIENT project*, Brussels, 2012.

Bennett, Colin J. and Charles Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, Ashgate, Burlington, 2003.

Bennett, Colin J., *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Victoria, British Columbia, 1992.

Benvenisti, Eyal, "Margin of Appreciation, Consensus, and Universal Standards". *N.Y.U. J. Int'l L. & Pol.*, Vol. 31, 1998-1999.

Bird & Bird, "German Constitutional Court creates a new fundamental 'IT Privacy' Right", 9 September 2008, http://www.twobirds.com/English/News/Articles/Pages/German_Constitutional_Court_creates_a_new_fundamental_IT_Privacy_Right.Aspx (last accessed 31 October 2012).

Black, Edwin, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, Crown Publishing, New York, 2001.

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*, Berlin, Springer, 2012.

Brown, Felicity, "Rethinking the Role of Surveillance Studies in the Critical Political Economy of Communication", IAMCR Prize in Memory of Dallas W. Smythe, 2006.

Burgess, J. Peter (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010.

Burton, Cédric, Christopher Kuner, Jörg Hladjk and Olivier Proust, "ECJ: Data Retention Directive has appropriate legal basis", *Lexology*, 16 March 2009, available at http://www.lexology.com/library/detail.aspx?g=aa3e4fbf-826a-416b-9c34-cbf631d27801 (last accessed 31 October 2012).

Bus, Jacques, Malcolm Crompton, Mireille Hildebrandt and George Metakides (eds.), *Digital Enlightenment Yearbook 2012*, Amsterdam, IOS Press, 2012.

Clarke, Roger, *Introduction to Dataveillance and information privacy, and definition of terms*, 2006, http://www.rogerclarke.com/DV/Intro.html (last accessed 31 October 2012).

Collins, Val, "Privacy in the United Kingdom: a Right Conferred by Europe?" *Int'l J.L. & Info. Tech.*, Vol. 1, 1993-1994.

Council of Europe, Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series, No. 108 (1981), *International Legal Materials*.

Council of Europe, European Commission for Democracy through Law (Venice Commission), *Opinion on Video Surveillance in Public Spaces by Public Authorities and the Protection of Human Rights*, 70th Plenary Session, 16-17 March 2007.

Dandeker, Christopher, *Surveillance, Power and Modernity*, Polity Press, Cambridge, 1990.

De Hert, Paul, "De wet van 30 juni 1994 en het afluisteren. Een sociaalrechtelijke toets" [Implications of the Belgian Tapping Act for Workplace activities], *Oriëntatie*, No. 4, April 1995.

Dennis, Mike, and Peter Brown, *Stasi: Myth and Reality*, Pearson Education, Longman, Harlow, 2003.

Dirix, Eric & Yves-Henri Leleu (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Bruylant, Brussels, 2011.

Dixon, John, Mark Levine and Rob McAuley, *Street Drinking Legislation, CCTV and public space: exploring attitudes towards public order measures*, Home Office Report, London, 2003.

Donnelly, Jack, *Universal Human Rights in Theory & and Practise*, Cornell University, 2003.

Dunnage, Jonathan, "Policing Right-Wing Dictatorships: Some preliminary comparisons of Fascist Italy, Nazi Germany and Franco's Spain", *Crime, History & Societies*, Vol. 10, No. 1, January 2006.

Dunnage, Jonathan, "Surveillance and Denunciation in Fascist Siena, 1927-1943", *European History Quarterly*, No. 38, April 2008.

Emsley, Clive Eric Johnson and Pieter Spierenburg (eds.), *Social Control in Europe*. 1800-2000, Vol. 2, Ohio State University Press, Ohio State University, 2004.

Engel, Christoph and Kenneth H. Keller (eds.), *Governance of Global Networks in the Light of Differing Local Values*, Nomos, 2000.

Eriksson, Lars D. et al. (eds.), *Dialectic of Law and Reality: Readings in Finnish Legal Theory*, University of Helsinki, 1999.

European Digital Rights (EDRI), "Romanian Constitutional Court Decision Against Data Retention. Digital Rights", Digital Civil Rights in Europe, 2 December 2009, available at http://www.edri.org/edrigram/number7.23/romania-decision-data-retention (last accessed 31 October 2012).

