European University Institute

DEPARTMENT OF LAW

EUI WORKING PAPERS

LAW 2015/41
Department of Law
SURVEILLE
Surveillance: Ethical Issues, Legal Limitations, and Efficiency

The Use of Surveillance Technologies for the Prevention, Investigation and Prosecution of Serious Crime

Céline C. Cocq and Francesca Galli

SURVEILLE

Funded by the European Union

European University Institute
Department of Law
SURVEILLE
Surveillance: Ethical Issues, Legal Limitations, and Efficiency

THE USE OF SURVEILLANCE TECHNOLOGIES FOR THE PREVENTION, INVESTIGATION AND PROSECUTION OF SERIOUS CRIME

Céline C. Cocq and Francesca Galli

EUI Working Paper **LAW** 2015/41
SURVEILLE Project
Surveillance: Ethical Issues, Legal Limitations, and Efficiency

ISSN 1725-6739

Printed in Italy
European University Institute
Badia Fiesolana
I-50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Foreword

This EUI Working Paper is based on research conducted in 2012-2015 in the FP7 project SURVEILLE. The research has earlier been reported to the European Commission in the form of what in that context is called project deliverables. Most of the deliverables have also been published on the website of the project. In order better to reach academic audiences in Europe and beyond, the EUI Law Department decided to publish selected SURVEILLE research reports also in the form of Working Papers. The current paper is one in that series.

SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency) was a multidisciplinary project that developed a new methodology for the assessment of surveillance technologies. This methodology seeks to enable a more rational and structured process of decision-making concerning the use of surveillance technologies, as compared to abstract references to the need to find a "balance", for instance between privacy and security. The methodology developed in SURVEILLE is based on three parallel expert assessments of the use of any specific surveillance technology in a given context. The technology assessment incorporates issues of actual delivery towards a legitimate aim such as improved security, and issues of various types of financial cost. It results in a so-called usability score, based on ten different criteria. This score can be compared against a fundamental rights intrusion score that is based on expert assessments of the importance of a fundamental right (often the right to privacy or the right to the protection of personal data) in the situation at hand, and of the depth of the intrusion into that right as results from the surveillance. An independent ethics assessment will inform the holistic overall assessment and the comparison between the two scores, by indicating three different levels of moral hazard in the use of surveillance. The SURVEILLE methodology can assist legislators, policymakers, technology developers and end-users of surveillance technologies (such as the police or local authorities) in a process of rational, transparent and controlled decision-making over surveillance. The traditional legal requirements of legitimate aim, necessity and proportionality are all incorporated into the SURVEILLE methodology but in a manner that allows their operationalisation through the multidisciplinary approach of the three parallel assessments and an informed comparison of their outcomes.

In addition to developing the assessment methodology as just described, SURVEILLE generated multiple lines of academic research on technological, sociological, ethical and legal issues concerning surveillance. The current Working Paper emanates from that research.

In Florence, 30 September 2015

Martin Scheinin, Professor of International Law and Human Rights, EUI

SURVEILLE Consortium Leader

SURVEILLE - Surveillance: Ethical Issues, Legal Limitations, and Efficiency

The SURVEILLE project received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725, for the period 1 February 2012 to 30 June 2015.

Authors' Contact Details:

Céline C. Cocq

PhD Candidate

Centre de Droit Européen
Université Libre de Bruxelles

Email: Celine.Cocq@ulb.ac.be

Francesca Galli

Lecturer in EU Law

Department of International and European Law
University of Maastricht

Francesca.Galli@maastrichtuniversity.nl

General Introduction

This Working Paper is based on two research reports that were the outcome of the research carried out by the team of the *Université Libre de Bruxelles* within the FP7 project SURVEILLE.[1] Such research focused on the use of surveillance technologies for the prevention, investigation, and prosecution of serious crime. Taken together, the two reports developed a comparative analysis of a number of surveillance technologies and techniques used at different stages of the criminal procedure within selected national jurisdictions. The first project deliverable, finalised in October 2012 and entitled "The use of surveillance technologies for the prevention and investigation of serious crime" (D4.1)[2], addressed the use of the interception of telecommunications and video-surveillance in three countries, namely France, Italy and the United Kingdom. The second deliverable, finalised in April 2013 and entitled "Comparative law paper on data retention regulation on a sample of EU Member States" (D4.3), examined the rules governing the retention of data by telecommunications companies and internet service providers for criminal justice purposes in nine countries (*i.e.* Belgium, France, Germany, Italy, the Netherlands, Poland, Romania, Spain and the United Kingdom). The two reports test the existence of what the authors call a double shift: the means at the disposal of competent national authorities (intelligence services and law enforcement agencies) in the fight against serious crime are evolving in such a way that the share of tasks and competences is now increasingly blurred.

The fundamental rights dimension was the normative background of the legal dimensions of the SURVEILLE project as a whole, and thus also of the present work. The impact of evolving trends in the use of surveillance upon the right to privacy and the right to the protection of personal data are at the core of this research undertaking.

The authors wish to highlight that legislation is changing very quickly in this domain both at the national level and at the EU level. In particular, the January 2015 attacks in Paris against *Charlie Hebdo*, the February 2015 attacks in Copenhagen and the increasing threat resulting from the foreign fighters phenomenon are significantly challenging the effectiveness of means used by States to prevent, investigate, detect and prosecute terrorist offences. Recent legislative developments deepen the blur between the tasks and functions of intelligence services and law enforcement agencies as well as the blur between administrative and criminal law measures. Furthermore, with the ruling by the Court of Justice of the European Union on 8 April 2014 in the *Digital Rights Ireland* case[3] - partially reaffirmed in *Schrems*[4], EU Member States together with EU institutions have to rethink the legal framework concerning the use of surveillance technologies and techniques in order to ensure a coherent relationship between on the one hand safeguarding the right to privacy and the protection of personal data, and on the other hand developing effective means to prevent, investigate, detect and prosecute serious crime.[5]

---

[1] See all deliverables and events organised during the project on SURVEILLE's website : www.surveille.eui.eu.

[2] The research conducted for this paper has also resulted in an article: Céline Cocq and Francesca Galli, "The catalysing effect of serious crime on the use of surveillance technologies for prevention and investigation purposes", *N.J.E.C.L.*, vol.4, 2013/3.

[3] CJEU, *Digital Rights Ireland and Seitlinger and Others* case, C-293/12 and C-594/12, 8 April 2014.

[4] CJEU, Schrems v DPC, C-362/14, 6 October 2015; 'Safe Harbour ruling'.

[5] See *e.g.* Céline Cocq and Francesca Galli, "Data retention regime within the EU: Reinventing a common framework after the CJEU ruling?" *European Journal of Policing Studies* (forthcoming in 2015).

Despite the fact that the two papers were written at least two years ago, the information remains largely up to date. These papers analyse a trend that has been occurring for some years and that is not over yet: a massive use of surveillance technologies and techniques by an increasing number of competent authorities leading to an exponential gathering of information by EU Member States aiming to fight more effectively against serious crime - often at the expense of fundamental rights.

Keywords

Surveillance Technologies, Serious Crime, EU Comparative Criminal Law

Table of contents

PART 1.
THE USE OF SURVEILLANCE TECHNOLOGIES FOR THE PREVENTION AND INVESTIGATION OF SERIOUS CRIME

INTRODUCTION 1

THE EXPANSION OF DEROGATORY REGIMES TO COPE WITH SERIOUS CRIME 4

TOWARDS A GENERALISED USE OF SURVEILLANCE TECHNOLOGIES?
THE INTERCEPTION OF TELECOMMUNICATIONS 7

Post-delictum interceptions 9
Actors 9
Scope 10
Duration 11
Ante-delictum interceptions 13
Actors 13
Scope 14
Duration 15
Particular comments 17

FROM A PREVENTIVE PURPOSE TO AN INVESTIGATIVE USE: VIDEO-SURVEILLANCE 17

Actors 19
France 19
The United Kingdom 20
Italy 20
Scope 20
France 20
Italy 21
The United Kingdom 21
Duration 22
Duration of the installation 22
Duration of the retention of information gathered by video-surveillance 22

INTERPLAY BETWEEN INTELLIGENCE SERVICES AND LAW ENFORCEMENT AGENCIES:
MUTUAL CONTAMINATION 24

France 25
Italy 26
The United Kingdom 27

CONCLUDING REMARKS 27

PART 2.
COMPARATIVE LAW PAPER ON DATA RETENTION REGULATION IN A SAMPLE OF EU MEMBER STATES

INTRODUCTION 30

NATIONAL LEGISLATIVE CHANGES SINCE 2011 32

DATA RETENTION VS. DATA PRESERVATION 34

CONDITIONS OF DATA RETENTION AND ACCESS IN THE DIFFERENT STATES 35

Legal basis and purpose of data retention 36

New stakeholders 37

Duration of retention 37

Access to data: authorities and procedure 38

Scope of data retention and access 41

ROLE OF RETAINED DATA AS EVIDENCE IN THE CRIMINAL JUSTICE SYSTEM 42

Rules of evidence 43

Comparative approach between the selected Member States 43

The exclusion of evidence: irregularity and illegality 44

Role and competences of intelligence services and law enforcement within the criminal justice system 45

Procedure for intelligence to become evidence 45

Assessment of evidence: prosecution and trial 47

Retained data as evidence 47

Intelligence 47

IMPLICATIONS OF DATA RETENTION FOR FUNDAMENTAL RIGHTS 48

Protection of privacy vs. intrusiveness 48

European framework on privacy 48

National authorities and Data Protection Acts 49

Current issues under discussion within Member States selected 50

ASSESSMENT OF THE USE OF RETAINED DATA IN THE CRIMINAL JUSTICE SYSTEM 51

Influence of serious crimes in the use of data 51

Increasing use of intelligence in the criminal justice system 52

Interference of the private sector in the criminal justice system 54

POTENTIAL INFLUENCE OF AN AUTHORITARIAN PAST 55

CONCLUSION 56

Part 1. The use of surveillance technologies for the prevention and investigation of serious crime

Introduction

The years following 11 September 2001 with the 2004 bombings in Madrid, the 2005 attacks in London, the 2011 attacks in Norway and the 2012 attacks in Toulouse show profound changes in the terrorism threat and the emergence of the parallel phenomena of home-grown terrorism and lone-wolves terrorist actors.[6]

Such changes have had a tremendous impact on the criminal justice system as a whole leading to a progressive shift towards prevention in the fight against terrorism at the national as well as at the EU level.[7] The evolving terrorist threat has had most importantly a catalysing effect on: the enactment of new inchoate offences and the criminalisation of preparatory activities[8]; and, the development of anticipative/proactive criminal investigation.[9]

The deliverable focuses on one fundamental change within this second dimension, namely the increasing use of surveillance technologies in the fight against serious crime,[10] and especially against terrorism.[11] In fact, by contrast with the DETECTER Project[12], for which the scope of the research was limited to terrorism, the FP7 SURVEILLE project covers "serious crimes"[13], which includes terrorism.[14]

Thus, this paper is to be seen in the context of the SURVEILLE project, which offers a legal and ethical analysis of issues surrounding the use of surveillance technologies in three phases of countering serious crimes (prevention, investigation and prosecution) at the national as well as at the

---

[6] See EUROPOL, *EU Terrorism Situation and Trend Report (TE-SAT)* (2012); K.L. Thachuk and al., *Homegrown Terrorism. The Threat Within*, Center for Technology and National Security Policy, National Defense University (2008); T. Precht, *Home grown Terrorism and Islamist Radicalisation in Europe*, Danish Ministry of Justice (2007).

[7] See *e.g.* G. de Kerchove, "L'Union européenne et le monde dans la lutte contre le terrorisme" *in* M. Dony (ed.), *La dimension externe de l'espace de liberté, de sécurité et de justice au lendemain de Lisbonne et de Stockholm: un bilan à mi-parcours*, Editions de l'Université de Bruxelles (Bruxelles, 2012); M. Donini, « Sicurezza e diritto penale », (2008) 10 Cass pen 3558.

[8] See *e.g.* K. Sugman Stubbs and F. Galli, "Inchoate offences. The sanctioning of an act prior to and irrespective of the commission of any harm" *in* F. Galli and A. Weyembergh (eds.), *EU counter-terrorism offences: what impact on national legislation and case law*, Editions de l'Université de Bruxelles (Bruxelles, 2012).

[9] See *e.g.* M.F.H. Hirsch Ballin, *Anticipative criminal investigations. Theory and counter-terrorism practice in the Netherlands and the United States*, TMC Asser Press, (The Hague, 2012).

[10] Yet serious crime is not defined as such in EU law (art. 83(1) TFUE). For the purpose of the analysis examples are hence taken from national legislation, mostly with reference to organised crime and terrorism. Both categories are particularly relevant because they have lead to the introduction of specific legal regimes for the use of surveillance technologies within the three countries.

[11] See *e.g.* H. Fenwick (ed.), *Development in counter-terrorist measures and uses of technology*, Routledge (Abingdon, 2012).

[12] DETECTER Project (Detection Technologies, Counter-Terrorism Ethics, and Human Rights), FP7 Security Programme, www.detecter.bham.ac.uk (accessed on 27 October 2012)

[13] SURVEILLE Project FP7, SEC 2011.6.1-5, Surveillance and challenges for the security of the citizen, Annex 1 – "Description of Work", p. 12

[14] SURVEILLE Project, Annex 1 – "Description of Work", p. 4-15

EU level. It is based on the definitions provided within this project[15] and should be read in conjunction with the other deliverables submitted or soon to be submitted.[16]

The comparative study tests the existence of a double shift mainly resulting from the catalysing effect of serious crime.

Firstly, surveillance technologies introduced in relation to serious crimes (*e.g.* interception of telecommunications) are increasingly used for the purpose of preventing and investigating "minor" offences; at the same time, surveillance technologies originally used for public order purposes in relation to minor offences (*e.g.* CCTV cameras) are now increasingly affected to the prevention and investigation of serious crime.

On the one side, serious crime including terrorism has had a catalysing effect on the criminal justice system, prompting an increased use of surveillance techniques and technologies. The subsequent introduction of derogatory provisions has been first regarded as exceptional and limited in scope first to terrorism and then to organised crime. Through a normalisation process at the initiative of the legislator, specific measures have become institutionalised over time as part of the ordinary criminal justice system and they have a tendency to be applied beyond their original scope.[17]

On the other side, a parallel shift has occurred in the opposite direction. Video-surveillance technologies, which are one of the most obvious and widespread signs of the development of surveillance, were originally conceived by the private sector for security purpose. They have been subsequently employed for public order purposes and finally in the prevention of minor offences and/or petty crimes (such as street crimes or small drug dealers). In such context, they were rather a tool to deter would-be criminals rather than an investigative means.[18] At the same time, the terrorist threat has become an argument for an even more extensive use of video surveillance.

The question therefore arises as to: whether there is still a difference to be made between means that can be used only in the fight against serious crime and others applicable only to counter minor offences; or whether a mutual contamination has occurred so that means originally introduced in one or the other domain are now applicable to both the prevention and investigation of serious crime and minor offences.

Secondly, means at the disposal of each actor (intelligence[19] and law enforcement agencies) for the prevention and investigation of serious crime are evolving so that the share of tasks and competences has become blurred.

When coping in particular with the terrorism threat, democratic States have had to redraw the boundaries between the different tasks involving surveillance, namely protecting national security,

---

[15] *See infra*.

[16] SURVEILLE, Surveillance : Ethical Issues, Legal limitations and Efficiency, FP7-SEC-2011-284725, "Report describing the design of the research apparatus for the European-level study of perceptions", D3.1, October 2012; "Survey of surveillance technologies, including their specific identification for further work", D2.1 August 2012.

[17] O. Gross, 'Chaos and rules' (2003) 112 *Yale Law Journal* 1011, 1090; D. Dyzenhaus, "The permanence of the temporary" *in* R.J. Daniels and others (eds.), *The security of freedom*, University of Toronto Press (Toronto, 2001).

[18] *e.g.* A. Bauer and F. Freynet, *Vidéosurveillance and vidéoprotection*, PUF (Paris, 2008); EFUS, *Citizens, Cities and video surveillance, Towards a democratic and responsible use of CCTV*, ed. EFUS (Paris, 2010) pp. 183-84; Vidéo-surveillance Infos, "Dispositif de sécurité au stade de France: ergonomie et évolutivité" (14 October 2011).

[19] Intelligence information refers to "secret material collected by intelligence agencies and increasingly by the police to provide background information and advance warning about people who are thought to be a risk to commit acts of terrorism or other threats to national security".[19] K. Roach, "Secret evidence and its alternatives" *in* A. Masferrer (ed.), *Post 9/11 and the state of permanent legal emergency. Security and human rights in countering terrorism*, Ius Gentium: Comparative Perspectives on law and justice, Springer (2012) p. 180.

maintaining public order, preventing and investigating crimes. This has taken several forms: the extension of surveillance powers in all these tasks; the emergence of new challenges resulting from the use of intelligence information gathered for national security purposes in criminal prosecutions; the sharing of information and the creation of "fusion centres" where data are merged while maintaining more or less a division of tasks between intelligence agencies and law enforcement authorities.

Such a development has led to an unclear situation as a broad range of investigation techniques and technologies may be used in relation to different offences as well as at different phases of the procedure, *e.g.* prevention or investigation.

The question to be assessed in relation to the second dimension of the shift is thus whether the current trend has provided an opportunity to clarify the share of tasks and competences between intelligence services and law enforcement authorities (including *police administrative* and *police judiciaire*) or rather whether it lead to a more blurred division.

A blurred division would lead to both a situation of legal uncertainty and a competition between the different actors involved.

Surveillance may be defined as "the keeping of watch over someone or something. Technological surveillance is the use of technological techniques or devices to detect attributes, activities, people, trends, or events."[20]

For the purpose of this research, two surveillance technologies – used by both law enforcement authorities and intelligences agencies – have been chosen as the examples of the first dimension of the double shift hypothesis: the interception of telecommunications and video surveillance (most importantly CCTV cameras).

It is noteworthy that interception of telecommunications is a broader category than "phone interception" as it encompasses also the interception of emails or other messages sent via the Internet.[21] This kind of interceptions operate in real time and may deal with the content of the telecommunications and is thus more intrusive into privacy than other measures such as identification or tracking, which do not address the content. The scope of this study does not include provisions on the retention on data by private companies for either commercial of law enforcement purposes which will constitute the focus of subsequent research.[22]

In relation to video-surveillance technologies, this article only focuses on the use devices installed either by public authorities (*e.g.* in the streets, train stations, airport, stadium) or by private companies (*e.g.* shopping malls, outside banks) for prevention purpose. Thus, neither the video-surveillance taking place in the framework of a criminal investigation, authorised and then executed by judicial competent authorities with reference to a targeted individual nor the video-surveillance under the supervision of public authorities in private premises are part of this deliverable.

---

[20] J.K. Petersen, *Handbook of surveillance technologies*, 3d ed., CRC Press, Taylor & Francis Group (2012) p. 10. Within the SURVEILLE Project, surveillance is defined as "targeted or systematic monitoring of persons, places, items, means of transport or flows of information in order to detect specific, usually criminal, forms or conduct, or other hazards, and enable, typically, a preventive, protective or reactive response or the collection of data for preparing such a response in the future". Surveillance technologies are hence "the use of any human-made devices in surveillance" or methods "used to detect something in a security or safety context, with the focus on a law enforcement, customs or security authority". SURVEILLE Project, Annex 1 "Description of Work", p. 5.

[21] In the United Kingdom, s. 2 RIPA 2000 defines a telecommunication system as « any system which exists for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy ». Remarkably, in some countries the same rules apply to the interception of communications via the Internet, whereas in others there is a gap in the existing regulation and this constitutes part of the problem.

[22] See "Comparative paper on data retention regulation in a sample of EU Member States", SURVEILLE Project, D4.3 (submitted on 30 April 2013).

This study focuses on three EU Member States, namely France, Italy and the United Kingdom. Various reasons justify this choice: these states have experienced terrorism before 9/11 and the fight against serious crime has long been a priority; they also are working together in the EU G6;[23] their national legislation has been a point of reference for the development of EU policies and instruments such as the two Framework Decisions on combating terrorism of 2002 and 2008.[24] Moreover the chosen case studies must be representative of: both common law and civil law systems; different criminal procedure systems (accusatorial/inquisitorial/mixed); different systems of share of competences and of articulation between intelligence and law enforcement bodies (including *police administrative* and *police judiciaire*).[25]

The use of surveillance technologies and additionally the information gathered is particularly sensitive with regard to the right to privacy they may affect and the principle of proportionality with reference to the conditions allowing for their use.[26] The human rights dimension will be the backdrop of this research.

The deliverable will provide a brief overview of criminal procedure developments in the selected Member States resulting from the catalysing effect of organised crime and terrorism (2). Then it will analyse the different elements of the double shift with reference to the two surveillance technologies chosen as case studies: the interception of telecommunications (3) and video-surveillance (4). Eventually, it will ascertain the existence of a blur in the share of tasks (5).