Flaherty, David, H., *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada & the United States*, Chapel Hill, The University of North Carolina Press, 1989.

Fonio, Chiara., "Surveillance under Mussolini's regime", *Surveillance & Society*, Vol. 9, No. 1/2, May 2011.

Franko Aas, Katja, Helene Oppen Gundhus, Heidi Mork Lomell (eds.), *Technologies of Insecurity. The Surveillance of Everyday Life*, Routledge-Cavendish, New York, 2009.

Funder, Anna, *Stasiland*, Granta, London, 2004.

Franzinelli, Mimmo, *I tentacoli dell'Ovra*, Bollati e Boringhieri, Torino, 1999.

Friedewald Michael, Van Lieshout M, Wright David and Gutwirth Serge, "Reconciling privacy and security". *Innovation. The European Journal of Social Science Research*, 2013, pp. 1-14.

Galdon Clavell, G. "Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia", *Information Polity*, 16(4), 2011.

Galdon Clavell, Gemma, "La videovigilancia va en Ómnibus", *Público,* Madrid, 2010, available at http://blogs.publico.es/civismos-incivicos/2010/07/06/la-videovigilancia-va-en-omnibus/ (last accessed 31 October 2012).

Galdon Clavell, Gemma, Zuloaga, L. and Romero, A., "CCTV in Spain: an empirical account of the deployment of video-surveillance in a Southern-European country", *Information Polity*, 17(1), 2012.

Garland, David, *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford University Press, Oxford, 2001.

Gavison, Ruth, "Privacy and the Limits of the Law", *Yale Law Journal*, Vol. 89, 1980.

Giddens, Anthony, "A Contemporary Critique of Historical Materialism", Vol.1: *Power, property and the state*, University of California Press, Berkeley, 1981.

Glenn, H. Patrick, "A Concept of Legal Tradition", *Queen's L. J*., Vol. 34, 2008-2009.

Glenn, H. Patrick, *Legal Tradition of the Worlds: Sustainable Diversity in Law*, Oxford, 2007, Goldman, 2008.

Goldman, David B., *Globalisation and the Western Legal Tradition*, *Recurring Patterns of Law and Authority,* Cambridge University Press, 2008.

Goldman, Lisa "Spain's Draft Law on Transparency and Access to Information Disappoints Civil Society NGOs", *Techpresident*, 15 August 2012, available at http://techpresident.com/news/wegov/22724/spains-draft-law-transparency-and-access-information-disappoints-civil-society-ngos (last accessed 31 October 2012).

González Fuster, Gloria and Raphaël Gellert, "The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right", *International Review of Law, Computers & Technology*, Vol. 26, No. 1, 2012.

Goold, Benjamin J., "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009.

Graham, S. *Cities under siege*. London, Verso, 2010.

Gras, Marianne L., "The legal regulation of CCTV in Europe", *Surveillance & Society*, Vol. 2, No. 3, 2004.

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

Haggerty, Kevin and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, New York, 2010.

Hale, Chris, Keith Hayward, Azrini Wahidin and Emma Wincup, *Criminology 2nd Edition*, Oxford University Press, Oxford, 2009.

Hear, Sean P. and Greenberg, Josh (ed.) *The Surveillance Studies Reader*, Open University Press, 2009,

House of Lords, *Surveillance: Citizens and the State*, Select Committee on the Constitution, 2nd report of Session 2008-09, London, 2009.

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdfhttp://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (last accessed 15 October 2012).

Jacobs, Bart, "Keeping our surveillance society non-totalitarian", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009.

Jarausch, Konrad, "Au-delà des condamnations morales et des fausses explications. Plaidoyer pour une histoire différenciée de la RDA", *Genèses*, Vol. 3, No. 52, Septembre 2003.

Koehler, John O., *Stasi: The Untold Story of the East German Secret Police*, Westview Press, Boulder CO, 1999.

Kuner, Christopher, *European Data Protection Law. Corporate Compliance and Regulation*, Oxford University Press, Brussels, 2007.

Leenes, Ronald, Bert-Jaap Koops and Paul De Hert (eds.), *Constitutional Rights and New Technologies*, T.M.C. Asser Press, The Hague, 2008.