The expansion of derogatory regimes to cope with serious crime

In the three Member States, specific (and often derogatory) provisions, both of substantive criminal law and criminal procedure, have been adopted over time in order to fight against serious crime, especially against terrorism and/or organised crime.[27]

Remarkably, both in France and in Italy there has been a reciprocal influence of anti-terrorism and anti-organised crime legislation during the last thirty years and the subsequent re-enactment of repealed provisions following a new outburst of terrorism or organised crime at different stages.

In Italy, since 1975 (Law 152/1975) special measures adopted to deal with the domestic terrorist threat have been progressively introduced as derogations to the ordinary principles of criminal law.[28] The

[23] The EU G6 is an internal security vanguard made up of the interior ministries of Britain, France, Germany, Italy, Poland and Spain. According to H. Brady, "with the possible exception of Poland, these countries all feel threatened by terrorism and have elaborate national counter-terror systems", H. Brady, "Intelligence, emergencies and foreign policy – The EU's role in counter-terrorism", *Centre for European Reform* (2009) p. 7.

[24] Framework Decision 2002/474/JHA on combating terrorism [2002] OJ L 164/3 and Framework Decision 2008/919/JHA [2008] OJ L 330/21. For a detailed comment on the interplay between the two instruments see Galli and Weyembergh (eds.), *EU counter-terrorism offences*, pp. 11-32, pp. 49-64; pp. 83-98; pp. 117-132.

[25] The organisation for each State differs according to his traditional system: the common law division (police intelligence, police investigation and prosecution by judicial authorities) and the civil law twofold division (administrative police and judicial police).

[26] S. Van Drooghenbroeck, *La proportionnalité dans le droit de la convention européenne des droits de l'homme. Prendre l'idée au sérieux*, Bruylant, (Bruxelles, 2001); C. Warbrick, 'The ECHR and the Prevention of Terrorism' (1983) 32 *ICLQ* 82 ; Institute for prospective technological studies, *Security and privacy for the citizen in the Post-September 11 digital age: A prospective overview*, Report to the European Parliament Committee on citizens' freedoms and rights, justice and home affairs (LIBE), EUR 20823 (July 2003); M. Levi and D.S. Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society" (2004) 31(2) Journal of Law and Society 194.

[27] F. Galli, *British, French and Italian measures to deal with terrorism: a comparative study*, Doctoral thesis, University of Cambridge, 2009 (yet unpublished).

[28] G. Illuminati, "Reati "speciali" e procedure "speciali" nella legislazione d'emergenza" (1981) Giustizia Penale 106.

enactment of the new *Codice di Procedura Penale* in 1988 was meant to redress the numerous derogations brought about by the emergency legislation in the previous decade. However, from when the level of the threat from organised crime increased once again at the beginning of the 1990s, the existing tools seem inadequate and major changes in the law came along in the form of subsequent layers of new principles, rules and exceptions and not as a coherent legislative design (see *e.g.* Law 203/1991). [29] With the enactment of Law 438/2001 and Law 155/2005 the scope of many of these provisions has been extended to cope with the newly emergent international terrorist threat.

On 9 March 2004, the French Parliament enacted the so-called *Loi Perben II* (Law 204/2004), which contains the most far-reaching amendments of substantive criminal law and criminal procedure of the last decades.[30] In this context special anti-terrorist procedures (*e.g.* with regard to house searches, identification of individuals, *garde à vue*, surveillance, or interception of communications) have been applied to a long catalogue of offences classified as "organised crime". As in the case of the definition of terrorism as a criminal offence, the legislator has not attempted to define "organised crime" and has merely introduced in the *Code de Procédure Pénale* a list of more than thirty offences to which special procedures become applicable. This list also includes a number of less serious offences (such as extortion, procuring or assistance in the illegal entry of immigrants) which do not obviously justify the use of extraordinary powers. The legislator can expand this catalogue at any time.

In the United Kingdom, the counter-terrorism "arsenal" is only the tip of the iceberg of a broader phenomenon, most importantly in relation to the use of administrative measures which are no longer exceptional and temporary, nor are they necessarily linked with a genuine emergency (see *e.g.* Sexual Offences Prevention Orders (SOPO) and Risk of Sexual Harm Orders, Anti-Social Behaviour Orders (ASBOs), Serious Crime Prevention Orders and Violent Offender Orders. Not all preventive orders require a criminal offence to have been committed).[31]

In relation to the **definition of terrorism** the three countries have taken similar approaches.[32] In the first place, the aim of the attempts was to prompt the use of special procedural measures. Secondly, the definitions adopted at different stages share a common core of *mens rea* derived from international sources: the intention to make indiscriminate use of violent activities to spread intimidation or terror within a community and thus influence an institutional figure for political or subversive purposes. French law attaches to such *mens rea* a list of existing criminal offences. The British definition, by contrast, encompasses only a list of behaviours exemplifying which type of activities would be proceeded against under the Terrorism Act 2000. And in Italy the definition is left open: any act committed with the identified *mens rea* would be considered an offence with a terrorist intent.[33]

---

[29] P.L. Vigna, "Il processo accusatorio nell'impatto con le esigenze di lotta alla criminalità organizzata" (1991) Giustizia Penale 462.

[30] J. Pradel, "Vers un ''aggiornamento'' des réponses de la procédure pénale à la criminalité" (2004) 19 Semaine Juridique 132 and (20) Semaine Juridique 134.

[31] Some require the subject to have been convicted or an offence, and others require the civil court imposing the order to be satisfied that he has committed one.

[32] art. 421(1) French *Code Penal*, art. 270 *sexies* Italian *Codice Penale*, s. 1 UK Terrorism Act 2000

[33] F. Galli, *British, French and Italian measures to deal with terrorism: a comparative study*, pp. 60-72 (yet unpublished).

Definition of organised crime

	France	Italy	United Kingdom
Definition	*Association de malfaiteurs*[34] (no need of a number of associates)	*Association de malfaiteurs* (identification of a number of associates)	"individuals, normally working with others, with the capability to commit serious crime on a continuing basis, which includes elements of planning, control and coordination, and benefits those involved. A significant proportion of organised criminals are motivated, principally, by the desire to make money." [35]
Reference	Art. 450(1) Penal Code	Art. 416 and 416 *bis* PC	HM Government, *Local to global: reducing the risk from organised crime*, within the organised crime strategy of 28 July 2011

In France and in Italy, the law aimed at criminalising only those associations which were actively organised in gangs, the members acting with a common purpose framed by the existence of chiefs and conventions for the distribution of profits. By contrast with the parallel Italian provisions, the French Penal Code did not identify a minimum number of associates.[36]

The United Kingdom definition is less precise than the French or Italian ones. The structure and organisation of such groups may vary: they may consist of a durable group of key individuals surrounded by a cluster of subordinates or loose networks of individuals coming together for the duration of a criminal activity, acting in different roles depending on their skills and expertise. [37]

[34] More narrowly drawn than the crime of conspiracy in English Law, in particular because the *association* must be demonstrated by acts putting it into execution.

[35] HM Government, *Local to global : reducing the risk from organised crime*, Policy paper, Organised crime strategy, 28 July 2011, p. 5 and 8.

[36] For a detailed account of the origins and purpose of this offence in Italy see G. Fiandaca, « I reati associativi nella recente evoluzione legislativa » *in* A. Spataro and others, *Il Coordinamento delle Indagini di Criminalità Organizzata e Terrorismo*, CEDAM (Padova 2004) pp. 1-34; and, in France, see M.C. Adolphe and M.F. Hélie, *Théorie du Code Pénal. Vol III*, Marchal et Billard (Paris 1887).

[37] Serious Organised Crime Agency at http://www.soca.gov.uk/threats/organised-crime-groups (accessed 1 March 2013); D. Blunkett, Home Secretary, White paper One Step Ahead – A 21st Century Strategy to Defeat Organised Crime, March 2004 used this definition adopted by the NCIS (National Criminal Intelligence Service); see also, M. Maguire, R. Morgan and R. Reiner (eds.), *The Oxford handbook of criminology*, 5th ed., (Oxford, 2012) p. 601.

Towards a generalised use of surveillance technologies? The interception of telecommunications

Provisions concerning the interception of telecommunications in terrorist and organised crime cases often derogate from the ordinary regime.

In France and in Italy, two types of interceptions of telecommunications exist according to the phases of the procedure.

In France, a distinction must be drawn between interception of telecommunications during a judicial investigation for the detection and the investigation of a crime (judicial interceptions), and interceptions authorised by the executive for security reasons (administrative interceptions) called *interceptions de sécurité*.[38]

Law 646/1991 provides the legal framework for both judicial (art. 100 ff *CPP*) and administrative interceptions (nowadays encompassed in the *Code de la Sécurité Intérieure*), as amended in 2002, 2004, 2006 and 2012.[39] Article 1 of Law 646/1991 reaffirms the principle of the secrecy of communications, from which only the public authority can derogate under the circumstances of public interest recognised and restricted by the law.[40]

As detailed below, over the years the legal regime of judicial interceptions has been considered by some to be too strict and inadequate and thus extraordinary provisions have been introduced for the purpose of an effective fight against organised crime.

The Italian regime reproduces the distinction between *ante-delictum* and *post-delictum* interceptions.[41] In ordinary cases, judicial interceptions of telecommunications are regulated by art. 266 and ff. *CPP*. Preventive interceptions are currently regulated under art. 226 *disp. att. CPP*, identifying the authorities entitled to apply for and issue interception warrants, the purpose of such application, and its specific content.[42] It is noteworthy that *ante-delictum* interceptions are not exclusively an administrative prerogative in Italian law.

The communications intercepted cannot be used as evidence when a professional privilege or a State or public secret is involved.[43] Additionally, interceptions made without complying with the relevant conditions are invalid and cannot be used at trial. This is one of the oldest 'exclusionary rules' in the Italian system.[44]

---

[38] F.-B. Huyghe, *Les écoutes téléphoniques*, Que sais-je ? PUF, n°3874 (Paris 2010) ; C. Guerrier, *Les écoutes téléphoniques*, CNRS (Paris, 2000) ; R. Errera, *Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques*, Revue trimestrielle des droits de l'homme 55 (July 2003) pp. 851-870 ; J. Pradel, 'Un exemple de restauration de la légalité criminelle' (1992) Dalloz 49.

[39] The law applies not only to phone tapping but to all means of telecommunications (telephone, fax, telex, communication by radio, broadcasting of images, electronic communication, etc.).

[40] Freedom of expression is considered of constitutional value. DC n°84-181 (1984). Also art. L241-1 *CSI*.

[41] G. Spangher, "La disciplina italiana delle intercettazioni di conversazioni o comunicazioni" 1 Archivio Penale 3, 1994; P. Balducci, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Milano, Giuffrè 2003; C. Parodi, *Le intercettazioni. Profili operativi e giurisprudenziali*, Giappichelli (2002); A. Balsamo, "Intercettazioni: gli standards europei, la realtà italiana, le prospettive di riforma"(2009) 10 Cass pen 4023.

[42] See in relation to terrorist offences G. Garuti, "Le intercettazioni preventive nella lotta al terrorismo internazionale" (2005) *Diritto Penale e Processo* 1457

[43] G. Illuminati (ed.), *Nuovi profili del segreto di stato e dell'attività di intelligence*, Giappichelli, (Torino 2011).

[44] art. 271 *CPP*.

Exceptional provisions for the interception of communication under less stringent requirements were first enacted by art. 13 Law 203/1991 for the investigation of organised crime offences.[45] The complete re-organisation of the provisions on interceptions is one of the most important features of the new anti-terrorism regime (Law 431/2001 and Law 155/2005).[46]

In the United Kingdom there is no distinction between administrative or judicial interceptions, which is comparable to the French or Italian models. Interception of telecommunications is regulated under the Regulation of Investigatory Power Act (RIPA) 2000.[47] This Act establishes the legal regime for different surveillance techniques.[48] In doing so, it takes into account not only the latest technological developments but also the ECHR and the related case law.[49]

The most important aspect of regulation in this context is that intercepted conversations are not admissible as evidence in criminal proceedings.[50] Interception of telecommunications can be used for investigative purposes and as an instrument for crime prevention (information gathering) but not for prosecution. The contents of interception of telecommunications may provide the police with lines of enquiry but may not be used as evidence in a public court.[51] Nevertheless, because the restrictions under s. 17 RIPA apply only to interception conducted in the United Kingdom, communications lawfully intercepted by foreign authorities in their own jurisdictions may be adduced in evidence in the UK court.[52]

It is noteworthy that, in the three countries, wiretapping or interception of telecommunications without legal authorisation is an offence.[53]

After this general presentation, the comparative study focuses on the actors involved in the interception for either authorisation or execution purposes, its scope and duration.

Differences exist between *ante-* (mainly administrative) and *post-delictum* (mainly judicial) interceptions. Interceptions of telecommunications have been first developed for investigative

---

[45] G. Melillo, "La ricerca della prova tra clausole generali e garanzie costituzionali: il caso della disciplina delle intercettazioni nei procedimenti relativi a 'delitti di criminalità organizzata'", (1997) Cassazione Penale 3512.

[46] e.g. F. Caprioli, 'Le disposizioni in materia di intercettazioni e perquisizioni' *in* G. Di Chiara (ed), *Il processo penale tra politiche della sicurezza e nuovi garantismi*, Giappichelli (Torino 2003).

[47] *e.g.* D. Ormerod and S. McKay, "Telephone intercepts and their admissibility" (2004) Criminal Law Review 15; P Mirfield, 'RIPA 2000: Part 2: Evidential Aspects' (2001) Criminal Law Review 91; M Ryder, 'RIPA reviewed',(2008) 4 Archbold News 6; Sir J. Chilcot, 'Privy Council Review of intercept as evidence: report to the Prime Minister and the Home Secretary', Chilcot Review (Cm 7324 2008).

[48] The investigatory powers regulated by RIPA 2000 are: the interception of communications, the acquisition of communications data (eg telephone billing data), intrusive surveillance (on residential premises or private vehicles), covert surveillance during specific operations, the use of covert human intelligence sources (agents, informants and undercover agents) and access to encrypted data.

[49] RIPA (ch.1, s. 5) introduced numerous changes in the Interception of Communications Act (IOCA) 1985, which had been enacted in response to the condemnation of the United Kingdom by the Strasbourg Court in the *Malone* case (*Malone* v. *UK* (1984)). In that case the Strasbourg Court made it clear that the existing rules and practices in the United Kingdom did not satisfy the requirement of art. 8 ECHR that any interference with a person's privacy by a public authority should be 'in accordance with the law'.

[50] This ban has long been the most controversial feature of the interception legal regime. At present, neither the government nor civil libertarians seem to be particularly concerned by the intrusion into personal privacy, as similar kinds of evidence (covert agents, bugging, eavesdropping, video-surveillance) are already admissible in court, even where not authorised, without any particular practical difficulty.

[51] s. 15(3) and 17 RIPA. See JUSTICE, *Intercept evidence: Lifting the ban*, Report (October 2006).

[52] *R.* v. *Aujla* [1998] 2 Cr App R 16 approved by the House of Lords in *R.* v. *P.* [2001] 2 WLR 463.

[53] arts. 615, 617, 617*bis*, 623*bis* CP.

purposes and then also used for preventive purposes. Therefore, the analysis will starts with the first one and then continue with the second one.

Post-delictum interceptions

Actors

With regard to actors, two issues are worth comparing: who authorises the interceptions and who executes them.

France

In most cases of **post-delictum interceptions,** the authorisation is given by a judicial authority both in France[54] and in Italy[55].

In terms of existing derogation, it is noteworthy that in France, Law 204/2004 extended the possibility to use judicial interceptions to preliminary and *in flagrante* police investigations (*i.e.* to cases where no *instruction* has been yet instituted) for a limited number of serious offences listed in art. 706(73) *CPP*. According to art. 706(95) *CPP*, these kinds of interception are requested by the prosecutor, authorised and supervised by the *juge des libertés et de la détention (JLD)*, and carried out by the police officers (*police judiciaire*). These operations and recordings are subjects to a statement (*procès-verbal*) written by the police.

This is the technique most often used by the *JIRS* (*juridictions inter-régionales spécialisées*)[56] for the purpose of investigation and prosecution of the crimes listed in article 706(73) CPP, the most serious offences, usually committed by an organised group.[57]

Italy

In the Italian regime**,** the interception warrant is issued by the judge for preliminary investigations (*giudice per le indagini preliminary, GIP*) upon the request of the prosecutor.[58] However, when the measure is motivated by emergency[59], the prosecutor may act without the prior authorisation of the judge.

In ordinary cases, the interception is authorised by a reasoned decision where there are serious grounds (*gravi indizi*) to believe that a crime has been committed and it is absolutely indispensible for the purposes of the investigation.[60] However, the GIP – who is formally in charge of keeping these proceedings under scrutiny – is unaware of the facts grounding the investigation. So it is difficult for

[54] art. 100 and ff *CPP*.

[55] art. 266 and ff *CPP*.

[56] The *JIRS*, created by Law 204/2004, bring together prosecutors and judges of the instruction and are specialised in organised crime, financial crime, but also in complex cases justifying significant investigation.

[57] J. Pradel and J. Dallest, *La criminalité organisée – Droit français, droit international et droit comparé*, Litec, (2012) p.144.

[58] art. 267 *CPP*.

[59] art. 267(2) *CPP*.

[60] F. Galluzzo, "Spunti di riflessione in tema di intercettazioni" (2010) 9 Cass pen 3141.

him to assess the seriousness of the file.[61] In addition, the prosecutor can exceptionally authorise interceptions when there is some urgency.[62]

After having been authorised, judicial interceptions must be carried out by the office of the prosecutor, but the measure may also be executed by the police under the supervision of the prosecutor.[63]

The United Kingdom

By contrast, in the United Kingdom, there is no distinction between *ante-* and *post-delictum*, thus the interception is always authorised by an administrative authority, and not a judicial one. There is a limited number of persons by whom, or on behalf of whom, the applications for issue of interception warrants may be made and all interception warrants are issued by the Secretary of State or by a senior official in urgent cases and where there is a request for international mutual assistance.[64]

Nevertheless some features of the regime are of interest. Under sections 5–8 RIPA at the request of authorised officials,[65] the Secretary of State may lawfully grant an interception warrant only if the existence of certain limited grounds are satisfied and only if necessary and proportionate.[66] The police act under this warrant. As underlined by Prof. Spencer, "in all three parts of the United Kingdom warrants to intercept communications are issued not by judges, but by ministers: usually the Home Secretary. Neither they nor their civil servants wish the legality or propriety of their decisions to issue warrants to be scrutinised by judges in any prosecutions that might follow, and to avoid this, prefer a situation in which the fruit of the intercept can only be used as "operational material", even though this is a dreadful obstacle to prosecution."[67]

Scope

France

Regarding the scope of the measure, in France, whereas "ordinary" interception is possible for any crime or *délit* punishable with a minimum sentence of two years of imprisonment, the **post-delictum interception** allowed by art. 706(95) *CPP* is possible only in case of offences listed in article 706(73) *CPP*, namely the most serious offences linked to organised crime (*e.g.* murder committed "*en bande organisée*") and in compliance with the necessity and proportionality of the use of such technique.[68]

It is noteworthy that police officers may extend the surveillance to the whole territory after informing the prosecutor (no agreement is required but the prosecutor can object), if there are one or several

[61] See D. Siracusano and others, *Diritto processuale penale Vol II*, Giuffrè (Milano 2006) pp. 151-52.

[62] The prosecutor must within 24 hours ask for validation by the judge (art. 267-2 CPP) who has to decide on the validity of the measure within 48 hours. If the authorisation is not validated within the prescribed period, the interception has to stop and the results cannot be used.

[63] art. 268(3) *CPP*.

[64] art. 6(2) and 7(2) RIPA 2000.

[65] *e.g.* Chiefs Constable, Chiefs of the Intelligence and Security Services, Director of Government Communication Headquarters, Director General of the National Criminal Intelligence Service; s. 6(2) RIPA 2000.

[66] s. 5(3) RIPA 2000.

[67] J.R. Spencer, "No thank you, we've already got one, Why EU anti-terrorist legislation has made little impact on the law of the UK", *in* Galli and Weyembergh (eds.), *EU Counter-terorrism offences*, p. 129.

[68] ECHR, *Huvig and Kruslin* v. *France*, 11105/84 [1990] ECHR 9, 24 April 1990 ; ECHR, *Lambert* v. *France*, 1998-V, n°86, 24 August 1998; ECHR, *Matheron* v. *France*, 57752/00, 29 March 2005.

plausible reasons to suspect someone of having committed one of the crimes and misdemeanours of the article 706(73).[69]

Italy

In Italy**, post-delictum interceptions** may be used in relation to most serious offences, such as intentional crimes punishable with imprisonment with a maximum penalty of at least five years (art. 266(1) *CPP*).

A specific regime applicable for organised crime was introduced in article 13 of Law 203/1991 and, then extended to terrorist cases by article 3 Law 438/2001 and more recently to human trafficking by article 9 Law 228/2003.

Three main derogations are thus introduced to the ordinary regime. Firstly, an interception can be authorised where there are sufficient (as against "serious") grounds (*sufficienti indizi*) for believing that a crime has been committed.[70] Secondly, interceptions need only to be necessary (rather than indispensable) for investigative purposes. Thirdly, the interception may aim at developing new investigative paths (rather than being merely employed in the course of an already established investigation).

In addition, article 6 of Law 438/2001 extends the authorisation of the use of interception of telecommunications (*intercettazioni ambientali*) to seek out fugitives.[71]

The United Kingdom

In the United Kingdom, by contrast to what have been said in the section on actors, a difference exists in relation to whether they are in the context of a prevention or investigation of offences. During the investigation phase, when law enforcement agents are gathering information, the methods used depend on the complexity of and not on the gravity of any suspected offence. Interception without a warrant is possible if one party consents and if surveillance by means of interception has been authorised under RIPA provisions.

Duration

Provisions concerning the **duration** of the measure are also different for *ante-delictum* or *post-delictum* interceptions.

France

Concerning ***post-delictum* interceptions**, in France**,** in ordinary cases, the *juge d'instruction* may authorise the interception for a maximum period of four months. Such an initial period can, however, be extended as long as necessary for investigative purposes.[72] However, in the framework of the fight against the most serious crimes, the *JLD* may, at the request of the prosecutor, authorise the interception for a maximum period of one month, renewable once under the same conditions of form

[69] art. 706-80 *CPP*.

[70] Note that following the enactment of Law 63/2001 on due process, information resulting from police informers or security services are not admissible for this purpose (art 203(1) *CPP*).

[71] art. 295(3) *CPP*.

[72] art. 100(2) *CCP*.

and duration.[73] Finally, the *procès-verbaux* are destroyed at the behest of the prosecutor and at the expiry of the limitation period for the public action.[74]

Italy

Post-delictum interceptions, in Italy**,** can last for up to fifteen days, renewable as many times as the reasons for the initial decision exist and upon authorisation of the judge for preliminary investigations.[75] Interceptions in terrorist and organised crime cases can last for up to forty days (rather than fifteen)[76], renewable for subsequent periods of twenty days (rather than fifteen), when the reasons for the initial decision still exist.[77] There is no limit on the number of possible renewals. In case of emergency, the renewal can be authorised by the prosecutor and then validated by the judge, who has to verify the existence of urgency.

The United Kingdom

In the United Kingdom**,** according to RIPA 2000, the duration of the initial interception warrant was originally meant to be of three months at most, although renewable. The Terrorism Act 2006 has amended RIPA so that the duration of the initial interception warrant issued in the interests of national security is extended to six months and it is renewable at any time before the end of the relevant period for another six-month period.[78]

Post-delictum interceptions

	France	Italy	United Kingdom
Ground 1	*Crimes* and *délits* (max penalty ≥ 2 years)	Crimes (max penalty ≥ five years (art. 266(1) CPP)	Complexity of the offence; only if necessary and proportionate
Authorisation	*Juge d'instruction* (art. 100 *CPP*)	Prosecutor after authorisation of the judge for preliminary investigation (art. 267 CPP); in the case of emergency, authorisation from the prosecutor	Secretary of State or by a senior official in urgent cases and where there is a request for international mutual assistance
Duration	4 months	15 days	6 months (Terrorism Act 2006)
Renewal	no limit	no limit	no limit
Ground 2	Suspicious deaths	organised crime (art. 13 Law 203/1991); extended	

[73] art. 706(95) *CPP*. An amendment to *Loi d'orientation et de programmation pour la performance de la sécurité intérieure* was adopted on 9 September 2010 on the initial deadline of 15 days changed to one month. The interception may last shorter than in oreinary cases because it is not requested by the juge d'instruction but simply at the request of the prosecutor and the judicial guarantees are thus more limited.

[74] Cass. Crim., 21 February 2007, BC 55, p. 304. The rule is not applicable to the *procès-verbaux* of the transcription of interceptions, which are procedural pieces.

[75] art. 267(3) *CPP*.

[76] art. 13 Law 203/1991.

[77] art. 13 Law Decree 152/1991, converted into Law 203/1991.

[78] s. 32 TA 2006.

	or disappearances	to terrorist cases by art. 3 Law 438/2001 and more recently to human trafficking (art. 9 Law 228/2003)	
Authorisation	*Juge d'instruction* (art.80(4) *CPP)*	prosecutor	
Duration	2 months	40 days (art. 13 Law 203/1991)	
Renewal	no limit	20 days each renewal (art. 13 Law 203/1991)	
Ground 3	Hunting of an individual on the run		
Authorisation	Public prosecutor under the authority of the *JLD* (arts. 74(2), 695(36) and 696(21) *CPP*)		
Duration	2 months		
Renewal	Renewable in the limit of 6 months for ordinary offences (*correctionnelle*)		
Ground 4	Organised crime		
Authorisation	Public prosecutor under the authority of the *JLD* (art. 706(95) *CPP)*		
Duration	1 month		
Renewal	once renewable		

Ante-delictum interceptions

Actors

France

Regarding the **administrative interception** of telecommunications, in France**,** the use of these means is possible after a written and motivated decision by the Prime Minister. This authorisation is given on the proposal of the Minister of Defence, Minister of the Interior or of the Minister of Customs.[79] This

[79] art. L 242-1 *CSI*.

decision is sent immediately to the *Commission nationale de contrôle des interceptions de sécurité*, which ensures compliance with procedural rules.[80]

With regards to the **execution** of these means, an interesting feature in France concerns the execution of administrative interceptions and their transcription, which relies upon "*les personnels habilités*" (authorised personnel)[81] and thus implies a police officer (not necessarily *police judiciaire*) or a special named judge.

Italy

In Italy, in the case of *ante-delictum* interception, the Ministry of Interior[82] has general competence to apply for an interception for both organised crime and terrorism offences.[83] The warrant is issued by the prosecutor of the district that authorises the interception when the prevention interception is justified by enough elements of investigation and when it is necessary.[84] This interception may be done under the initiative of the law enforcement services and not only at the initiative of the prosecutor. In order to allow systematic scrutiny of the operations, the equipment to intercept the communications is physically located within the prosecutor's office. Law 155/2005 established a wider range of circumstances enabling the relevant authority to implement interceptions. In order to foster investigative and intelligence activities, the head of security and intelligence services (*SISMI* and *SISDE*) – acting after being delegated to do so by the Prime Minister – may apply to the prosecutor for an interception warrant whenever they are deemed to be necessary to prevent terrorist activities or subversion of the constitutional order *ex* art. 226 *disp. att. CPP*.[85] The legislator has thus attributed to the executive an important role in the political coordination of intelligence activities but has also placed a powerful new instrument in the hands of the security services.[86]

The United Kingdom

As previously said, the interception is always authorised by an administrative authority. According to the purpose of the interception and the degree of intrusion into the privacy, the level of authorisation is higher.

Scope

France

In France, ***ante-delictum*** **interceptions** are only used in exceptional cases as the research of information concerning national security[87], safeguarding essential elements of the scientific and

[80] See the reports of the Commission nationale des interceptions de sécurité *in* La documentation française.

[81] art. L 242(5) *CSI*.

[82] Or, on his mandate, the central bodies of the police forces, the "questore", the province commander of the Carabineers and of the *Guardia di Finanza*. From the sole interpretation of the legislation one cannot understand whether these authorities can act autonomously.

[83] Whereas the director of the national Anti-Mafia Directorate has a role limited to organised crime offences.

[84] M.-L. Cesoni (ed.), *Nouvelles méthodes de lutte contre la criminalité: La normalisation de l'exception*, p. 196. Art. 5 Law 438/2001 provides for this possibility with wide discretion respecting to the ordinary regime.

[85] J.A.E. Vervaele, "Special procedural measures and the protection of human rights, General report", (2009) 5(2) *Utrecht L Rev*.

[86] On intelligence services' competence and organisation see Law 801/1977 as amended by Law 207/2007.

[87] See Commission nationale de contrôle des interceptions de sécurité, *Annual report*, 2009, 18th ed., Paris, La documentation française, p. 39 and ff.

economic potential of France, the prevention of terrorism, of crime and organised crime or prevention of reconstitution or of maintaining of outlawed groups.[88] The Prime Minister motivates their use and "fishing expeditions"[89] are not allowed.

Italy

In Italy**,** *ante-delictum* interceptions are allowed to gather information when it is necessary for the prevention of organised crime, terrorism offences and human trafficking.

The extension of preventive interception is, in principle, offset by a more rigorous application of the rule of the inability to use the information within the criminal process[90], but only for investigative purposes. They are neither to be mentioned in investigative acts nor to be further disseminated by oral deposition or any other means.[91] They can be used as an element of a *notitia criminis* on which a prosecutor can start an investigation.[92] In addition, although the intercepted material cannot ground any other act or investigative tool, it can lead the police to the development of further autonomous investigations. Revealing this information is heavily penalised under Italian law.[93]

The United Kingdom

It is remarkable that in the United Kingdom, the use of interception of telecommunications is justified by the complexity of an offence and not by its seriousness. Hence the margin of appreciation of intelligence services and police in using this means is much broader.

For preventive purposes, the police can carry out telephone tapping in four situations: (1) in the interests of national security, (2) for the purpose of preventing or detecting serious crime, (3) for the purpose of safeguarding the economic wellbeing of the United Kingdom, (4) or in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.[94]

Duration

France

By contrast, in the case of **administrative interceptions** in France the authorisation is given for four months, renewable.[95] The recording is destroyed a maximum of ten days after the date on which it was

---

[88] art. L 241(2) *CSI*.

[89] A fishing expedition is a proactive action with surveillance technologies ; a speculative demand for information without a suspect, any real expectation about the outcome of the demand or its relevance to the investigation, where there is insufficient evidence to justify the issuing of a search warrant.

[90] art. 226(5) *disp. att. CPP* as modified by art. 5(5) Law 438/2001. See G. Melillo, 'Le recenti modifiche alla disciplina' (2002) Cass pen 904, 911; F. Ruggieri, *Divieti probatori e inutilizzabilità nelle intercettazioni telefoniche*, Giuffrè (Milano, 2001); C. Conti, "Intercettazioni e inutilizzabilità" (2011) 10 Cass pen 638; P. Sechi, "Intercettazioni e procedimento di prevenzione" (2011) 3 Cass pen 1082; S. Beltrani, "Intercettazioni inutilizzabili e procedimento di prevenzione" (2010) 9 Cass pen 2093.

[91] Two new criminal offences have been created in order to prosecute individuals who disseminate the intercepted material or the name of the officials involved in the proceedings.

[92] Cass. pen. 29 October 1998; Cass. pen. 10 November 2000.

[93] Vervaele, "Special procedural measures and the protection of human rights, General report" p. 94.

[94] s. 5 RIPA 2000.

[95] art. L242(3) *CSI*.

made.[96] The transcripts of the recordings are destroyed once their storage is no longer necessary for the aforementioned preventive purposes.[97] A report of each operation is drafted, which mentions the date and time when the interception started and ended.

Italy

In Italy for *ante-delictum* interceptions, operations can last for a maximum of forty days, subject to subsequent renewals of twenty days each, where the legal requirements still exist (as confirmed by the prosecutor in his written motivated application).[98] Preventive interceptions must end once a criminal activity becomes manifest (*notitia criminis*).[99] However, the law does not limit the number of available renewals. Intercepted material and all copies, extracts and summaries identified as the product of an interception, must be securely destroyed as soon as they are no longer needed for any of the authorised purposes.

The United Kingdom

In the United Kingdom, the duration of interception is the same than for investigative purposes: six months renewable.

Ante-delictum interceptions

	France	Italy	United Kingdom
Ground	Prevention of terrorism, crime and organised crime; national security; scientific and economic protection; outlawed groups	Prevention of organised crime, terrorism offences and human trafficking	(1) Interests of national security, (2) prevention or detection of serious crime, (3) safeguard of the economic wellbeing of the United Kingdom, (4) or in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement (RIPA 2000)
Authorisation	Prime Minister (art. L242-2 CSI); proposal of the Minister of Defence, Minister of the Interior or of the Minister of Customs.	Ministry of Interior has a general competence; prosecutor of the disctrict authorises when there are enough elements of investigation and when it is necessary	Secretary of State or by a senior official in urgent cases and where there is a request for international mutual assistance
Duration	4 months	40 days	6 months (Terrorism Act 2006)

[96] art. L242(6) *CSI*.

[97] art. L242(7) *CSI*.

[98] art. 226 *CPP*. For the purpose of an increased transparency, the requirement of a written motivated application represents a novelty of the Law.

[99] At this point, the file is transferred to the Public Prosecutor who may decide to open a judicial investigation.

Renewal	no limits (art. L 242(3) CSI)	20 days each renewal (art. 226 CPP)	no limits

Particular comments

After this comparative analysis, some remarks can already be formulated.

Firstly, it is remarkable that both for judicial (ordinary cases or organised crime/terrorism offences) and administrative interceptions, the duration of a warrant is much shorter in Italy than in the other two countries. However there is no limit to the available number of renewals.

Secondly, specific elements of evolution can be underlined for each country. In France**,** judicial interceptions have long been available for both minor and serious offences. Organised crime and terrorism have played a catalysing effect in the introduction of derogatory provisions and in the expansion of powers of actors involved in either the authorisation or the execution process. Primarily introduced for the purpose of preventing and investigating terrorism and organised crime, the scope of these provisions was then extended to cover also other types of crimes of less serious nature.[100]

In Italy**,** over time the use of the judicial interception of telecommunications has expanded both for the ordinary and derogatory regimes (*i.e.* the use of interceptions is possible in a wider number of cases and more easily authorised). This trend is a clear result of the catalysing effect of serious crime as the provisions under analysis are encompassed in legislation focusing on organised crime (*e.g.* Law 152/1991) and terrorism (*e.g.* Law 438/2001). The same trend can be easily identified in relation to the provisions on *ante-delictum* interceptions (*e.g.* art. 5 Law 438/2001 on terrorism, art. 13 Law 203/1991 on organised crime and art. 9 Law 228/2003 on human trafficking).[101]

The regime in the United Kingdom is particularly different from the French and Italian one (*e.g.* there is no distinction between judicial and administrative interceptions). However, as in the other two countries, serious crime broadens the possibility of using this technology, leads to the multiplication of actors who can authorise and execute interceptions (*e.g.* SOCA), enlarges the scope and extends the duration in terrorism and organised crime cases.

From a preventive purpose to an investigative use: video-surveillance

In relation to video-surveillance, the three regimes analysed are quite similar. Most importantly video-surveillance was at first introduced in the three countries by the private sector and then by public authorities (especially at the local level) for public order, prevention purposes. The question arising over time has been to understand whether and how videos and images so gathered can be used for investigation and prosecution purposes.

In France**,** the legal regime of video-surveillance now called *vidéoprotection* systems is mainly regulated by the *Code de la Sécurité Intérieure*.[102] A section of the Code focuses on video-protection

[100] See development of art. 706(73) CPP over time.

[101] In the last years, many scandals concerning illegally obtained interceptions and their subsequent publication by newspapers have revealed how the current regime is too easily subject to abuses. Thus, a reform of the legislative framework has been discussed. Disegno di Legge 1415, "Norme in materia di intercettazioni telefoniche, telematiche e ambientali" (30 giugno 2008). See F. Ruggieri, "Il Disegno di legge governativo sulle intercettazioni: poche note positive e molte perplessità" (2008) 6 Cass pen 2239.

[102] *e.g.* E. Heilmann and P. Melchior, *Vidéo-surveillance ou vidéo-protection ?*, Le choc des idées, Le Muscadier, Paris, 2012; A. Bauer and F. Freynet, *Vidéosurveillance et vidéoprotection*, Que sais-je ? PUF, 2012; A. Bauer and C. Soullez, *Les politiques publiques de sécurité*, Que sais-je? PUF (Paris 2011); F. Ocqueteau, "A comment on video-surveillance in France: regulation and impact on crime" (2001) 25(1/2) *International journal of comparative and applied criminal justice*

in general[103] and another section is rather devoted to the fight against terrorism[104]. Since its introduction by Law 73/1995[105], the use of this technology in the public sphere has become particularly important for anti-terrorism purposes as a tool to gather evidence when an offence is actually committed.[106]

In Italy**,** the fight against terrorism has led to a redefinition of priorities, objectives and instruments by national agencies, which significantly stimulated the use of new technologies. This lead to a larger deployment of video-surveillance systems (*videosorveglianza)* for crime and terrorism prevention purposes as a response to citizens' anxiety and need of reassurance.[107]

Video-surveillance is allowed only under certain conditions. In the public sphere, it is governed by specific data protection rules as detailed by art. 34 of the Code for data protection[108] and by the decision of 8 April 2010[109] of the Italian data protection authority.

"For the past 25 years, the United Kingdom has experienced an exponential increase in these technologies and is now the world leader in the use of video surveillance". [110] There are few restrictions on the use of cameras in public areas.[111] It is noteworthy that there is no specific statutory provision for video surveillance but only a CCTV code of practice, issued by the Information Commissioner's Office.[112] Such a code encompasses recommendations and not mandatory provisions. General video surveillance with CCTV operations does not need to be authorised under RIPA 2000. However, pre-planned, covert operations to follow known individuals for investigation purposes, which involve the use of CCTV, need authorisation. Members of the public need to be made aware that such systems are in use, and their operation is especially covered by the Data Protection Act 1998 and the CCTV Code of Practice.

As in relation to interceptions, three elements may be used to highlight similarities and differences of the legal regimes in the three countries: the actors, the scope and the duration of video-surveillance.

(Contd.)

103; N.C. Ahl, "La vidéo-surveillance en trompe-l'oeil", Le Monde, (29 October 2011); E. Heilmann, "La vidéo-surveillance, un mirage technologique et politique" *in* L. Mucchielli, *La frénésie sécuritaire*, La decouverte (Paris, 2008); N. Le Blanc, "Le bel avenir de la vidéosurveillance de voie publique" (2010) 2(62) Mouvements 32; T Le Goff, "Politique de securité: les chiffres et les impages, (2010) 3 Esprit 90; C. Laval, "Surveiller et prevenir" (2012) 2 *revue du MAUSS* 47. See also the reports of CNIL (*commission nationale de l'informatique et des libertés*).

[103] arts. L251(1) to L255(1).

[104] arts. L223(1) to L223(9).

[105] Law 73/1995.

[106] J. Pradel, *Procédure pénale*, 16th ed., Cujas (Paris, 2011) p. 407.

[107] *I sistemi di videosorveglianza 2, Videosorveglianza e privacy: quadro normativo, casistica e aspetti tecnici*, Transcrime, Inforsicurezza (4 May 2006) p.11.

[108] Legislative Decree 196/2003 bearing the adoption of the *Codice in material di protezione dei dati personali*.

[109] Garante per la protezione dei dati personali, Provvedimento in material di videosorveglianza, G.U. 99 (29 April 2010).

[110] EFUS, *Citizens, Cities and video-surveillance, Towards a democratic and responsible use of CCTV*, EFUS press (Paris, 2010) p. 14.

[111] On the United Kingdom regime, on CCTV cameras in relation to terrorism prevention see *e.g.* Q.A.M. Eijkman and D. Weggemans, "Visual surveillance and the prevention of terrorism: What about the checks and balances? »; *D. Fenwick*, "Terrorism, CCTV and the Freedom Bill 2011: Achieving compatibility with Article 8 ECHR?" and *B. Sheldon*, "Camera surveillance within the UK: Enhancing public safety or a social threat?" *in* H. Fenwick, *Developments in Counter-Terrorist Measures and Uses of Technology*, Rouledge (2012); D Giannoulopoulos, « La vidéosurveillance au Royaume-Uni. La caméra omniprésente », (2010) 1 Archives de politique criminelle 245.

[112] The Protection of Freedoms Act 2012 specifically requires the Secretary of State to prepare a code of practice containing guidance on the development of surveillance camera systems and the use of processing of images or other information obtained by virtue of such system. It also appoints a person as the Surveillance Camera Commissioner in order to encourage compliance with the surveillance camera code, review its operation and provide advice about the code (including changes to it or breaches of it).

Actors

In terms of actors, unlike in Italy, in France and in the United Kingdom, both the installation and the use of video-surveillance is authorised by an administrative authority.

France

In France**,** *vidéoprotection* can be authorised to ensure security when the places and buildings are especially exposed to a risk of assault and theft[113] and only if *vidéoprotection* does record neither the interior of dwellings and private buildings nor their entrances.[114] When the images gathered allow the identification of an individual, their use must comply with provisions of Law 17/1978 on data protection.