Lilly, J. Robert and Joan Himan, *The Electronic Monitoring of Offenders: Symposium Papers, Second Series.* De Montfort University Law School Monographs, Leicester, 1993.

Lindenberger, Thomas, "Secret et public: société et polices dans l'historiographie de la RDA", *Genèses*, Vol. 3, No. 52, Septembre 2003.

Lopez-Rodriguez, Ana M, "Towards a European Civil Code Without a Common European Legal Culture? The Link Between Law, Language and Culture", *Brook J. Int'l L,* Vol. 29, 2003-2004.

Lyon, David (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London, 2005.

Lyon, David, "Airport screening, surveillance and social sorting: Canadian responses to 9/11 in context", *Canadian Journal of Criminology and Criminal Justice*, Vol. 48, Issue 3,

Lyon, David, *Surveillance Society: Monitoring Everyday Life*, Buckingham, Open University Press, 2001.

Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007.

Lyon, David, *Terrorism and Surveillance: Security, Freedom and Justice after September 11 2001*, Paper given at the Privacy Lecture Series <http://privacy.openflows.org> on November 12, 2001, available at http://privacy.openflows.org/pdf/lyon_paper.pdf (last accessed 31 October 2012).

Lyon, David (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Willan, Cullompton UK, 2006.

Lyon, David, *Terrorism and Surveillance: Security, Freedom and Justice after September 11 2001*, Paper given at the Privacy Lecture Series <http://privacy.openflows.org> on November 12, 2001, available at http://privacy.openflows.org/pdf/lyon_paper.pdf

Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, Polity Press, Cambridge, 1994.

Majtenyi, Laszlo (ed.), *The Door Onto the Other Side: A report on information rights*, Office of the Parliamentary Commissioner for Data Protection and Freedom of Information, Budapest, 2001 [bilingual edition].

Markovski, Veni, "Bulgarian Court Annuls A Vague Article Of The Data Retention Law", Digital Civil Rights in Europe, European Digital Rights (EDRI), 17 December 2008, available at http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention (last accessed 31 October 2012).

Marryman, John and Perez Perdomo Rogelio: *The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America*, Stanford University Press, 2007.

Marx, Gary T., *Undercover: Police Surveillance in America*, University of California Press, Berkeley, 1988.

Masterman, Roger, *The Separation of Powers in the Contemporary Constitution, Judicial Competence and Independence in the United Kingdom*, Cambridge, 2011.
Mattelart, Armand, *The Globalization of Surveillance,* Polity Press, 2007.
Max Weber, *Oeuvres politiques*, Paris, Albin Michel, 2004.
McCahill, Michael and Clive Norris, "On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts", *Working Paper No. 3 CCTV in Britain,* RTD-Project (September 2001 – February 2004) 5th Framework Programme of the European Commission, Contract No.: HPSE-CT2001-00094, 2002.
McCahill, Michael and Clive Norris. *CCTV in Britain*, Urbaneye Working Paper no. 3, Berlin, Centre for technology and Society, Technical University of Berlin, 2002.
McCulloch, Jude and Sharon Pickering, "Pre-Crime and Counter-Terrorism: Imagining Future Crime in the 'War on Terror'", *British Journal of Criminology,* Vol. 49, Issue 5, 2009.
Miller, Barbara, *Narratives of Guilt and Compliance in Unified Germany: Stasi Informers and Their Impact on Society*, Routledge, London, 2000.
Mink, Andras, *The Defendant: the State. The Story of the Hungarian Helsinki Committee,* Hungarian Helsinki Committee, Budapest, 2005.
Murakami Wood, D., Ball, K., Lyon, D., Norris, C. and Raab, C. 'A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network'. 2006.
Murakami Wood, David, "The Surveillance Society: Questions of History, Place and Culture", *European Journal of Criminology,* Vol.6, Issue 2, 2009.
Nellis, Mike, "Out of this World: The Advent of the Satellite Tracking of Offenders in England and Wales", *The Howard Journal,* Vol. 44, Issue 2, 2005.
Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010.
Norris, Clive and Gary Armstrong, *The maximum surveillance society: The rise of CCTV,* Berg, Oxford (England), 1999.
Nouwt, Sjaak, Berend R. De Vries and Corien Prins (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, The Hague, 2005.
OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 9-12, 1980 (1981) *International Legal Materials*, I., 317.
Orwell, George, *1984*, Penguin Modern Classics, London, 2004.
Perrin, Nathalie, "Practical Measures for Reducing Irregular Migration in Belgium", Report for the European Migration Network (EMN) Belgium National Contact Point, Brussels, 2012.
Poppe, Ulrike, "Que lisons-nous lorsque nous lisons un dossier personnel de la Stasi", *Genèses*, Vol. 3, No. 52, September 2003.
Privacy International, "CHAPTER: II. Surveillance policies. National security, government surveillance and law enforcement", 1 January 2011, available at https://www.privacyinternational.org/reports/spain (last accessed 31 October 2012).
Raab, Charles and Benjamin Goold, *Protecting Information Privacy*, Research Report 69, Equality and Human Rights Commission, London, 2011.
Rachels, James, "Why privacy is important", *Philosophy and Public Affairs*, Vol. 4, No. 4, 1975.
Rössler, Beate, *The Value of Privacy* (translated by R .D. V. Glasgow), Cambridge, Polity Press, 2005.