This measure is submitted to the authorisation of the *Préfet*, which can be made at any time by *arrêté préfectoral*, after consulting the *Commission départementale*.[115] It prescribes all necessary precautions, especially about the status of the persons in charge of the exploitation of the video-protection system or viewing images.[116] The authorisation is given to certain categories only, identified in relation to a specific case only, namely police agents and *gendarmerie*. It specifies the method of transmission and the duration of conservation of images. The *Commission départementale de vidéoprotection* gives an opinion on the implementation of such a technology, if these cameras are filming public roads or places or establishments open to the public.[117]

Yet, for the purpose of preventing terrorist acts, the representative of the State in the Department and, in Paris, the *Préfet* of police may prescribe the implementation of *vidéoprotection* systems and authorise also a broader category of individuals to view and use images.[118]

In urgent cases and in particular when under exposure to the risk of terrorist acts, the representative of the State in the Department and, in Paris, the *Préfet* of police may issue, without prior notice to the *Commission départementale de vidéoprotection*, provisional authorisation to install a video-protection system. The Chairman of the Commission will be informed of this decision so that the Commission provides its opinion.[119]

In order to best reconcile security needs and the right to privacy, ethics committees have been introduced. An institution, solely established for this purpose, monitors video-protection, in some French cities such as Lyon and Le Havre, with the specific aim of ensuring the respect of freedoms.[120]

For investigative purposes, a police officer can have access to the information gathered by video-protection via an ordinary judicial warrant (prosecutor or judge on the basis of specific provisions).

---

[113] art. L 251(2) *CSI* as introduced by Law 267/2011 that explains the purpose of video-protection. DC 2011-625, 10 March 2011.

[114] art. L 251(3) *CSI*.

[115] art. L 252(2) and L 252(3) *CSI*.

[116] art. L 252(1).

[117] art. L 251(4) *CSI*; the *Commission nationale de vidéoprotection* created by Law 2011/267 has a mission of advice and evaluation of the effectiveness of the video-protection at the level of the Ministry of Interior.

[118] art. L 223(2) *CSI*; see also J.-P. Courtois and C. Gautier, *Rapport d'information sur la vidéosurveillance*, Senate, n°131, 10 December 2008.

[119] art. L223-4 and L223-5 CSI.

[120] EFUS, *Citizens, Cities and video surveillance*, pp.141-142.

The United Kingdom

The use of CCTV cameras, in the United Kingdom**,** was motivated by the will to fight against street crime around shopping malls and stadium. Originally managed at the local level, it became a national policy thus engendering a need to coordinate local activities and favour the share of information.[121] CCTV cameras are overt and do not constitute intrusive and directed surveillance[122] (unless they focus on a specific group of people or individual and thus record movement and activities of a private person) and thus do not require an authorisation under Part II of RIPA 2000.

In the case where they are used as law enforcement activities, authorisation must be obtained, setting out what is authorised, how it will be carried out (*e.g.* which cameras are to be used), and what activity is to be caught and held on the tape or disk that results. Authorising officers have to take into account the risk of collateral intrusion into the privacy of persons who are not the subjects of the investigation.

Italy

By contrast, in Italy**,** since Law 38/2009, municipalities may use video-surveillance systems in order to guarantee urban security in public area[123] for public order purposes.

The Municipal Police manages the installation with the help of technicians from a private company and with the advice of the National Police. The National Police, the Municipal Police and the *Carabinieri* control the cameras. When the images are sent to the operator in the National Police Headquarters, they can, on the one hand, view the images from all cameras and, on the other hand, control the cameras remotely. The choice of operators is limited by national legislation to judicial police officers.

In the Municipal Police's video surveillance central operations office, three police officers work relayed shifts to ensure 24 hours coverage. Meanwhile, in the National Police headquarters, a State Police Inspector and two assistants are on hand 24 hours a day.

The images are sent simultaneously to the headquarters of both the national and municipal police forces. The National Police Headquarters can then send the images to the judicial authorities as items of evidence. In total, a dozen operators drawn from the national police, municipal police and *Carabinieri* consult images, which cannot be shared in real time with other services. Only agents of the judicial police can access the saved images, with the authorisation of a judge. To view the images, not only authorisation but also physically the key is needed. However, only the system manager has permission to consult the recordings and must use a specific access key.

Scope

In all these Member States, the scope of the use of video-surveillance technologies is crime prevention.

France

In France, *vidéoprotection* is built to record what happen in public area in order primarily to prevent[124] and then to investigate offences, whether serious or not. In fact, this instrument has been recently

[121] *ibid.*, pp.184-185.

[122] s. 26(2)(a)/1(2)(a) RIPA 2000, defining directed surveillance.

[123] art. 6(7) Law 38/2009.

[124] Law 125/1995 as amended by *Ordonnance* 351/2012.

extended to judicial investigation. The government announced that video-protection is an important component of urban safety policies. If video-protection was developed originally to fight against common offences,[125] the anti-terrorism context mainly justified further development and multiplication of *vidéoprotection*. As mentioned above, specific provisions exist in the code (an actual separate section) in relation to video-surveillance for the prevention and investigation of terrorism. These derogatory provisions grant more powers and more margin of manoeuvre to the authorising[126] (larger number of circumstances justifying the installation) and executing authorities.

There is no special offence motivating the use of video-protection but the transmission and recording images collected by this system are submitted to various conditions depending on the criminal context; the level of powers granted to authorities depends on the type of offences concerned. Terrorism extends the permitted space of video-protection to the immediate vicinity of buildings and facilities by other legal persons and places likely to be exposed to acts of terrorism.[127] It can be carried out in exceptional circumstances and under strict conditions.

Italy

In Italy**,** video-surveillance have diverse purposes, some of which can be grouped into the following categories: "(1) protection and integrity of individuals – including urban security; public order; public bodies' prevention, detection and/or suppression of offences; streamlining and improving publicly available services also in order to enhance user safety; (2) protection of property; (3) detecting, preventing and controlling breaches of the law; (4) gathering of evidence."[128]

As in the other countries, the use of video-surveillance in urban transports (where it was most importantly installed at the beginning) has rapidly spread because of the terrorist threat.[129] Its purpose remains the prevention of more petty crime but its use is extended to the prevention of and information gathering in relation to more serious offences, including terrorism.[130]

The preventive aspect is less clear. Citizens' satisfaction is nonetheless high, even if the system does not meet all the expectations. A greater surveillance gives citizens a feeling of greater protection, with the possibility of a more rapid response from the police. The displacement effects (relocation of criminal activities) are not quantifiable, due to a lack of reliable statistics. However, a research study claims that the message given to the public opinion was "+ video-surveillance = + prevention of offences = - criminality".[131]

The United Kingdom

In the United Kingdom**,** video-surveillance is used for a number of monitoring and surveillance purposes, but is mainly used for security purposes. The development of CCTV was felt by many to be

---

[125] art.4 Law 73/1995. Priority tasks of the police are for example the fight against urban violence and the control of public order.

[126] *e.g*. larger number of circumstances justifying the installation; the *Préfet* may authorise an installation before that the commission has given his advice.

[127] art. L223-1 and art. 223-2 CSI.

[128] Garante per la Protezione dei dati personali , *Video surveillance*, Decision (8 April 2010).

[129] *I sistemi di videosorveglianza 2, Videosorveglianza e privacy: quadro normativo, casistica e aspetti tecnici*, Provincia autonoma di Trento, Transcrime, Inforsicurezza (4 May 2006) p.49

[130] F. Caprioli, "Nuovamente al vaglio della Corte Costituzionale l'uso investigative degli strumenti di ripresa visiva", (2008) 3 Giur Cost 1832.

[131] See *I sistemi di videosorveglianza 2*, p.11.

a major breakthrough in crime prevention. It forms a major part of crime prevention strategy in the United Kingdom and is often used as important evidence in court trials and in the identification of suspects.[132] CCTV may have other deterrence and safety-related benefits, although these are debated. However, its multiplication in the country is considered as an erosion of civil liberties.

Duration

With regard to the duration, two issues are of importance. On the one side, how long the authorisation given by the authority to deploy the video-surveillance system lasts; and, on the other side, how long the information gathered by the video-surveillance device can be retained for.

Duration of the installation

Concerning the length of deployment, only in France, the installation of video-surveillance devices lasts only to a limited amount of time: 5 years renewable. By contrast, in Italy and the United Kingdom, there is no duration limit to the deployment.

Duration of the retention of information gathered by video-surveillance

On the second issue, the situation of the Member States varies broadly. In all of them, information can be retained until they are no longer necessary. Besides, some jurisdictions provide for specific delays.

France

In France the authorisation prescribes the duration of retention of images within one month after the transmission or access to them, without prejudice to the necessity of their conservation for the needs of the criminal proceedings.[133] Except in case of investigation of *flagrante delicto*, a preliminary investigation and an *information judiciaire*, the retention of images may not exceed one month.[134] If the conditions of urgency and of exposure of the risk of terrorist acts are present, video-protection is installed for four months[135] and the renewal is possible after a consultation of the *Commission départementale de vidéoprotection*.[136]

Italy

In **Italy,** concerning the video-surveillance devices installed by municipalities for public order purposes, the local and national Police can view the encrypted images and keep them for up to seven days until their destruction except if the information is subject to special needs for further storage.[137] However, the duration can be extended in places particularly exposed to terrorist threat up to thirty days.[138] In cases where video-surveillance systems had been installed (*e.g.* by private individuals or companies) for other purposes than public order, data may be retained for a maximum of 24 hours.

---

[132] Unlike the interception of telecommunication, which cannot be used as evidence at trial .

[133] art. L252-3 CSI

[134] art. L252-5 CSI

[135] art. L223-4 CSI

[136] art. L223-5 CSI.

[137] art. 6(8), Law 38/2009. In cases where video-surveillance systems had been installed (*e.g.* by private individuals or companies) for other purposes than public order, data may be retained for a maximum of 24 hours.

[138] Garante per la protezione dei dati persnali, *Prescrizioni per la videosorveglianza presso i siti di interesse culturale maggiormente esposti alla minaccia terroristica* (12 March 2009).

The United Kingdom

Finally, in the **United Kingdom,** an indication on duration is provided in a non-statutory instrument, *i.e.* a code of practice. The indication is moreover extremely vague. According to the Code of practice, "[y]ou should not keep images for no longer than strictly necessary to meet your own purposes for recording them. On occasion, you may need to retain images for a longer period, where a law enforcement body is investigating a crime, to give them opportunity to view the images as part of an active investigation."[139] An example of duration is given, "images from a town centre system may need to be retained for enough time to allow crimes to come to light, for example, a month. The exact period should be the shortest possible, based on your own experience."[140]

Installation of video-surveillance

	France	Italy	United Kingdom
Ground 1	Security purposes/public order, especially for areas exposed to a risk of assault and theft but also to a risk of terrorism	Security purposes/public order	Security purposes/public order
Authorisation	Representative of the State in the Department and, in Paris, *Préfet* of police after consulting the *Commission départementale*	Municipalities	Chiefs Constable, Chiefs of the Intelligence and Security Services, Director of Government Communication Headquarters, Director General of the National Criminal Intelligence Service
Duration	5 years renewable	no limit	no limit
Ground 2	In case of emergency		
Authorisation	State in the Department and, in Paris, *Préfet* of police without consulting the *Commission départementale* (informed after)		
Duration	4 months renwable after consultation of the *Commission départentale de la vidéoprotection*		

Retention of information gathered by video-surveillance

	France	Italy	United Kingdom
Ground	public order and investigation of crimes	public order and investigation of	Public order and investigation of any

[139] CCTV code of practice, Data protection, Information Commissioner's Office (revised ed. 2008) p. 14

[140] *ibid.*

		crimes	offences
Authorisation	police officer, prosecutor and judge	law enforcement authorities	law enforcement authorities
Duration	1 month, without prejudice to the necessity of their conservation for the needs of the criminal proceedings; in flagrante delicto, no more than one month	7 days; if gathered for other purposes than public order, retained for max 24 hours	"no longer than necessary"

The comparative analysis validates the second dimension of the first shift tested in this paper. In the three states under scrutiny, video-surveillance was at first introduced by private citizens and companies and then by public authorities (especially at the local level) for public order prevention purposes. The data gathered are now used in the context of the prevention and investigation of serious crimes, including terrorism.

Interplay between intelligence services and law enforcement agencies: Mutual contamination

According to a strict principle of separation, traditionally the activities of intelligence services and police authorities in the prevention and investigation of crime were clearly distinct. In fact, there is a profound difference (at least in general terms) in the specific purposes of the two bodies. The police, in its judicial function, have the task of gathering information in relation to a specific offence for prosecution purposes; intelligence services do not have the objective of investigating offences but rather to recognize threats and to provide intelligence assessments to policy makers. In this framework, intelligence information is mostly secret, whereas police information is subject to scrutiny via cross-examination in court. However, nowadays the distinction is not always so clear, intelligence is also given operational tasks and this leads to a problematic coordination and overlap.[141]

The shift towards prevention in the fight against serious crimes, including terrorism, attributes a greater role to ductile means of intelligence to the detriment of more traditional means of investigation. The current trend leads to an intense and dangerous osmosis and blur between criminal justice and secret investigations (significantly much of the activities of the intelligence falls within the realm of State secret[142]). Intelligence activities and police investigations tend to converge as of their object, scope, means, particularly in relation to offences such as terrorism and organised crime where intelligence is crucial to understand at best the organisational dimensions of complex, widely spread and long-lasting phenomena which threaten national security.[143]

In addition, intelligence must only be accountable in front of the executive. Given the new role of intelligence in public order activities and the investigative domain, the issue at stake is hence that of the relationship, yet to be defined, between intelligence and the judiciary.

---

[141] The distinction of roles and information sharing between intelligence services and law enforcement authorities with a view of preventing an combating terrorism has been highly discussed and let to controversial case-law also in other UE countries such as the Netherlands. See J.A.E Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law? » (2005) 1(1) *Utrecht Law Review* 1.

[142] See, re. Italy, R. Orlandi, "Segreto di Stato e limiti alla sua opponibilità fra vecchia e nuova normativa" (2010) 6 Giur cost 5224; A Pace, "L'apposizione del segreto di Stato nei principi costituzionali e nella legge n.124 del 2007, (2008) 5 Giur Cost 4041.

[143] See R. Orlandi, "Attività di intelligence e diritto penale della prevenzione" and F. Sommovigo, "Attività di intelligence e indagine penale" *in* G. Illuminati, *Nuovi Profili.*

The second shift the authors are testing in this paper is thus the evolution, potentially leading to a blur, of the share of roles, competences and means of intelligence services and law enforcement authorities. The question to explore is whether, and to what extent, the three countries have established structures of coordination/centralisation between intelligence, police and judiciary in particular in the field of organised crime and terrorism in order to manage the overlap of competences and avoid the blur.

France

France constitutes, from a law enforcement perspective, a very effective example of coordination between intelligence services, police, prosecutors and *juges d'instruction* via its centralised investigation and prosecution of terrorist offence and the coordination of organised crime cases in Paris.[144]

Since the first anti-terrorist law in 1986, co-ordination between the various intelligence and police services and the French government has improved with the creation of the *Unité de Co-ordination de la Lutte Anti-Terroriste* and the 14th section of the Parquet of Paris. By contrast, in the field of organised crime, there is no centralisation of prosecutions and trials but only a coordination of investigations.

The new *Direction Centrale du Renseignement Intérieur* (*DCRI*), the French internal intelligence service, is the centralised agency responsible for the preventive and investigative phases. The *DCRI*[145], operational since 1st July 2008, combines law enforcement and intelligence service agents and is meant to monitor, detect and investigate individuals. Thus this service, which can be used by prosecutors and *juge d'instruction* in serious crime investigations, encompasses both police and intelligence agents. Its composition and structure favours the sharing of information both at the prevention and investigation phases between the two services in an effective and rapid manner, leading to the so-called "judiciarisation" of intelligence information.[146]

Such a centralisation offers some advantages as it results in the competent judges and prosecutors being more specialised and in them having more knowledge and expertise in terrorist matters as well as the establishment of closer links with the intelligence services. However, at the same time, it has been considered as a dangerous concentration of very far-reaching powers in the hands of only a few.[147]

Remarkably, no specific rule forbides the use of intelligence (including the information gathered via administrative interceptions) as evidence during criminal proceedings. However, in practice, intelligence services have never used so far the results of administrative interception at trial.[148] Intelligence can always be used as a lead for initiating judicial investigations. Moreover, despite the

---

[144] The French system is currently evolving towards a centralisation of the execution and the consequent use of judicial interception based on the model of the centralised system of administrative interceptions (art. 4 Law 91/73). See *plate-forme nationale des interceptions judiciaires* and *Commission nationale de controle des interceptions de sécurité.*

[145] Gathering of the *Direction de la surveillance du territoire* (DST) and of the *Direction centrale des Renseignements Généraux* (RG).

[146] Interview with P. Caillol, Deputy Director of the *Institut national des hautes études de la sécurité et de la justice* (Paris, 28 November 2012).

[147] L. Caprioli and J.-P. Pochon, "La France et le terrorisme international, Les racines historiques et organisationnelles du savoir policier", round table organised by J. Ferret and A. Wuilleumier, (2004) 55 *Cah. S.I.*, pp. 147-179; FIDH, *Paving the way for arbitrary justice*, (1999) 271(2).

[148] This is probably because the transcription of the interception is only possible for the purpose of article L241-2 CSI (art. L242-5). In addition, the recording is destroyed within ten days (art. L242-6) and the transcription within four months (L 242-3). No article provides for any extension of preservation for judicial purpose. Information from P. Caillol, Deputy Director of the *INHESJ* (22 April 2013).

establishment of central coordination structures, the police sometimes do not trust the intelligence information received because they cannot have access to sources. In the Merah case, the sharing of information between the intelligence services and the police was particularly deficient; Merah was under surveillance by intelligence services but the information was never passed on to the police in order to start an investigation and thus arrest the suspect.[149]

Italy

A similar overlap and blur of competences between intelligences services and police authorities may be seen in Italy in relation to offences which threaten not only individual citizens but also national security. A number of legislative provisions thus increasingly involve intelligence services in public order policies. A good example is that of the Law 155/2005 enabling intelligence services to apply to the prosecutor for an interception warrant where deemed to be necessary to prevent terrorist activities or subversion of the constitutional order *ex* art. 226 *disp. att. CPP*.[150]

Already Law 410/1991 established a general Council for the fight against organised crime, including intelligence service agents with the task of intelligence gathering in relation to any form of subversion by any type of organised group threatening institutions and public life.[151] The intelligence agents had only an obligation to communicate to judicial police forces any information on Mafia organised crime groups.

In addition, the *Agenzia Informativa di Sicurezza Interna* (AISI) – created in 2007 to replace the SISMI – has a specific competence of information gathering in the domain of subversion, terrorism (particularly international terrorism) and organised crime offences. In these domains, a precise distinction of the field of intervention of police and intelligence is particularly complicated.[152]

At the stages of pre-trial and trial, there is no centralisation of powers in the fight against serious offences. However, with a view to favoring effective prosecution of terrorist offences and valid judicial scrutiny of police investigations, a coordination of different cases to share knowledge and information on terrorist networks has certainly been considered fruitful. This has lead to a specialisation of investigating judges, prosecutors and the police. In relation to terrorism cases, during the 1970s and 1980s, informal networks for the prosecutors grew up in order to share information and competences. Judges have often advocated the establishment of coordination between prosecutors who would deal with terrorism offences under the auspices of the National Anti-Terrorism Directorate.[153] In relation to organised crime, judicial and police investigations, as well as preventive actions, are coordinated respectively by the National Anti-Mafia Directorate (DNA) and the Anti-Mafia Investigations Directorate (DIA). The coordination ensures information sharing between judicial authorities and police services among themselves and among each other on all investigations concerning organised crime. The DNA may directly rely upon the DIA in the case of specific investigations. However, the two Directorates do not directly involve members of the intelligence services.

In 2004, a *Comitato di Analisi strategica anti-terrorismo* has been created within the Ministry of Interior to assess any information on international and domestic terrorist threats and thus coordinate any intervention. The agency involves members of police forces, carabineers, guardia di finanza and intelligence services. Law 207/2007 concerning the re-organisation of intelligence services establishes

---

[149] Interview with T. Fragnoli, Procureur, Parquet anti-terrorisme, Tribunal de Grande Instance (Paris, 29 November 2012).

[150] Vervaele, "Special procedural measures and the protection of human rights, General report", *Utrecht L Rev.*

[151] Law 410/1991.

[152] See Law 124/2007, art. 7. More information available at www.sicurezzanazionale.gov.it (accessed 23 May 2013).

[153] G. Melillo and A. Spataro, "Senza la creazione di una Procura nazionale" (2005) 33 Guida Dir 48.

the *Dipartimento delle Informazioni per la Sicurezza* (*DIS*) which also coordinates the exchange of information between intelligence services and police authorities.

For the purpose of improving the cooperation, Law 207/2007 has also introduced art. 118 *bis CPP* so that the Prime Minister may ask to the judiciary information which are relevant to the activities of the intelligence even in derogation to the secrecy of investigations (art. 329 *CPP*). Meanwhile, the judiciary may ask the intelligence services to obtain documents or information relevant to a judicial investigation (art. 256 *bis CPP*).

The United Kingdom

In the United Kingdom, the coordination of law enforcement authorities and intelligence services has been achieved through the creation of dedicated coordinating bodies that have provided a central mechanism for disseminating information and availing inter-agency operations.[154]

The lack of trust between police and intelligence and different counter-terrorism agencies have often hampered an effective information sharing.

The most important interface between the intelligence community and the police departments is the National Criminal Intelligence Service (NCIS). Over the past decade, the Security Service has become more involved in judicial investigations by providing evidence at trials involving terrorist and serious criminal offences.

Within police departments, the link with intelligence services (mostly the MI5) is ensured by Special Branches, having counter-espionage, counter-proliferation, and counter-subversive functions. They constitute the primary instrument to translate intelligence information into operational activities, investigations and prosecutions. Thus Special Branches provide national operational support to the Security Service.

Moreover, in June 2003 the United Kingdom has established a fusion centre, the Joint Terrorism Analysis Center (JTAC), comprised of representatives from eleven government departments relating to international terrorism (*e.g.* Home Office, Police, FCO and Ministry of Defence) and meant to produce finished intelligence for a wide variety of audience. Such a fusion centre aims at the inclusion in the intelligence arena of non-traditional players.

The blur of competences between law enforcement authorities and intelligence services in the country has been favoured by a fundamental shift in policing towards a strategic, future-oriented and targeted approach to crime control - broadly represented in the concept of "intelligence led policing" (ILP) - built around analysis and management of problems and risks, rather than reactive responses to individual crimes (a "forward looking" focus on threats to community safety).[155]

Concluding remarks

The overview of each Member State's response to serious offences of two surveillance technologies identified previously (interceptions of telecommunication and video-surveillance) allows to understand the specificity of each regulatory framework as well as the most important similarities and differences between national regimes in relation to actors involved, the scope and the duration of the two surveillance technologies chosen as case studies in the prevention and investigation phases.

---

[154] P. Chalk and W. Rosenau, " Confronting the Enemy Within", Security Intelligence, the Police, and Counterterrorism in Four Democracies, RAND (2004).

[155] M. Maguire and T. John, "Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK" (2006) 16(1) *Policing and society* 67-85.

In general terms, one can argue that there has been an overall toughening, and a parallel higher curtailment of civil liberties, of the provisions concerning the use of surveillance technologies in the prevention and investigation of serious crime. Indeed, both terrorism and organised crime certainly had a catalysing effect on this development.[156]

As underlined in this deliverable, serious crime has certainly played a catalysing effect on the introduction of derogatory provisions and in the expansion of powers of actors involved in either the authorisation or the execution process of the interception of telecommunications. Primarily introduced for the purpose of preventing and investigating terrorism and organised crime, the scope of these provisions was then extended to cover also other types of crimes of less serious nature. In addition, the comparative analysis validates the hypothesis that video-surveillance was, at first, introduced by the private sector and then by public authorities for public order prevention purposes. The data gathered are now used in the context of the prevention and investigation of serious crimes, including terrorism.

Besides, serious crime has had a catalysing effect in redefining the competences of intelligence services and police authorities leading to an overlap of roles and tasks and potentially a blur. With regards to the interception of telecommunications, the blur is less visible in the United Kingdom than in France or Italy. In fact, in the United Kingdom, there has never been a difference between *ante-delictum*/preventive interceptions (allowing for an involvement of intelligence services and not admissible as evidence at trial) and judicial interceptions (prerogative of the police conducted under judicial scrutiny). The increasing involvement of intelligence services in any kind of interception is thus less remarkable!

However, the blur of competences between law enforcement and intelligence services had the positive consequence of stimulating an increased coordination and sharing of information between the two bodies and the creation of infrastructure to institutionalise this relationship, which enhances the effectiveness and the rapidity of the investigation. There is not yet a well-defined share of competences and a new balance and the three countries are still in a situation of blur and uncertainty. This blur is once again less noticeable in the United Kingdom where the distinction between the phase of prevention and investigation is less important than in the other two countries where the "charge" plays a more important role.

After having examined the use of surveillance technologies for preventive and investigative purposes, it would be interesting to focus on the next phase of criminal procedure, *i.e.* the retention and use of information gathered via surveillance technologies for the prosecution and trial of serious crimes, including terrorism.[157] A huge amount of information is nowadays retained by private companies such as networks and service providers, but also by different CCTV operators. The question is under which circumstances such information can be accessed and used by different actors of criminal procedures (police officers, intelligence services, prosecutors and judges) for the purposes of investigating and prosecuting serious crimes. The question is whether serious crime had a catalysing effect on the increasing use of data retained by telecommunication companies and Internet service providers by law enforcement officials not for preventive but for judicial investigation purposes; and whether data retained were originally only related to serious crime and then expanded to less serious ones.

The retention of data for investigation and prosecution purposes raises the question of the collaboration between public authorities and private companies and what kind of obligations one may impose upon them. An additional question relates to the role of information gathered by intelligence

[156] France developed an anti-terrorist arsenal and centralised its approach as well as increased its use of surveillance technologies (often on the basis of derogatory provisions) such the interception of telecommunications for the purpose of preventing and investigating serious crimes.

[157] See "Comparative paper on data retention regulation in a sample of EU Member States", SURVEILLE Project, *op. cit.*

services within the criminal proceedings in the investigation, prosecution and trial of serious crimes, including terrorism.

Part 2. Comparative law paper on data retention regulation in a sample of EU Member States

Introduction

Since the 9/11 terrorist attacks of 2001, law enforcement agencies have increasingly called for new tools to address a wide range of contemporary crimes in a manageable and cost-efficient manner.[158] Between 9/11 and the London bombings in 2005 the increased threat of terrorism and, to a lesser extent, organised crime resulted in a push for a more flexible (legal) regime to allow the use of various technologies enabling the interception of telecommunications. Since such interceptions reveal the content of personal communications, they are seen as very intrusive in the right to privacy. Instead, the EU's Declaration on combating terrorism, which was adopted just after the Madrid bombings, encouraged the Council to examine measures that dealt with the retention of communication traffic data by service providers. This measure is seen by some as less intrusive than interception.[159] Both traffic data and location data have been considered very useful for investigating the terrorist attacks in Europe.[160]

Before looking at the details of national law, it is necessary to define the concepts under scrutiny. The retention of data refers to the retention of "traffic data and location data and the related data necessary to identify the subscriber or user"[161] to the extent that those data are generated by providers of publicly available electronic communications services or of a public communication network within their jurisdiction in the process of supplying the communications services concerned.[162] Communications data may be defined as the data identifying: who made a communication[163]; who received it; where the communication was made; what communication services were accessed by a user; and how the service were accessed. There exists three types of communications data: traffic data, service use data and subscriber information data.[164] More specifically, the Data Retention Directive applies to the fields of fixed network telephony, mobile telephony, Internet access, Internet email and Internet telephony.[165] Although EU provisions are clearly defining the purpose for which information may be retained, they are however vague with regard to the conditions for the retention and subsequent use of such information.

Member States generally seemed to find data retention to be at least valuable, and in some cases indispensable[166], for preventing and investigating serious crimes.[167] Equally, it is often seen as an

---

[158] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011, p. 25.

[159] European Council, Declaration on Combating terrorism, 25 March 2004.

[160] Preamble 11 Directive 2006/24/EC.

[161] Art. 2 Directive 2006/24/EC.

[162] Art. 3 Directive 2006/24/EC.

[163] In the case of any pre-paid anonymous services, the identification of the subscriber is more difficult. So, the date and time of the initial activation of the service and the cell ID from which the service was activated should be required to have more information.

[164] Art. 5 Directive 2006/24/EC.

[165] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011, p. 12.

[166] The United Kingdom police agency described the availability of traffic data as 'absolutely crucial … to investigating the threat of terrorism and serious crime'. Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011, p.23.

important tool for the prosecution as it can produce evidence to be brought to trial. Some prosecutors even declare that a number of guilty verdicts are almost exclusively based upon such retained data.[168]

This deliverable analyses how data are being retained for the purpose of investigating and prosecuting serious crime, on the basis of the Data Retention Directive, and subsequently used. In this context, the authors test a "catalysing effect" hypothesis. The hypothesis relates to the so-called catalysing effect[169] of serious crime on the increasing use of data retained for the purpose of investigating and prosecuting serious crime by telecommunication companies and Internet service providers by law enforcement officials and intelligence services. It is clearly stated in the preamble that the threat of serious crimes including terrorism is one of the factors motivating the drafting of the Directive.[170]The catalysing effect of serious crime on the use of data retention is amplified by the fact that the Directive leaves a wide discretion to Member States and that the implementing legislation broadens the scope of application of data retention both regarding offences and authorities involved.

In implementing the Data Retention Directive, Member States have often widened the scope of application of certain provisions. Firstly, according to the Directive, access to retained data should be limited to the purposes of investigating, detecting and prosecuting serious crimes only.[171] However, no definition of what constitutes 'serious crimes'[172] was introduced, and as a result the access and use of retained data has been extended to less serious offences in some Member States (*e.g.* Belgium, Italy, United Kingdom). Secondly, the Data Retention Directive allowed Member States to define which 'competent national authorities' may access the retained traffic data, and under which specific conditions.[173] National legislation often gave intelligence services access to retained data, thereby allowing the use of data retention also for preventive purposes.[174]

As a consequence, the Data Retention Directive contributes to the blur of competences between law enforcement authorities and intelligence services in the prevention and investigation of serious crimes[175] as well as to a general shift towards prevention, proactive investigations and intelligence-led

(Contd.)

[167] Conclusions of the Justice and Home Affairs Council, 2477th Council meeting, PRES/02/404, 19 December 2002. It underlines that data are a "valuable tool" in the prevention, investigation and prosecution of criminal offences, in particular organised crime. See also the UK, Malcolm Rifkind, MP (Chairman), Access to communications data by the intelligence and security agencies, Intelligence and Security Committee, February 2013, p. 8.

[168] See *e.g.* interview with B. Michel, Federal Prosecutor (Brussels, 26 February 2013).

[169] See C. Cocq and F. Galli, "The use of surveillance technologies for the prevention and investigation of serious crimes", SURVEILLE Deliverable, D4.1 (October 2012).

[170] See preamble 8 of Directive 2006/24/EC.

[171] Art. 1 Directive 2006/24/EC.

[172] See art. 83 TEU: serious crime concerns the offences "with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis" including terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. However, the UN Convention against Transnational Organised Crime (2000) defines the concept as follows: "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.

[173] Art. 4 Directive 2006/24/EC.

[174] There is no European instrument on the use of surveillance technologies, including data retention, by intelligence services. See also *e.g.* M. Rifkind, MP (Chairman), Access to communications data by the intelligence and security agencies, Intelligence and Security Committee, February 2013, p. 10; in fact, the report considers that "communications data is integral to the work of the intelligence and security Agencies and, certainly in terms of the Security Service, it is used in all their investigations".

[175] Intelligence agencies would generally provide background information and "advance warnings about people who are thought to be a risk to commit acts of terrorism or other threats to national security", but would – unlike law enforcement agencies – not be actively engaged in investigating acts of terrorism. K. Roach, "Secret evidence and its alternatives" *in*

policing within the criminal justice system.[176]This hypothesis is tested within nine EU Member States, namely Belgium, France, Germany, Italy, the Netherlands, Poland, Romania, Spain and the United Kingdom.

For the purpose of the comparative research, national reports were drafted on the basis of a grid of analysis. Semi-structured interviews have been carried out, where appropriate, to complete the black-letter law study and test the main hypothesis with practitioners. These countries have been chosen because of their importance in the fight against terrorism[177] and because they have experienced different histories, including the existence of authoritarian regimes, which may have influenced the development of the domestic criminal justice system.[178] The comparative analysis of the case studies will allow us to highlight potential differences in provisions regulating the retention and subsequent use of information between European Member States with an authoritarian past and Member States without such a past. As such, it can shed light on an initial hypothesis of SURVEILLE, which was that countries that have experienced at various historical phases an authoritarian past (Italy, Germany, Spain, Romania and Poland) may, as a result, have developed more robust fundamental rights safeguards in their data retention procedures. If such a conclusion can be drawn, it will need also to be assessed whether it relates only or mainly to 'new' Member States with an authoritarian past, or also to countries that at an earlier phase had experienced totalitarianism.[179]

The topic is particularly sensitive as data retention may clash with the constitutional traditions (particularly the respect of the right to privacy) of different Member States. This has led to difficulties in the implementation of the Data Retention directive.

National legislative changes since 2011

For the time being, the Data Retention Directive has been fully implemented in all other jurisdictions chosen as case studies for this deliverable (ES, FR, NL, RO, PL, IT, UK). In some of those Member States, provisions on data retention already existed before the implementation of the Data Retention Directive (*e.g.* UK).

(Contd.)

A. Masferrer (ed.), *Post 9/11 and the state of permanent legal emergency. Security and human rights in countering terrorism*, Ius Gentium: Comparative Perspectives on law and justice 14, Springer, 2012, p. 180.

[176] Proactive investigation has been defined as "the prevention of serious crimes that threaten the safety of many citizens, in particular terrorism, and for which reason the traditional criminal investigative functions (evidence gathering) and intelligence investigative functions (the gathering of information about threats to national security for the purpose of prevention) have been merged." M. F.H. Hirsch Ballin, *Anticipative criminal investigation. Theory and counter-terrorism practice in the Netherlands and the United-States*, Springer, 2012, p. 4.

[177] Some of them have experienced terrorism before 9/11 and have a long tradition of countering it; their national legislation has been a point of reference for the EU. More generally, the chosen Member States have significant experience in the fight against organised crime. Another reason for this selection is also to have a sample of States that is representative of: both common law and civil law systems; different criminal procedural systems (accusatorial/inquisitorial/mixed systems); different systems of distribution of competences and of articulation between intelligence and law enforcement bodies (*administrative police* and *police judiciaire*).

[178] While the SURVEILLE Description of Work document did not include a list of countries in the description of Deliverable D4.2, a list of eight countries was included in the description of the corresponding Task T4.2.2, namely Belgium, France, Germany, Ireland, the Netherlands, Portugal, Romania and the United Kingdom. In the course of the research Ireland was replaced by Italy, Portugal by Spain and Poland was added as a ninth country. These changes were made to secure comprehensive comparative coverage and the availability of complete sources.

[179] See K. Hadjimatheou, "Paper on the ethics of data retention distinguishing between democratic and authoritarian regimes", SURVEILLE Deliverable, D4.4 (forthcoming).

In 2011, the European Commission issued an evaluation of the implementation of the Data Retention Directive.[180] That report highlighted that the Directive was not implemented or was only partially implemented in three of the countries under scrutiny: Belgium, Germany and Romania. Since the Commission's evaluation came out, Romania implemented the Directive by Law 82/2012 on 18 June 2012. The Constitutional Court of Romania had ruled in 2009 that the previous law[181] that had implemented the Directive, violated the fundamental right to private life as provided by article 26 of the Romanian Constitution. Therefore, this law had been declared unconstitutional in its entirety.[182] However, the European Commission urged Romania to fully implement the Data Retention Directive within two months[183] and national authorities eventually implemented it.

Two Member States have not yet fully transposed the 2006 Directive: Belgium and Germany.

The German Constitutional Court concluded in May 2010 that the Data Retention Directive violated the Constitution.[184] German authorities have suggested that a "quick freeze" method of data preservation could be an alternative to the mass retention of data. First, on 19 January 2011, the German Ministry of Justice published a report on data retention, in which it encouraged telecommunications providers to 'freeze' the traffic data of the users suspected of offences, as they could be necessary for the investigation of crimes as well as for detecting alleged criminals. Interestingly, the report found no indication that retained traffic data would have prevented serious crimes such as terrorist attacks. It further found that the absence of a data retention regulation did not lead to less crimes being solved since 2010 – to the contrary.[185] Then, on 10 June 2011 Justice Minister Sabine Leutheusser-Schnarrenberger released a discussion paper about the data retention debate in Germany, suggesting a "quick freeze" method in order to replace mass data retention.[186] Under such a procedure, law enforcement authorities and intelligence agencies may require the 'freezing' of specific data relating to a suspect after having obtained a specific order.

After the evaluation report of the Commission came out in 2011, [187] a new debate took place. Despite the fact that 50.000 citizens signed a petition against the Directive, the Commission required Germany to implement it, threatening to launch an infringement procedure before the Court of Justice of the European Union. On 27 January 2012, the Federal Ministry of Justice addressed[188] a report on the effects of the Constitutional Court's decision in 2010 and asserted the need for retention of

---

[180] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011.

[181] Law 298/2008 regarding the retention of data generated or processed by the public electronic communication service providers or public network providers, which was a word by word translation of the EU Directive 2006/24/EC on the data retention was held to be contrary to the fundamental right to private life provided by Art. 26 of the Romanian Constitution, and therefore declared unconstitutional in its entirety.

[182] Constitutional Court of Romania, Decision n°1258 of 8 October 2009, O.J. n°798, 23 November 2009.

[183] European Commission, Data Retention: Commission requests Germany and Romania fully transpose EU rules, IP/11/1248, 27 October 2011; letter n° C(2011) 4111 of 16 June 2011.

[184] Bundesverfassungsgerichtsurteil, NJW 2010, 833; see *e.g.* Shadow evaluation report on Data Retention Directive (2006/24/EC), European Digital Rights, 17 April 2011, p. 8; K. de Vries, R. Bellanova and P. De Hert, "Proportionality overrides unlimited surveillance – The German Constitutional Court judgement on data retention", CEPS, May 2010.

[185] Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung, p. 219, http://vds.brauchts.net/MPI_VDS_Studie.pdf (accessed on 27 August 2012). See also Vorratsdatenspeicherung: Friedrich stellt Studie infrage, focus (27 January 2012), http://www.focus.de/politik/deutschland/vorratsdatenspeicherung-friedrich-stellt-studie-infrage_aid_707678.html (accessed on 27 August 2012).

[186] Quick Freeze/Datensicherung, Bundesministerium der Justiz, http://www.bmj.de/SharedDocs/Reden/DE/2011/20110125_rechtspolitischer_Neujahrsempfang.html?nn=1463642 (accessed on 22 April 2013).

[187] Evaluation report on the Data Retention Directive, COM(2011) 225 final, 18 June 2011.

[188] On the basis of a study carried out by Max Planck Institute.

communication traffic data for law enforcement and security purposes. Later in March, the Ministry of Justice announced the launch of a cabinet study in order to analyse further the "quick freeze" option of retaining traffic data. After having reiterated its implementation request, the Commission officially opened an infringement procedure against Germany in May 2012.[189] However, since then, there have been no further legal developments on the matter.

Belgium has also only partially implemented the Directive, and as a result it has been subject to legal action by the Commission. In particular, Belgium has not implemented the provision concerning the duration of the retention. In fact, there has been intense discussion in Belgium about the time a service provider would need to retain data. NGOs, communications services and Internet providers were not only against the Directive because of its implications for the right to privacy, but they also argued that the period of retention should not be enshrined in secondary legislation (an *Arrêté Royal*), but in a law. That is the reason why the adoption of the *Arrêté Royal*, which should have specified how long data would be retained, in application of Law 2010 MRD/BIM (*méthodes de recueil des données par les services de renseignement et de sécurité)* has been delayed. However, very recently, the Council of Ministers agreed on a draft legislation and a draft royal decree aiming to fully implement the Data Retention Directive. [190] These drafts should be discussed in Parliament soon in order to comply with all requirements of the Directive.

Data retention vs. data preservation

The data retention, as provided for by the Data Retention Directive, requires operators to retain data, excluding the content, generated or processed as a result of activities of all users of operators' communications or network services so that they can be accessed by State authorities and used for public order purposes when necessary and lawful.[191]

An alternative method is known as expedited preservation of retained data or "quick freeze". Data preservation only requires preserving specific data either in relation to a specific person or in relation to specific offence. It refers to situations where a person or an organisation (which may be a communications service provider or any physical or legal person who has the possession or control of data) is required by a State authority to preserve certain data only from loss or modification for a specific period of time.[192] Data preservation therefore requires that data already existing in a stored form be protected from external factors that would cause them to be deleted or their quality or condition to change or deteriorate. Preserved data or copies of those data may be accessed and used for legitimate purposes by authorised persons defined by national legislation. This method is considered as less intrusive into the right to privacy than data retention. Data retention involves an undifferentiated storage of data while the storage by the data preservation is more specific and only concerns certain data. In Germany, data preservation has been preferred over data retention for this reason. However, the Commission has made clear that data preservation as is currently being discussed in Germany would not amount to a full transposition of the Directive.[193]

---

[189] Data retention: Commission takes Germany to Court requesting that fines be imposed, 31 May 2012, http://europa.eu/rapid/press-release_IP-12-530_en.htm (accessed on 22 April 2013).