Rule, James B., and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation,* Edward Elgar Publishing Ltd., November 2008.
Shute, Stephen, *Satellite Tracking of Offenders: A Study of the Pilots in England and Wales (Research Summary 4),* Ministry of Justice, London, 2007.
The Eötvös Károly Institute (EKINT), *Hungarian NGOs assess the new Constitution of Hu*ngary, http://www.ekint.org/ekint/ekint_angol.news.page?nodeid=454 (last accessed 31 October 2012).
The Eötvös Károly Policy Institute, *Analysis on the Constitutional Changes in Hungary,* http://alaptorveny.eu (last accessed 31 October 2012).
The Eötvös Károly Policy Institute, *Letter on the Independence of the Data Protection Authority,* http://alaptorveny.eu, also available at http://www.ekint.org/ekint_files/File/barroso_dpa_independence_20111106_printed.pdf (last accessed 31 October 2012).
Tugendhat, Michael and Christie Iain (eds.), *The Law of Privacy and the Media,* Oxford, Oxford University Press, 2002.
Vermeulen, Mathias, Rocco Bellanova and Serge Gutwirth "A fundamental rights analysis of smart surveillance", *SAPIENT project,* D. 1.1, January 2012.
Warren, Samuel and Louis Brandeis, "The Right to Privacy", Harvard Law Review, Vol. 4, No. 5, 15 December 1980.
Weber, Max, *Economie et Société,* Paris, Agora, 2003.
Webster, William, "CCTV policy in the UK: reconsidering the evidence base", *Surveillance & Society,* Vol. 6, Issue 1, 2009.
Westin, Alan F., *Privacy and Freedom,* New York, Atheneum, 1967.
Wood, David, "Editorial. People Watching People", *Surveillance & Society,* Vol. 2, No. 4, April 2005.
Yesil, Bilge, "Watching ourselves: Video surveillance, urban space, and self responsibilization", *Cultural Studies,* 2006.
Yourow, Howard C, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence,* Martinus Nijhoff Publisher, 1996.
Zedner, Lucia, "Pre-Crime and Post-Criminology?", *Theoretical Criminology,* Vol. 11. 2007.
Zureik, Elia, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan (eds.), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons,* McGill-Queen's University Press, Montreal & Kingston, London, Ithaca, 2010.

List of cases – European Court of Human Rights (ECtHR)