[190] Council of Ministers, Transposition de la directive européenne "conservation des données", Brussels (BE), 29 March 2013: http://www.presscenter.org/fr/pressrelease/20130329/transposition-de-la-directive-europeenne-conservation-des-donnees (accessed on 20 April 2013).

[191] Art.1 Directive 2006/24/EC.

[192] Art. 16 Cybercrime Convention, for a maximum of 90 days.

[193] European Commission, "Data retention: Commission takes Germany to requesting that fines be imposed", Press Release, IP/12/530, 31 May 2012.

The Cybercrime Convention of the Council of Europe requires only data preservation.[194] Therefore, Member States that have also ratified the Convention have the obligation to implement both measures.

At the national level, data preservation provisions apply to any criminal offence in five countries (BE[195], DE[196], FR[197], IT[198], PL[199], RO[200]), while one country limits slightly its scope (NL[201]). Moreover, some are preserving data via a general obligation to protect and secure data from accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure" (ES[202], UK[203]). Germany also provides for a general obligation to protect data against unauthorised access and thus potential alteration.[204] Even if the scope differs from a State to another, it is noteworthy that all States have created legal provisions to implement the EU and Council of Europe requirements even if the methods used are not the same.

Conditions of data retention and access in the different States

The Data Retention Directive requires Member States to ensure that operators respect four principles. "The retained data shall be:

- of the same quality and subject to the same security and protection as those data on the [public communications] network ;
- subject to appropriate technical and organisation measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure ;
- subject to appropriate technical and organisational measures to ensure that they can be accessed by especially authorised personnel only ; and
- destroyed at the end of the period of retention, except those that have been accessed and preserved [for the purpose set down in the Directive]." [205]

---

[194] Art. 16-17 Convention on Cybercrime.

[195] Art. 16 Law (*portant assentiment à la Convention sur la Cybercriminalité*), 3 August 2012. Terminology used: "conservation rapide des données informatiques stockées". Data kept for the time necessary and for no long than 90 days.

[196] Art. 96 Telekommunikationsgesetz (TKG). Data are preserved for commercial purposes because there is no transposition for judicial purposes.

[197] Art. 34 Law 17/1978. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), judicial police, Ministry of Interior are responsible for the preservation.

[198] Art. 247 (1bis) CCP.

[199] Art. 218a and b CCP. Method of preservation is provided into Regulation of the Minister of Justice, 28 April 2004.

[200] Art. 154 CCP and art. 54(1) Law 161/2003, chapter IV Procedural provisions. Before Directive 2006. In urgent and dully justified cases, if there are substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be disposed.

[201] Art. 126ni and 126ui CCP for serious crimes and especially art. 126zja CPP for terrorist purposes. See also art. 67 CPP: in case of suspicion of an offence punishable to imprisonment of four years or more.

[202] Art. 8 Law 25/2007. There is no specific procedure in Spanish Law to preserve data. Moreover, it is noteworthy that data retention and data preservation are translated into the same term "conservación de datos".

[203] Art. 6 Data Retention (EC Directive) Regulations 2009.

[204] §109 TKG.

[205] Art. 5 Directive 2006/24/EC amending Directive 2002/58/EC; Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 15.

Operators are prohibited from processing data retained under the Data Retention Directive for other purposes, provided that the data would not otherwise have been retained.

Belgium has implemented three of these principles but does not explicitly provide for the destruction of data at the end of the period of retention.[206] Italy provides for the destruction of data.[207] France[208] and the United Kingdom[209] have transposed all the four principles.

Legal basis and purpose of data retention

The Data Retention Directive imposed on Member States an obligation for providers of publicly available electronic communications services and public communication networks to retain communications data for the purpose of the investigation, detection[210] and prosecution of serious crime, as defined by each Member State in national law, and sought to harmonise EU regulation on data retention. It amended article 15(1) of the e-Privacy Directive[211] so that the principle of confidentiality it enshrined does not apply to data retention.

Five Member States (DE[212], ES[213], NL[214], RO[215], UK[216]) have defined "serious crime", with reference to a minimum prison sentence, to the possibility of a custodial sentence being imposed, or to a list of criminal offences defined elsewhere in national legislation. Nevertheless, these definitions are often different from one Member State to another. By contrast, four Member States (BE[217], FR[218], IT[219], PL[220]) require data to be retained not only for investigation, detection and prosecution in relation to serious crime, but also in relation to all criminal offences and even for crime prevention purposes, or on general grounds of national or state and/or public security.

---

[206] Art. 6 *Arrêté Royal* of 9 January 2003.

[207] Art. 123 and 126 Data protection Code.

[208] Art. D. 98-5 Code des Postes et des Communications Electroniques (CPCE); art. L-34-1 (V) CPCE; art. 34 Act 17/1978; art. 34-1 CPCE; art. 11, Law 17/1978.

[209] Art. 6 Data Retention Regulation.

[210] Detection could be defined as the fact of the police discovering information about crimes.

[211] Art. 15(1) Directive 2002/58/EC, "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

[212] Art. 100a stop (German Code of criminal procedure).

[213] Art. 1(1) Law 25/2007.

[214] Art. 126 CCP.

[215] Art. 2(e) Law 82/2012.

[216] S. 93(4) Police Act 1997.

[217] Art. 126(1) Law of 13 June 2005 concerning electronic communications.

[218] Art. L.34-1(II), CPCE, Law 64/2006 and Law 669/2009.

[219] Art. 132(1) Data Protection Code.

[220] Art. 180a, Telecommunications Law of 16 July 2004 as amended by art. 1 Act of 24 April 2009.

New stakeholders

The Data Retention Directive applies to 'the providers of publicly available electronic communications services or of public communications networks' (art. 1(1)). Interestingly, because of the cost imposed, providers are searching a new way to reduce the cost imposed to medium and small operators, for example, in organising hosted third-party storage service.221 The United Kingdom does not require small operators to retain data222 because the costs both to the provider and to the State of doing so would outweigh the benefits to the criminal justice system and law enforcement authorities. Other Member States (e.g. NL, PL, ES223) do not specifically differentiate between large and small operators in their legislation. Indeed, while large operators benefit from economies of scale in terms of costs, smaller operators in some Member States tend to set up joint ventures or to outsource to companies that specialise in retention and retrieval functions in order to reduce retention costs. Such outsourcing of technical functions does not affect the obligation of providers to appropriately supervise processing operations and to ensure that the required security measures are in place, which can be problematic particularly for smaller operators.[224] However, the European Commission considered that even if telecommunication providers have had to bear considerable costs, the health of the telecom sector does not seem to be affected by the Directive to any significant degree. Operators' different perceptions may result from differences in implementation. Clearer rules are required, including on State compensation for the cost of data retention.[225]

Duration of retention

Article 6 of the Directive requires the Member States to retain data for periods of not less than six months and not more than two years from the date of the communication. This provision gives important latitude to Member States to decide the duration of retention. However, States do not exceed the period provided for by the Directive. The nationally defined period to retain data differs not only from one Member State to the other but it also depends sometimes on the type of communication. In fact, two Member States differentiate between telephone data and Internet data (IT, NL).

States	Duration
Belgium	Between **1 year and 36 months** for 'publically available' telephone services. No provision for internet-related data.[226]

[221] See *e.g.* in Sweden, the *Stadsnatsforeningen och Stadsnat* is negotiating a hosted third-party storage service for 150 network operators.

[222] Evaluation report on the Data Retention Directive COM(2011) 225 final, p. 9. It is justified by the burden of the cost imposed to them.

[223] However, according to art. 10(4) and (5) of the Spanish Telecommunications Law (linked to Law 25/2007), those operators with no impact in the market might receive a special treatment regarding some general obligations, or even a complete exclusion from such obligations, at the discretion of the *Comisión del Mercado de las Telecomunicaciones*. Recently, the Royal Decree 1619/2012 aims to reduce the cost of small and medium companies with a specific and regulated billing system.

[224] See also "La protection des données personnelles: les petites et moyennes entreprises mettent en garde", EU-logos, 21 February 2013, http://eulogos.blogactiv.eu/2013/02/21/protection-des-donnees-personnelles-les-petites-et-moyennes-entreprises-mettent-en-garde/ (accessed on 15 April 2013).

[225] Cecilia Malmström, "Taking on the Data Retention Directive", SPEECH/10/723, European Commission conference, Brussels, 3 December 2010.

[226] Art. 126(2) Law of 13 June 2005 concerning electronic communications. Because no duration has been implemented in a specific manner. The Arrêté Royal planned to specify the duration has finally not been decided. This is the reason why

France	The period of data retention is of **one year**.[227] Operators and providers take, without delay, all the measures in order to retain, for a duration not exceeding one year, the content of the information accessed by the user. The information must be given to the competent national authorities without delay[228].
Germany	Telecommunications companies store traffic data for commercial purposes up to **six months**[229]
Italy	The period of data retention depends on the different categories of data.[230] Land-line and mobile communication data are retained for **2 years**. Internet access, internet email and internet data are retained for **one year**.
Netherland	Traffic data and subscribers' data in relation to telephone services for **12 months**[231], and traffic data and subscribers' data in relation to Internet access services must be retained for **6 months**[232].
Poland	**One year**[233]
Romania	**Six months**[234]
Spain	**One year**[235]
United Kingdom	**One year** as of the date of the communication[236]

Access to data: authorities and procedure

Most Member States under analysis, both national police forces and prosecutors may access retained data.[237]

States	Competent authorities to access	Procedure
Belgium	Prosecutor, judge (*juge d'instruction*); police[238]; intelligence services[239]	Access must be authorised either by a judge or prosecutor. Upon request, operators must provide, without delay, subscriber data and traffic and

(Contd.)

the Commission sent a formal notice to Belgium, infringement n° 2012/2152. In practice, operators and providers retained data for one year. Prosecutor B. Michel, interview, 26 February 2013.

[227] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 13.

[228] Art. 60-2 CCP.

[229] §97 TKG.

[230] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011, p. 14.

[231] Art. 13.2a(3)(a) Telecommunications Act.

[232] Art. 13.2(3)(b) Telecommunications Act.

[233] "Report on the retention of telecommunications data", Raport dotyczący retencji danych telekomunikacyjnych opracowany przez sekretarza stanu ds. bezpieczeństwa w Kancelarii Premiera Jacka Cichockiego, 8 june 2011. It recommended the shortening of the retention period for telecommunication data to one year, which was implemented at the end of January 2013.

[234] Art. 3(2) Law 82/2012.

[235] Law 25/2007.

[236] §5 Data Retention Regulations 2009.

[237] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 9.

[238] Law of 21 March 2007 (*réglant l'installation et l'utilisation de caméras de surveillance*).

		location data for calls made within the last month. Data for older calls must be provided as soon as possible. The Prosecutor cannot have access to all data relating to telecommunications in the same ways as the *juge d'instruction* (this is in cases where the warrant is initiated by him instead of the JI).
France	Prosecutor[240], police under the prosecutor's warrant after prior authorisation of the judge (JLD)[241]; Minister of the Interior	Police must provide justification for each request for access to retained data and must seek authorisation from a person in the Ministry of the Interior designated by the *Commission nationale de contrôle des interceptions de sécurité*. Requests for access are handled by a designated officer working for the operator. In cases where access is requested by the Minister of Interior, an independent authority the *Commission nationale du contrôle des interception de sécurité* controls the actions carried out by the administrative police.
Germany	Judges[242] can have access to traffic data; Prosecutor[243] in case of emergency; in specific cases, the Federal Network Agency (*Bundesnetzagentur*[244]) (FNA)	The judicial authority gives an authorisation to have access to data. However, according to some specific agreements between the FNA and the operators, the FNA may have access to data without the knowledge of operators[245].
Italy	Prosecutor, judge[246], Police, defence counsel for the defendant or the person under investigation[247]; intelligence services[248]	Access requires a "reasoned warrant" issued by the public prosecutor. Thus, Prosecutor, law enforcement, defence counsel for the defendant or the person under investigation have access to data.[249]
Netherlands	Prosecutor[250]	Access must be given by a warrant of the prosecutor or the investigative judge

(Contd.)

[239] Law 4 February 2010 (*Méthodes de Recueil des Données)*.

[240] Art. 60-1 CPP as modified by the Law 2004/204 of 9 March 2004 and the Law 2007/297 of 5 March 2007.

[241] Art. 6 Law 2004/575.

[242] § 100g StPO.

[243] "Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie", *im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie,* 10.3.2008, p.32, fn.14.

[244] Federal Authority within the scope of the German Federal Ministry of Economics and Technology

[245] § 112(1) TKG.

[246] In Italy, the duration of retention is divided into two periods. In the first period, the Prosecutor may require directly the access, but for the second period the authorisation has to be given by the judge.

[247] Art. 132(3) Data Protection Code ; art. 15 Italian Constitution.

[248] Art. 26 §1 Law 124/2007 only for security purposes.

[249] Art. 132(3) Data Protection Code.

[250] Art. 126ni CCP.

Poland	Police, Border control officers, Treasury Intelligence, Military Gendarmerie, Customs Service, Internal Security Agency, Central Anti-Corruption Bureau, Military Counter-Intelligence Services[251]	Access to data is subject to a written request[252] or an oral request.[253] s. 37 of the Protection of Freedoms Act 2012 requires that local councils obtain judicial approval from a judge before accessing communications data.
Romania	Prosecutor, courts, and State authorities with responsibilities in national security[254], the police (under the supervision of the Prosecutor for data retention)[255]	Requests of the prosecution, the courts and State authorities in charge of national security will be made on the basis of legal provisions[256] and will be transmitted electronically signed with advanced electronic signature based on a qualified certificate issued by an accredited certification service provider. Data are transmitted electronically in Romania[257] in order to avoid any modification of these data.
Spain	Court warrant[258]; director of State Security[259]	Once the judge has issued his/her decision, the prosecutor will be informed[260]; the director of State Security communicates it to the competent judge immediately.[261]
United Kingdom	Serious Organised Crime Agency, the Scottish Crime and Drug Enforcement Agency, Her Majesty's Revenue and Customs, any of the intelligence services and	Access permitted, subject to authorisation by a 'designated person' and necessity and proportionality test, in specific cases and in circumstances in which disclosure of the data is permitted or required by law. Specific procedures have been agreed with operators.

[251] Art. 20c(1) State Police Act, 6 April 1990; art. lOb(1) Border Guard Act, 12 October 1990; art. 36b(1) pt 1 Fiscal Control Act, 28 September 1991; art. 30(1) Military Police and Military Law Enforcement Authorities Act, 24 August 2001; art. 28(1) pt 1 Internal Security Agency and Intelligence Agency Act, 24 May 2002; art. 18(1) pt1 Central Anti-Corruption Bureau Act; art. 32(1) pt 1 Military Counter-Intelligence Service and Military Intelligence Service Act, 9 June 2006; art. 179(3), Telecommunications Law 16 July 2004 as amended by art. 1, 24 April 2009.

[252] The Chief Commander of the Police or the Regional Commander of the Police, or a person they authorised/General Fiscal Control Inspector/ Head of the Customs Service or the Director of the Customs Chamber, or a person they authorised/Chief Commander of the Border Guard or a commander of the Border Guard's division, or a person they authorised/Chief Commander of the Military Police or a commander of the Military Police' division, or a person they authorised/ the Head of Internal Security Agency, Central Anti-Corruption Bureau, Military Counter-intelligence Service or a person authorised by that authority.

[253] An officer of authorised agency holding a written authorisation issued by an appropriate senior official in the organisation.

[254] Art. 16 Law 82/2012.

[255] Art. 18 Law 82/2012.

[256] Art. 3, 15(1) and 16 Law 82/2012.

[257] Art. 16 Law 82/2012.

[258] Spanish law 25/2007; See STS 1330/2002, 16 July; STC 123/2002.

[259] Art. 579(4) CCP: i) emergency cases and, ii) investigations of organised crimes, terrorism or rebels.

[260] Art. 306 LECr (CCP).

[261] The judge has then seventy-two hours to revoke or confirm the authorisation. Likewise, communications' interventions of prisoners can be authorised by the Director of the prison, who will later inform the competent judge, called *Juez de Vigilancia Penitenciaria*. See SSTC 106/2001, de 23 April y 128/1997, 14 July.

	some other public authorities[262]; intelligence services [263]	

The access to data retained by operators or providers located outside the EU area follow specific procedures. A request for mutual legal assistance or a judicial decision is the only way to obtain these data.[264]

Scope of data retention and access

The retention applies to the source of communications[265], the destination of communications, the data, time and duration of communications,[266] type of communications, user's[267] communication equipment or what purports to be their equipment, and, finally, the location of mobile communication equipment[268]. The different Member States include these elements in their implementing legislation. However, the grounds on which the access to data is allowed are different. Some States, only permit access for the purpose of pending proceedings (PL[269], ES[270]), while other governments allow access for the much broader purpose of preventing or detecting crime or of preventing disorder, or in the interests of public safety (serious crimes and security purposes) (BE[271], DE[272], UK[273]). In any case, each request to access data or images must be justified.

---

[262] S. 25 RIPA 2000.

[263] S. 7 Data retention Regulation and 22 RIPA.

[264] See Convention on mutual assistance in criminal matters between the Member States of the European Union, O.J.C. 197, 12 July 2000, 29 May 2000 ; Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member Statesof the European Union, 18 December 2006 ; see also Council of Europe, Rapport sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale, 2002. At the national level, Draft Communications Data Bill Joint Committee (UK), Juridictional issues, Requests addressed to overseas CSPs, 11 December 2012, §231; art. 694 to art. 695-9-49 french CCP.

[265] Art. 2 Directive 2002/58/EC. See 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

[266] 'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

[267] 'User' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.

[268] 'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

[269] Art. 18(6) *Act on providing services by electronic means.* The report on the retention of telecommunications data already mentioned (n.77) recommends a limitation of the scope for the possibility of using such data only to prosecution of serious offences and special cases specified by law. Such provisions should apply only to offences subject to the imprisonment of minimum 3 years. The limitation recommended in the proposal, as applied, observed Panoptykon Foundation, does not solve the problem. In practice it allows to obtain telecommunication data in cases of offences that are not of a 'serious nature', such as the one defined in art. 290 PC - appropriating fallen trees in a forest.

[270] Spanish law 25/2007 permits access to law enforcement authorities as long as it is for the investigation of a serious crime.

[271] Art. 19/1 Law 2010 MRD.

[272] Art. 100a and g StPO, art. 113 TKG.

[273] S. 7 Data retention Regulation and s. 22(2) of RIPA.

Role of retained data as evidence in the criminal justice system

In some cases, data that needs to be retained under the Data Retention Directive has enabled the construction of trails of evidence leading up to an offence.[274] Retained data are used to detect, or to corroborate other forms of evidence on the activities and links between suspects. Location data has been used, both by law enforcement and defendants, to exclude suspects from crime scenes and to verify alibis. This evidence can therefore remove persons from criminal investigations, thereby eliminating the need for more intrusive inquiries, or leading to acquittals at trial.[275]

Data that needs to be retained under the Data Retention Directive has been essential in the investigation of a number of serious crimes.[276] In Belgium, for example, one may refer to the 2008 conviction of the perpetrators of a so-called tiger kidnapping[277] of an employee of Antwerp criminal court, in which location data linking their activities in three separate towns was decisive in convincing the jury of their complicity. In a case of a motorcycle-gang related murder in 2007, location data from the offenders' mobile phones proved that they were in the area when the murder took place and led to a partial confession.[278] In Belgium and in the United Kingdom, certain crimes involving communication over internet can only be investigated via data retention: for instance, threats of violence expressed in chat rooms often leave no trace other than the traffic data in cyberspace. A similar situation applies in the case of crimes carried out over the telephone. For example, in Poland, a case of fraud against elderly persons in late 2009/early 2010 has been carried out by means of telephone calls, where perpetrators pretended to be family members in need of loans; they could only be identified through retained telephony data.[279]

Secondly, there have been cases for which, in the absence of forensic or eyewitness evidence, the only way to start a criminal investigation has been to access and analyse retained data. In Germany, there was the example of the murder of a police officer, where the assailant had escaped in the victim's vehicle, which he then abandoned. It was possible to establish that he had then telephoned for an alternative means of transport. There was no forensic or eyewitness evidence as to the identity of the murderer, and the authorities were dependent on the availability of this traffic data to enable them to pursue the investigation. In cases of internet-related child sexual abuse, data retention has been indispensable to successful investigation.[280] On the EU level, the effectiveness of Operation Rescue

---

[274] C. Goemans and J. Dumortier, "Mandatory retention of traffic data in the EU : possible impact on privacy and on-line anonymity", Digital Anonymity and the Law, series IT & Law/2, T.M.C. Asser Press, 2003, p 161-183 ; interviews with different actors of the criminal justice system in Belgium, France, the United Kingdom.

[275] *Ibid.* ; This was claimed in DE, PL and the UK, according to the Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 23.

[276] Council of the European Union, Answers to questionnaire on traffic data retention, 11490/1/02 CRIMORG 67 TELECOM 4 REV 1, Brussels, 20 November 2002. Q7: How would you rate the solution of creating an instrument on traffic data retention for law enforcement purposes at a European level? For instance, Belgium declared that "data retention being a useful tool for investigating cybercrime, as well as serious crime involving the use of a computer, the general principles of data retention should be determined in an EU instrument"; Greece considers the creation of such a legal tool to be important, useful and essential; the United Kingdom, "to resolve these issues on a European basis would be very useful". Cecilia Malmström, "Taking on the Data Retention Directive", SPEECH/10/723, 3 December 2010.

[277] The kidnapping of a person in order to compel him/her or a third person to commit another crime.

[278] National Policing Improvement Agency, United-Kingdom, *The journal of Homicide and Major Incident Investigation*, vol.5, issue 1, Spring 2009, pp. 39-51.

[279] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 24. See also European Parliament, Parliamentary questions, Juozas Imbrasas (EFD), the application of preventative measures to combat telephone fraud, 19 June 2012

[280] See *e.g.* the debate in Data retention as a tool for investigating internet child pornography and other internet crimes, Hearing before the subcommittee on crime, terrorism and homeland security of the Committee on the judiciary house of representatives, serial 112-3, 25 January 2011.

(facilitated by Europol) in protecting children against abuse has been hampered because the non-transposition of the Data Retention Directive has prevented certain Member States from investigating members of an extensive international paedophile network by using IP addresses.[281]

Rules of evidence

Data retention is not only useful for investigation purposes but also as evidence at trial. Rules of evidence are hence worth exploring. Of interest in relation to the main hypothesis of this paper is also whether and upon which conditions any information gathered by intelligence agencies may be used as evidence.

Comparative approach between the selected Member States

In most countries, the rules of evidence can be summarised according to three principles:

1. The legality of the collection of evidence.

Evidence may only be admitted if legally obtained (BE282, ES283, FR, PL284). This principle may considerably hamper the effect of irregular evidence, i.e. evidence collected in violation of procedural or substantial evidence gathering rules.285 Yet, in some countries, such evidence may be admitted if its irregular nature does not harm the interests of the party (BE286, FR, NL).287 Similarly, where evidence can be cross-examined at trial, irregular evidence may not be excluded if it does not constitute the sole basis of the proceedings (i.e. if corroborating evidence exists).288

2. The freedom in the types of evidence employed[289] (BE[290], DE[291], ES, FR, NL, PL, RO[292], UK)

However, some countries limit the types of evidence, which could be presented at trial by specific rules (DE[293], RO).

---

[281] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 24.

[282] *e.g.* art. 18/3 and art. 18/9 Law 4 February 2010.

[283] Art. 11(1) LOPJ; art. 15 Spanish Constitution.

[284] Art. 170 CCP.

[285] French procedural law distinguishes textual nullities, *i.e.* nullities explicitly provided for in the CCP. See for instance, art. 59(2) CCP concerning formalities prescribed for search and seizure; art 80-1 CCP concerning the late placement under judicial examination; art. 100-7 CCP concerning the interception of telecommunication of a defence lawyer, substantial nullities, *i.e.* nullities decided in a case-by-case basis, codified by art. 171 CCP, which states that 'There is a nullity when the breach of an essential formality provided for by a provision of the present Code or by any other rule of criminal procedure has harmed the interests of the party it concerns' and public order nullities, which concerns irregularities affecting an important public interest.

[286] Cass. 14 October 2003, *Antigone* case; see also, M. Delmas-Marty and J.R. Spencer (eds), *European Criminal Procedures* (CUP, Cambridge, 2006), p. 122.

[287] However, case law often considers that textual nullities are subject to the same requirement. See, ECtHR, *Schenk* v. *Switzerland*, 12 July 1988, 13 EHRR 242. The Court admitted that illegal evidence can be produced and used in court, as soon as it had been discussed in the context of a fair trial.

[288] *e.g.* in BE, Cass. 18 January 1971, Pas. 1971 I. 459; Cass. 10 June 1974, 1974 I. 1040; in the UK, Chp. 2, Part 11, Criminal Justice Act 2003 ; in ES, art. 297 LECr.

[289] Evidence may be supplied in any appropriate form except where the law provides otherwise.

[290] Cass., 27 February 2002, *Pas.*, 2002, p. 598; Cass. 5 March 2002, *Pas.*, 2002.

[291] Art. 261 CCP.

[292] Art. 741 CCP.

[293] Art. 244 (II) StPO.

3. And, its corollary, the discretion of the judge to assess it.[294]

Some States give more liberty to the Prosecutor in the gathering of evidence because only the judge has the discretion to decide whether evidence is illegal or irregular (BE[295], IT[296], UK[297]).

Finally, it is important to note that the gathering of evidence and their presentation at trial must not interfere with the rights of the defence and the right of fair trial.[298]

The exclusion of evidence: irregularity and illegality

Irregularly obtained evidence can be withdrawn from the case file directly by the prosecutor (BE[299], FR, RO) or later in court by the judge (DE, ES[300], NL[301], UK). However, more generally, limitations to the admission of evidence are often confined to public authorities (BE, FR); the judges cannot discard evidence produced by the private parties, defence or others, for the sole reason that it may have been obtained illegally or unfairly.[302]

The judge's task or the jury's task is to assess the probative value of evidence. This task is especially important when the admissibility of evidence is poorly regulated, as is the case for instance in France.[303] In some countries, the court has a discretionary power to reject (*inter alia*) evidence that has been illegally or improperly obtained (NL, UK[304]). Some countries explicitly prohibit the "fruit of the poisonous tree"[305] (ES[306], PL) while others do not (IT[307]).

In fact, the European Court of Human Rights deems the procedure fair if national legislation provides for the opportunity to question the authenticity of the evidence and to oppose its use,[308] including through contradiction in court (BE[309], ES, PL, RO, UK).[310]

---

[294] See *e.g.* M. Delmas-Marty and J.R. Spencer (eds), *European Criminal Procedures*.

[295] Indeed, Belgium agrees that evidence gathered illegally may also be taken into account by the judge. See Cass. 18 January 1971, Pas. 1971 I. 459; Cass. 10 June 1974, 1974 I. 1040.

[296] Art. 192 CPP.

[297] Art. 78-1 Police and Criminal Evidence Act 1984; *R.* v. *Looseley*, Att-Gen's Reference (n°3) [2002] 2 Cr App R 29, relating to entrapment; see also the question of torture considered as an erosion of the right to a fair trial.

[298] *e.g.* in BE, Cass. 14 October 2003, *Antigone* case

[299] Cass., 23 March 2004 (P.040012N), *R.A.B.G.*, 2004, p. 1061; Cass., 12 October 2005, *J.L.M.B.*, 2006, p. 585, *Rev. Dr. Pén.*, 2006, p. 211, *J.T.* 2006, p. 109.

[300] Art. 658 and 659 (I) CCP. See *escritos de calificación provisional.*

[301] Art. 359a CCP.

[302] In France, Cass. crim 28 April 1987, Bull crim n°173. More recently: Cass. crim 27 January 2010, Bull crim n°16 (concerning documents stolen by an employee). Where there is a breach of professional secrecy, the evidence is admissible provided that the breach is necessary to the defence and proportionate to the rights of the parties (Cass. crim 24 April 2007, Bull crim n°108).

[303] C. Ambroise-Castérot, P. Bonfils, *Procédure pénale*, Paris, PUF, 2011, 190f.

[304] S. 78 PACE 1984.

[305] The principle that prohibits the use of secondary evidence in trial that was gathered directly from primary evidence derived from an illegal search and seizure.

[306] STC n°114/1984, 29 November 1984.

[307] According to case law, it could be applied in Italy but the decisions of the judges on this matter are neither frequent nor clear.

[308] See *e.g.* ECtHR, *Lee Davies* v. *Belgium*, 18704/05, 28 July 2009, §42; applied by Cass., *Antigone* case, 14 October 2003.

[309] Cass. 18 January 1971, Pas. 1971 I. 459; Cass. 10 June 1974, 1974 I. 1040.

[310] See *e.g.* ECtHR, 10 March 2009, *Bykov* v. *Russia*, req. n°4378/02, §95.

Role and competences of intelligence services and law enforcement within the criminal justice system

In some countries, public officials (including intelligence services) have the obligation to report crimes and misdemeanours (BE, FR). In this context, the relationship between judicial authorities and intelligence services is becoming more important (ES, IT, FR[311], NL). Information gathered by intelligence services can generally be shared with prosecutorial or judicial authorities in order to open an investigation (BE, DE, ES, FR, NL[312]) but this information cannot always be shown in court. This is the case for instance in France and the United Kingdom.[313]. In France, intelligence is assessed by the Prosecutor, who decides whether the information is admissible to be submitted in Court.[314]

Some countries do not differentiate whether the information is coming from intelligence services or from law enforcement agencies (PL), while other countries (DE, ES) do. This differentiation is explained by the fact that the different weight that intelligence and information gathered by law enforcement agencies could have. It is important to notice that, only in Italy, intelligence cannot be used as evidence at trial. [315]

Procedure for intelligence to become evidence

The centralisation, coordination and exploitation of intelligence is increasingly organised and institutionalised (*e.g.* DE, ES, FR, IT[316]).

For instance, France constitutes, from a law enforcement perspective, a very effective example of coordination between intelligence services, police, prosecutors and *juges d'instruction* via its centralised investigation and prosecution of terrorist offence and the coordination of organised crime cases in Paris.[317] The national and central organisation that the *DCRI*[318] is, by its composition - law enforcement and intelligence service agents – and its structure favours the sharing of information between the two services in an effective and rapid manner, leading to the so-called "judiciarisation" of intelligence information.[319] Such a centralisation offers some advantages as it results in the competent judges and prosecutors being more specialised and in them having more knowledge and expertise in terrorist matters as well as the establishment of closer links with the intelligence services.

In Germany, legislative and institutional reforms occurred to improve the coordination between the two bodies, including the Act on Joint Databases,[320] which promotes the collaboration of the

---

[311] M. Trévidic, parliamentary committee of inquiry, "Fonctionnement des services de renseignement", National Assembly, 14 February 2013.

[312] HR 5 September 2006, NJ 2007, 336.

[313] A. Masferrer (ed.), *Post 9/11 and the State of Permanent Legal Emergency. Security and Human Rights in countering Terrorism*, p. 180-182.

[314] M. Trévidic, parliamentary committee of inquiry, "Fonctionnement des services de renseignement", National Assembly, 14 February 2013.

[315] *e.g.* arts. 203 and 240(2) CPP.

[316] Art. 2 Decree 2008/609.

[317] The French system is currently evolving towards a centralisation of the execution and the consequent use of judicial interception based on the model of the centralised system of administrative interceptions (art. 4 Law 91/73). See *plate-forme nationale des interceptions judiciaires* and *Commission nationale de controle des interceptions de sécurité.*

[318] Gathering of the *Direction de la surveillance du territoire* (DST) and of the *Direction centrale des Renseignements Généraux* (RG).

[319] Interview with P. Caillol, Deputy Director of the *Institut national des hautes études de la sécurité et de la justice* (Paris, 28 November 2012).

[320] *Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des*

intelligence services and police, and attempts to improve the exchange of information. The database contains personal data of members or supporters of a terrorist organisation and their contacts, suspected members or supporters of a group that supports a terrorist association, extremists who are ready to or tend to use violence and their contacts.[321] With this database, the principle of the separation of police and intelligence services, the German *Trennungsprinzip*[322], is further weakened. Intelligence and police forces now share the same data.[323]

Some intelligence services can act in, for instance, intercepting telecommunication, requiring retained data without an authorisation by a judge and are not subject to any form of judicial scrutiny (FR, IT, NL, UK), which has constituted a matter of concern in certain countries.[324]

Depending on the country, intelligence obtained by administrative warrants (administrative police and intelligence services) may be officially recorded in a statement (BE[325], FR, NL[326]) in order to be presented as evidence at trial. This is a kind of "laundering of administrative information" in the sense that it integrates administrative gathering of information by the intelligence services and administrative police primarily without any control by the judiciary, into the judicial procedure.[327] In some countries, evidence can only be disclosed in court so there is no specific procedure to be followed beforehand (DE, NL, PL[328], ES, UK[329]).

(Contd.)

Bundes und der Länder (Gemeinsame-Dateien-Gesetz), 22 December 2006, *BGBl*. I, at 3409; a thorough discussion of the law is provided by Roggan and Bergemann (2007).

[321] §2 first sentence, sub-paragraphs (1a) - (3).

[322] Principle installed after World War II as a reaction to the abuses of power by the formerly centralised "secret State police", the Gestapo. See T. Würtenberger, "Das Polizei- und Sicherheitsrecht vor den Herausforderungen des Terrorismus" *in* J. Masing and O. Jouanjan (Hg.), *Terrorismusbekämpfung, Menschenrechtsschutz und Föderation*, 2008, s. 27-48; A. Oemichen, *Terrorism and anti-terror legislation: the terrorised legislator? A comparison of counter-terrorism legislation and its implications on human rights in the legal systems of the United Kingdom, Spain, Germany and France*, Intersentia, School of Human Rights Research series, vol. 34, 2009, p. 267 ff.

[323] With, for instance, the different national platforms such as the Gemeinsames Internet-Zentrum, the Gemeinsame Analyse- und Strategiezentrum illegale Migration, the Nationale Cyber-Abwehrzentrum and recently the Gemeinsames Extremismus- und Terrorismusabwehrzentrum; see R. Warnes, *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, chp. V Germany, ed. B. A. Jackson, RAND, 2009, p. 101.

[324] In France, this possibility offered by Law 2006/64 has been criticised: Prosecutor for the *Cour de Cassation* Jean-Louis Nadal considers it is "indispensable […] que la phase […] de recueil des preuves soit toujours effectuée sous le contrôle de l'autorité judiciaire". J.-L. Nadal, Speech pronounced for the formal hearing of the Beginning of the year of the Cour *de Cassation*, Paris, 6 January 2006, http://www.courdecassation.fr/publications_cour_26/rapport_annuel_36/rapport_2005_582/deuxieme_partie_discours_585/audience_solennelle_7798.html (accessed on 1 February 2013)

[325] Art. 19/1 Law 1998 on intelligence services. C. Constit., *Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité* (art. 2, 3, 10, 14 à 18 et 35 à 38), 2011-145, n° 4955-5014, 22 September 2011. A *procès-verbal non-classifié* written by the President of the administrative commission in charge of monitoring specific and exceptional methods of data gathering by intelligence and security services can be transmitted. However, the Commission does not send a lot of PV's to the prosecutor and this could not be the main form of evidence. (Interview of Prosecutor B. Michel, Federal Prosecutor Office, Belgium, 26 February 2013).

[326] Art. 36- 38 Act on Intelligence and Security Services 2002.

[327] It is also called the "judicialisation" process of evidence.

[328] Principle of immediacy, art. 207 CCP.

[329] A. Masferrer (ed.), *Post 9/11 and the State of Permanent Legal Emergency. Security and Human Rights in countering Terrorism*, p. 181; see also, C. Walker, *Terrorism and the Law*, OUP, 2011, pp. 110-112.

Assessment of evidence: prosecution and trial

Retained data as evidence

Data may be disclosed on different grounds but mainly in relation to whether proceedings, criminal or not, are pending. However, in certain countries (*e.g.* in PL, RO, UK), retained data may be accessed by a larger number of authorities and also for purposes other than investigation.

In order for the prosecutor and judge to assess the probative value of retained data, the original evidence has to be presented: a copy of the document being less valuable. However, the fact of having only a copy does not always prevent its admissibility (UK[330]). Some countries (*e.g.* RO) are working towards the electronic transmission of retained data, in order to avoid any alteration of the original data. In the United Kingdom, the judge assesses the gathering of evidence and may direct the jury on the value they should attach to it or exclude the evidence in consideration of it being unfairly obtained and prejudicial to the Defendant.

It may not always be possible to evaluate the impact of retained data on the basis of the success of criminal investigations and prosecutions, because courts assess all evidence presented to them and rarely find that a single piece of evidence is conclusive (*e.g.* BE). However, some prosecutors have indicated that cases have been prosecuted and decided almost solely on the basis of data retained.[331] In The Netherlands, for instance, from January to July 2010, historical traffic data has been a decisive factor in 24 court judgments.[332] In the United Kingdom, there are data that sought to quantify the impact of data retention on criminal prosecutions; for three of its law enforcement agencies, retained data was needed in most if not all investigations resulting in criminal prosecution or conviction.[333]

Intelligence

As already explained, in some countries, the prosecutor assesses all evidence, including intelligence, in order to determine the relevance of this information as potential evidence at trial (BE[334], DE, FR[335], RO[336], UK). In some countries, intelligence must always be corroborated by other evidence (BE[337], ES[338]); it does not have any evidentiary value if it is presented as sole source of evidence.

Evidence is also assessed in court. For instance in Romania, all elements have to be disclosed in court in order to be taken into account by the judge.[339] Intelligence is then taken into account by the judge,

---

[330] CCTV information, CCTV Advisory Service, http://www.cctv-information.co.uk/i/Digital_Images_as_Evidence (accessed on 4 February 2013).

[331] *e.g.* interview with the Prosecutor B. Michel (BE), (Brussels, 26 February 2013).

[332] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p.25.

[333] *Ibid.*

[334] *e.g.* art. 29 CCP.

[335] M. Trévidic, parliamentary committee of inquiry, "Fonctionnement des services de renseignement", National Assembly, 14 February 2013.

[336] Art. 7 CCP.

[337] Art. 19/1 §4 Law 2010 MRD. C. Constit., *Loi du 4 février 2010*.

[338] Faustino Gudín Rodríguez-Magariños, "La pre Raquel Castillejo Manzanares sunta prueba pericial de inteligencia: análisis de la STS de 22 de mayo de 2009", *La Ley Penal*, n°64, Sección Jurisprudencia aplicada a la práctica, October 2009, p. 11.

[339] SN judgment of 20 February 2002, V KKN 586/99, Prok. i Pr. 2002, supplement "Orzecznictwo", n°11, item 10, LEX 53048.

but it is not a decisive element (BE, DE, ES[340], FR, NL[341], RO[342]). The judge may even decide not to consider such evidence at all (ES[343], RO). In some countries, evidence presented by police agencies has a higher value (ES[344]) compared to evidence provided by intelligence agencies.

Due to the sensitive nature of intelligence, a number of Member States created specific disclosure procedures in order for this information to be admitted as evidence in court (IT[345], UK[346]). In Italy, evidence is excluded but disclosure may be requested on specific grounds and it has to go through a specific procedure. Under this kind of procedure, the trial judge may order that intelligence should not be disclosed or should only be disclosed to the accused in a written form. The judge may require a full disclosure at some later stage in the proceedings if that is necessary to ensure the fairness of the trial. If the prosecutor is not in a position to disclose the material, the case may be closed (UK, IT). Finally, it is important to note that all national judges still have to give specific reasons for their decision, no matter whether the evidence presented in court has been gathered through intelligence services or law enforcement agencies.

Implications of data retention for fundamental rights

Protection of privacy vs. intrusiveness

European framework on privacy

Data retention interferes with the rights to privacy and the protection of personal data, which are fundamental rights in the EU[347]. Such intrusiveness must be 'provided for by law and respect the essence of those rights, subject to the principle of proportionality'[348], and justified as necessary and meeting the objectives of general interest. This means that any limitation must[349] (1) be formulated in a clear and predictable manner; (2) be necessary to achieve an objective of general interest or to protect the rights and freedoms of others; (3) be proportionate to the desired aim; and (4) preserve the essence of the fundamental rights concerned.

Moreover, article 8(2) ECHR recognises that interference to a public authority with a person's right to privacy may be justified as necessary in the interest of national security, public safety or the economic

---

[340] STS 31.03.2010; Raquel Castillejo Manzanares, 2012, p. 4.

[341] Art. 359a CCP.

[342] Art. 410 CCP.

[343] Faustino Gudín Rodríguez-Magariños, "La presunta prueba pericial de inteligencia: análisis de la STS de 22 de mayo de 2009", *La Ley Penal*, No 64, Sección Jurisprudencia aplicada a la práctica, October 2009, 10-11.

[344] Raquel Castillejo Manzanares, 2012, p. 6.

[345] When a statement relates a State secret, the court shall inform the President of the Council of Ministers, asking that it be given confirmation. See also art. 256 §3 CPP.

[346] Public interests in UK Courts, http://publicinterest.info/public-interest-immunity (accessed on 11 February 2013); see *Regina* v. H. *and C.*, conjoined appeal, Court of Appeal (Criminal Division), UKHL 3, 2004, §18; A. Masferrer (ed.), *Post 9/11 and the State of Permanent Legal Emergency. Security and Human Rights in countering Terrorism*, p. 193.