ECtHR, *Armstrong v. the United Kingdom*, application no. 48521/99, judgement of 16 July 2002.
ECtHR, *Biriuk v. Lithuania*, application n. 23373/03, judgement of 25 November 2008.
ECtHR, *Chalkley v. the United Kingdom*, application no. 63831/00, judgement of 12 June 2003.
ECtHR, *Copland v. the United Kingdom*, application no. 62617/00, judgement of 3 April 2007.
ECtHR, *Friedl v. Austria*, application No. 15225/89, judgement of 31 January 1995.
ECtHR, *Funke v. France*, application no. 10828/84, judgement of 23 February 1993.
ECtHR, *Halford v. the United Kingdom*, application no. 20605/92, judgement of 25 June 1997.
ECtHR, *Hewitson v. the United Kingdom*, application no. 50015/99, judgement of 27 May 2003.
ECtHR, *Huvig v. France*, application no. 11105/84, judgement of 24 April 1990.
ECtHR, *I. v. Finland*, application n. 20511/03 of 17 July 2008, para 38 and *C.C. v. Spain*, application n. 1425/06, judgement of 6 October 2009.
ECtHR, *Khan v. the United Kingdom*, application no. 35394/97, judgement of 12 May 2000.
ECtHR, *Khan v. the United Kingdom*, application no. 35394/97, judgement of 12 May 2000.
ECtHR, *Klass v. Germany*, application no. 15473/89, judgment of 6 September 1978.
ECtHR, *Kopp v. Switzerland*, application no. 23224/94, judgement of 25 March 1998.
ECtHR, *Kruslin v. France*, application no. 11801/85, judgement of 24 April 1990.
ECtHR, *L.L. v. France*, application n. 7508/02, judgement of 10 October 2006.
ECtHR, *Leander v. Sweden*, application No. 9248/81, judgement of 26 March 1987.
ECtHR, *Liberty and other organisations v. the United Kingdom*, application no. 58234/00, judgement of 1 July 2008.
ECtHR, *Loizidou v.Turkey*, application no. 15318/89 judgement of 23 March 1995.
ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, judgement of 2 August 1984.
ECtHR, *Mamatkulov and Askarov v. Turkey*, application no. 46827/99 and 46951/99, judgement of 4 February 2005.
ECtHR, *Niemietz v. Germany*, application no. 13710/88, judgement of 16 December 1992.
ECtHR, *P.G. and J.H. v. United Kingdom*, application no. 44787/98, judgement of 25 September 2001.
ECtHR, *Peck v. United Kingdom*, application no. 44647/98, judgement of 28 January 2003.
ECtHR, *Perry v. the United Kingom*, application no. 63737/00, judgement of 17 July 2003.
ECtHR, *Pretty v. United Kingdom*, application no. 2346/02, judgement of 29 April 2002.
ECtHR, *Rotaru v. Romania*, application no. 28341/95, judgement of 4 May 2000.
ECtHR, *S. and Marper v. the United Kingdom*, application n. 30562/04 and 30566/04 judgement of 4 December 2008.
ECtHR, *Silver and Others v. the United Kingdom*, judgement of 25 March 1983.
ECtHR, *Taylor-Sabori v. the United Kingdom*, application no. 47114/99, judgement of 22 October 2002.
ECtHR, *Tyrer v. the United Kingdom*, application no. 5856/75 judgement of 25 April 1978.
ECtHR, *Uzun v. Germany*, application no. 35623/05, judgement of 2 September 2010.
ECtHR, *Valenzuela Contreras v. Spain*, application no. 27671/95, judgement of 30 July 1998.
ECtHR, *Van Kück v. Germany*, application no. 35968/97, judgement of 12 June 2003.
ECtHR, *Weber and Saravia v. Germany*, application no. 54934/00 admissibility decision, para 93 of 29 June 2006.
ECtHR, *Z. v. Finland*, application no. 22009/93, judgement of 25 February 1997.

List of cases – European Court of Justice (ECJ)

ECJ, *B. v. France*, C-13343/87, judgement of 25 March 1992.
ECJ, C-101/01, *Bodil Lindqvist*, judgement of 6 November 2003, para 40. Joined Cases C-465/00, C-138/01.
ECJ, C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge and Republik Österreich*, judgement of 12 June 2003,
ECJ, C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgement of 20 May 2003.
ECJ, C-262/06, *Deutsche Telekom AG v. Bundesrepublik Deutschland,* judgement of 22 November 2007.
ECJ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU,* judgement of 29 January 2008.
ECJ, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, judgement of 7 May 2009.
ECJ, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GBR and Hartmut Eifert v. Land Hessen*, judgement of 9 November 2010.
ECJ, *Keegan v. Ireland*, C-16969/90, judgement of 26 May 1994.
ECJ, *Mikulic v. Croatia*, C-53176/99, judgement of 7 February 2002.
ECJ, *Van Kück v. Germany*, judgement of 12 June 2003.