[347] Art. 7 and 8 of the Charter of Fundamental Rights of the European Union (O.J. C 83, 30 March 2010, p. 389) guarantees everyone's right to the "protection of personal data concerning him or her". Art. 16 TFEU enshrines everyone's right to the "protection of personal data concerning them".

[348] Art. 52(1) Charter for Fundamental Rights.

[349] Commission's Fundamental Rights Check-List for all legislative proposals in Commission Communication COM (2010) 573/4, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'.

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.

However, the ECtHR also leaves room for discretion by national courts in the admission of evidence, in accordance with the principle of subsidiarity.[350] Where the investigation relies on unlawfully obtained evidence the Court will verify whether the "unlawfulness" in the domestic terms did not coincide with the "unfairness" in the autonomous terms of the Convention and it would further verify whether the applicant had an opportunity to raise the matter before the domestic courts.[351]

Hence, subsequent case law of the European Court of Justice and the ECtHR has developed the conditions that any limitation on the right to privacy must satisfy. [352] These judgments are of relevance for whether the Directive should be amended, particularly in terms of the conditions for access and use of retained data.

Article 15(1) of the e-Privacy Directive and the recitals to the Data Retention Directive reiterate these principles underpinning the EU's approach to data retention. However, article 11 of the Data retention Directive restricts such these provisions because it specifies that this article 15(1) is not applicable to the Directive. This means that the intrusiveness provided for by the Data Retention Directive is not subject to such a legal framework.[353]

National authorities and Data Protection Acts

Most countries have established data protection authorities that are responsible for the protection of data, such as those that are required to be retained by the Data Retention Directive as part of a national Data Protection Act.

States	Authorities	Acts
Belgium	Commission for the protection of privacy (Commission de la protection de la vie privée)	Law on the protection of privacy with regard to the processing of personal data, 08 December 1992
France	National Commission of security interceptions and the Departmental Commission of video-surveillance	Law 17/1978 on computers, databases and freedom
Germany	Federal Commissioner for data protection and freedom of information	Federal Data Protection Act (*Bundesdatenschutzgesetz*)
Italy	Garante della Privacy	Code of privacy

[350] ECtHR, 6 December 1988, *Barbera, Messegue and Jobardo* v. *Spain*, serie 4, n°146, §68; ECtHR, 19 February 1991, *Isgro* v. *Italy*, §31; 5 November 2002, *Allan* v. *U.-K*; A. Cammilleri-Subrenat, R. Prouvèze and I. Verdier-Büschel, *Nouvelles technologies et défis du droit en Europe, L'imagerie active au service de la sécurité globale*, coll. Travaux de droit international et européen, Bruylant, Bruxelles, 2012, p. 83.

[351] ECtHR, *Schenk* v. *Switzerland*, §§47-51; *Heglas*, §§89-93.

[352] See e.g. *Klass and others* v. *Germany*, 6 September 1978, §§ 49-50, serie A n°28 ; *Weber and Saravia* v. *Germany* (dec.), 54934/00, § 94, ECHR 2006-XI; *Liberty and others* v. *United Kingdom*, 58243/00, § 62, 1 July 2008 ; *Uzun* v. *Germany*, 35623/05, 2 September 2010.

[353] Because the national provisions vary considerably on the requirement of article 15(1), is does not apply by itslef to the data retention Directive. However, article 8 ECHR is still applicable. See n.55 for the provisions of article 15(1).

Netherland	Data Protection Authority	Data Protection Act
Poland	Inspector General for Personal Data Protection (Polish abbrev. GIODO); Polish Ombudsman (*Rzecznik Praw Obywatelskich, literally Ombudsman for Citizen Rights*)	Responsible under the Personal Data Protection Act for supervision over the compliance of data processing with the provisions on the protection of personal data
Romania	National Authority for the Supervision of Personal Data Processing	Law 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Law 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing.
Spain	Spanish Data Protection Authority	Organic Law 15/1999, Protection of Personal Data
United Kingdom	Information Commissioner[354]	Data Protection Act 1998 allow such arrangements for purposes related to national security and law enforcement.

It is noteworthy that in Poland, the GIODO has neither access to data held by intelligence services,[355] nor handles citizens' complaints about unlawful storage of their data[356]. His/her only possible control focuses on the gathering and processing of the crime-related information by law enforcement agencies.[357] He/she may not act as an appeal instance or control whether a refusal of the entity controlling the data to disclose one's own records is legitimate or not.

National legislations provide for the respect of the principles of necessity and proportionality in the access to data, which are strong criteria in the United Kingdom where there is no specific duration of retention and where the control by the hierarchical supervisor is important.[358]

Current issues under discussion within Member States selected

In many European countries constitutional debates (DE, IT, PL, RO) developed in relation to the implementation of the Data Retention Directive.

[354] UK Info Commissioner Challenges Legality of Data Retention, Privacy International, 30 July 2002, http://web.archive.org/web/ 20110603035433/ https://www.privacyinternational.org/article/uk-infocommissioner-challenges-legality-data-retention.

[355] Art. 43 s. 1 and 1a Personal Data Protection Act.

[356] Art. 43 s. 2 Personal Data Protection Act.

[357] Art. 18(1) Law of 6 July 2001 on gathering, processing, and transfer of criminal information.

[358] See *e.g.* in PL, in the light of the rulings of the Constitutional Tribunal, the premise of the necessity of limitation referred to in art. 31(3) of the Polish Constitution is essentially identical to the proportionality principle and entails the statutory obligation to choose the least bothersome means. See, *inter alia*, the ruling of 26 Apr 1999, file ref. n°K 33/98, OTK z 1999 r., Nr 4, poz. 71, the ruling of 11 May 1999, File ref. n°K 13/98, OTK z 1999 r. Nr 4, poz. 74; in the UK, Info Commissioner Challenges Legality of Data Retention, Privacy International, 30 July 2002; https://www.privacyinternational.org/article/uk-infocommissioner-challenges-legality-data-retention (accessed on 20 April 2013). Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM (2005) 438 final, 26 September 2005.

A first controversy was displayed in demonstrations by NGOs and criticisms by operators against the Data Retention Directive, which focused on how the Directive violated the right to privacy (DE[359], NL, RO[360]) and on the overall competences of authorities, including the increasing competences of intelligence services, to access data (PL). As explained above, such demonstrations certainly had an impact on legislative developments in at least two countries (BE, DE[361]). A second controversy is based on the broad definition of the different concepts such as "prevention or detection of crimes" (PL). Opponents of the Directive requested that specific elements must be specified including the conditions and circumstances under which monitoring may be used, the rights and rules on the storage and use of gathered data. Finally, it is important to highlight that data retention has generally been considered a less intrusive means of investigation than interception of communications because the authorities have no access to content but only to traffic data, location data and user data. Member States found the retention of such data less intrusive compared with allowing for a more flexible communication interception regime. Some Member States, such as the United Kingdom, claimed that the use of retained data even helps to clear persons suspected of crimes without having to resort to other methods of surveillance such as interception, which could be considered more intrusive. However, the number of data to which authorities have access is extremely high, and the use of data retention is not an alternative but rather an addition to more intrusive means such as interceptions. As a consequence, one cannot really argue that data retention is de facto less intrusive than other means.

Assessment of the use of retained data in the criminal justice system

In this section, we will provide some conclusions about the current evolution of the criminal justice system and on the use of data retained as a result of the Data Retention Directive.

Influence of serious crimes in the use of data

Serious crimes have been an important driver for the introduction and increasing use of intrusive methods for prevention and investigation purposes.

The adoption and implementation of the Data Retention Directive and the different national parliamentary and governmental works indicated a general willingness in many Member States to adopt efficient but less intrusive methods to counter serious crimes. [362] At the same time, national legislation and case law have shown that such methods have been increasingly used in relation to other offences as well. This is especially the case in BE, but also in DE[363], PL and the UK.[364] For instance, in Belgium, article 46bis §1 authorises the prosecutor, which acts before seizing of the investigative judge[365], to access retained data in the case of crimes and misdemeanours. Belgium has therefore

---

[359] "German Government Proposes Extended Tracking Of Internet Users", *Edri*, 5 December 2012; http://www.edri.org/edrigram/number10.23/germany-extended-tracking-internet-users (accessed on 20 April 2013.

[360] The debates and demonstrations do not seem to end with the Law 82/2012.

[361] BVerfG, 1 BvR 256/08, §§ 173, 174; see Shadow evaluation report on Data Retention Directive (2006/24/EC), European Digital Rights, 17 April 2011, p. 8.

[362] See preamble of Data Retention Directive 2006/24/EC.

[363] http://spd-eimsbuettel-nord.de/2012/09/27/die-spd-und-die-vorratsdatenspeicherung/; Some would argue that the use of data for investigating these kinds of offences is in praxis unconstitutional, since they are not part of "serious crimes".

[364] The access to data does not depend on the gravity of the offences but more on the complexity of the case investigated by intelligence services and law enforcement agencies. However, legislation evolves from the Anti Terrorism, Crime and Security Act 2001, which imposed the existence of the most serious crimes (national security), to Data Retention (EC Directive) Regulations 2009, which require the access only in specific cases and in circumstances in which disclosure of the data is permitted or required by law. The last regulation is opening the possibility of using this method.

[365] See art. 88*bis* CIC.

significantly in extended the initial scope of the Directive. Also, in France, law enforcement officials, prosecutors or investigative judges cannot only gather data for the investigation, detection and prosecution of criminal offences but also for civil litigation.[366]

Data that needed to be retained in order to detect and investigate serious crimes are now often also available for intelligence agencies. For instance, in France, the administrative agents or intelligence services may access retained data for the prevention of terrorism acts.[367] In Spain, the law implementing the Data Retention Directive also extends access to intelligence services.[368]

In terms of statistics, it is clear that the requests for data increased, for example in France, from 38306 in 2008 to 43559 in 2009, with 34911 accepted data requests in 2008 and 39070 in 2009.[369] In Poland, in 2011 (one year after the Directive's implementation) authorities requested users' traffic data retained by operators and ISPs over 1.85 million times (almost half a million times more than in 2010 - 1.4 million).[370] The great majority of requests are made by courts, prosecutors and police services, whereas a little more than one fourth was submitted by intelligence services.[371] However, such increased use of data in the criminal process is not necessarily matched by a parallel phenomenon of decrease in the number of serious crimes committed (DE[372], FR).

Since the definition of "serious crimes" differs from one Member State to another, there are no harmonised criteria in the context of data retention. A European definition of what constitutes a 'serious crime' would be welcome in this context. Such a EU definition would contribute to harmonise the national definitions thereby preventing Member States to extend the original scope of the Directive.

Increasing use of intelligence in the criminal justice system

This deliverable tries to argue that intelligence services became a real actor of the criminal justice system, primarily because of developments taking place in the fight against terrorism and/or organised crime. Intelligence services may have access to retained data and so may use them for prevention purposes as well as for judicial purposes when needed. Therefore, it seems interesting to make a point on the increased use of intelligence for prosecution purposes.

According to a strict separation of powers principle, traditionally the activities of intelligence services and police authorities in the prevention and investigation of crimes were clearly defined and distinct. In fact, there is a profound difference (at least in general terms) in the specific purposes of the two bodies. The police, in the framework of its judicial function, have the task of gathering information in

---

[366] Art. L34-1 *Code des postes et des communications électroniques* and art. 60-1, 77-1-1, 99-3 and 230-8 CCP.

[367] Art. L222-1 and -2 CSI.

[368] Art. 6(2) Law 25/2007.

[369] *Commission Nationale de contrôle des interceptions de sécurité*, "Le controle des opérations de communication des données techniques (loi n°2006-64 of 23 January 2006)", 18th report of activity, Year 2009, La Documentation française, p. 31.

[370] The statistics presented are obtained on the basis of the provision of the Freedom of Information Act obliging telecommunications and ISPs to report annually to the Polish government the total number of requests received from law enforcement agencies. Their general character impedes understanding the specificity of services' practices.

[371] Biuro Kolegiu do spraw służb specjalnych (Office of the Council for Special Services) Sprawdzenia dokonywane przez uprawnione instytucje u operatorów telekomunikacyjnych, p. 8.

[372] An analysis of Federal Crime Agency (BKA) statistics published in 2011 by civil liberties NGO AK Vorrat revealed that data retention, while in force, has not made the prosecution of serious crime any more effective. See "Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics", retrieved from http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf.

relation to a specific offence for prosecution purposes; intelligence services do not have the objective of investigating offences but rather to recognise threats and to provide intelligence assessments to policy makers. In this framework, intelligence information is mostly secret, whereas police information is subject to scrutiny via cross-examination in court. However, nowadays the distinction is not so clear. Intelligence services have also been given operational tasks and this could lead to coordination and overlap problems between police and intelligence agencies.[373]

This trend leads to an intense and dangerous osmosis and blurring of competences between criminal justice and intelligence investigations especially since most intelligence activities are covered by the State Secrecy principle.[374] Intelligence activities and police investigations tend to converge in terms of their object, scope and means, particularly in relation to serious crime where intelligence is crucial to understand at best the organisational dimensions of complex, widely spread and long-lasting phenomena which threaten national security.[375] In this context, the relationship between intelligence and the judiciary needs to be better defined, especially since retained data may be used by the competent authorities for both intelligence and judicial procedure purposes.

National legislation has normalised, and even institutionalised, an increased gathering of information by both intelligence services and law enforcement agencies. Information gathering in the hands of intelligence services is the most problematic from a privacy perspective mostly because information is secretly gathered. Even if a hierarchical supervisor authorises the access, there is often no official record. As a result, individuals are not aware of the proceedings and the reasons for such an access, but they also often have no possibility to contest these activities. This method appears to constitute the most profound change in the ways crime is being prevented in the Member States.

An even more problematic trend that can be witnessed is the use of data gathered by intelligence services that did not have to take into account the rules on judicial procedures in the investigation and prosecution of serious crimes (BE[376], DE, FR, PL, RO, ES[377]). Law sometimes restricts the use of new powers by intelligence services (BE[378], FR, RO[379]), whereas other countries allow the use of such intelligence for the only purpose of prevention and investigation (such as in IT where intelligence cannot be presented at trial). [380] In fact, it is noteworthy that Italy is the only State of our case studies that does not accept intelligence as evidence in court. In contrast, other countries (*e.g.* PL) witness a much bigger convergence of the competences of intelligence agencies and law enforcement agencies involving an increasing use of intelligence at trial.

---

[373] The distinction of roles and information sharing between intelligence services and law enforcement authorities with a view of preventing an combating terrorism has been highly discussed and let to controversial case-law also in other UE countries such as the Netherlands. See J.A.E Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law? » (2005) 1(1) *Utrecht Law Review* 1.

[374] See in Italy, R. Orlandi, "Segreto di Stato e limiti alla sua opponibilità fra vecchia e nuova normativa" (2010) 6 Giur cost 5224; A Pace, "L'apposizione del segreto di Stato nei principi costituzionali e nella legge n.124 del 2007, (2008) 5 Giur Cost 4041.

[375] See R. Orlandi, "Attività di intelligence e diritto penale della prevenzione" and F. Sommovigo, "Attività di intelligence e indagine penale" *in* G. Illuminati, *Nuovi Profili.*

[376] The theoretical prohibition to present intelligence in court alleviate recently.

[377] Art. 5(5) Law 11/2002.

[378] Art. 18/9 Law 4 February 2010.

[379] Serious crime as defined in art. 2(e) Law 82/2012.

[380] Art. 118*bis* CPP introduced by Law 124/2007 on the Information System for the security of the Republic; art. 329 CPP provides for the confidentiality of the investigative measures. In this case, the inforamtion may only be obtained with the prior authorisation of the competent judicial authority. Art. 15 Law 124/2007. G. Illuminati (dir.), *Nuovi profili segreto di Stato e dell'attivita di intelligence*, G. Giappichelli editore, Torino, 2010, p. 233.

Defence lawyers and human rights organisations criticize the extended use of intelligence in court. They fear that the increased acceptance of intelligence, for instance in terrorism cases, is expanding through case law and will be increasingly accepted in other 'less serious' cases. Terrorism cases have set a precedent in this context. Belgian magistrates Daniel Fransen and Damien Vandermeersch confirm that there is a thin line between intelligence and judicial information in their gathering and increasingly in their use as evidence in court.[381] In some countries, they may even end up having the same value in court (DE, FR, PL) or at least they become increasingly valuable (RO). This is certainly dangerous as intelligence information is gathered under little to no judicial scrutiny.

Interference of the private sector in the criminal justice system

Traditionally, the State and public authorities have a sort of monopoly on the law enforcement and criminal justice systems. Such classical feature tends to evolve due to the growing intervention of private actors in the fight against serious crime. The importance and purpose of such intervention vary significantly.[382] The adoption of the Data Retention Directive and its implementation by Member States demonstrate this increasing involvement of the private sector in the criminal justice system.

The involvement of the private sector in data retention, and more broadly the use of surveillance technologies by the private sector for public order purposes (*e.g.* video-surveillance), has led to abuses because private companies have sometimes used data for other purposes than those envisaged by the 2006 Directive. [383]

In order to prevent such abuses, in Poland, a "Report on the retention of telecommunications data"[384] by the Secretary of State for security and public order, recommended the establishment of an independent supervising body appointed by Parliament, which would be in charge of controlling the compliance of the access to the data retained with the Constitution and other provisions (especially those related to the rights and freedoms of the citizens); introducing an absolute obligation to destroy data which has proven unhelpful or ceased to be useful for the achievement of the aim for which they were obtained; and a duty to report on how data subject to telecommunications secrecy have been used by the authorities.[385] These recommendations have not been yet adopted but would create more control upon the private sector involved and, above all, would enable citizens to question the lawfulness and correctness of the activities performed by the Police or other services.[386] Similar concerns and attempts to find a proper solution have been discussed in Spain**.**

---

[381] D. Fransen and D. Vandermeersch, "Les mesures d'investigation et les droits de l'Homme", *in* L. Hennebel and D. Vandermeersch (dir.), *Juger le terrorisme dans l'Etat de droit*, Bruylant, Magna Cart, Bruxelles, 2009, p. 370.

[382] See P. Breyer, "Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" (2005) 11(3) *European Law Journal* 365; I. Brown, "Government access to private-sector data in the United Kingdom" (2012) 2(4) *International Data Privacy Law* 230; S. Chesterman and A. Fisher "Private security, public order. The outsourcing of public services and its limits" (2011) *European Journal of International Law* 909; E. Kosta and P. Valcke, "Telecommunications – the EU data retention directive" (2006) 22(5) *Computer Law & Security Review* 370.

[383] See *e.g.* ECtHR, *M.M.* v. *the United Kingdom*, 24029/07, 13 November 2012.

[384] Raport dotyczący retencji danych telekomunikacyjnych opracowany przez sekretarza stanu ds. bezpieczeństwa w Kancelarii Premiera Jacka Cichockiego, 8 June 2011.

[385]Założenia projektu ustawy o zmianie niektórych ustaw, w związku z pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych, 28 May 2012.

[386] Letter of Fundacja Panoptykon to the Minister of Internal Affairs, 13 June 2012, p.5 and 7

Potential influence of an authoritarian past

As mentioned in the introduction, a number of countries chosen as case studies have been selected because they have experienced authoritarian regimes. This topic will be better explored by empirical research of "the paper on the ethics of data retention, distinguishing between democratic and authoritarian regimes" of the SURVEILLE Project[387].

On the basis of the black letter legal analysis conducted for this paper, there is no conclusive evidence to suggest that this past had a uniform impact on national data retention regulations and institutional arrangements. The influence of an authoritarian past appears to vary between relevant Member States.

In Germany, Poland and Spain**,** the authoritarian regime definitely had an adverse impact on constitutional safeguards and/or criminal procedure. The main reason for establishing extra safeguards in these countries' criminal procedure after the authoritarian period ended was the necessity to set limits to potential abuse by the government, and to avoid that an individual exceeds existing limitations to power. Therefore, constitutional guarantees were established, so that all exercises of State power were subjected to the law and that human dignity would be respected in every situation. The national Constitutions of these three States established a catalogue of fundamental rights affecting all legal procedures,[388] including the confidentiality of the contents of communication and of the specific circumstances of communications discoveries.[389]

Germany developed an intelligence structure based on numerous independent intelligence agencies reflecting the federal structure with 16 *Länder.* This system of decentralisation to the *Land* level was a deliberate historical anomaly instituted after the Nazi regime to ensure that excessive powers were not centralised in the hands of the federal government.[390]

In Poland, systemic changes initiated amendments of the code of Criminal Procedure expanded the scope of the courts' powers in preparatory proceedings. However, given the lack of control by courts of preparatory proceedings – among other reasons -, the current model does not seem clearly to break with the tradition of the Soviet model.

In Spain, a decision of the Supreme Court of 27 February 2012[391], declared that the amnesty law, under appeal, is part of a transition from an authoritarian regime to democracy. This transition is considered as a model and was the result of the embrace between the "two Spains" faced in the Civil War. So, it is not a rule imposed by the victorious of the conflict to obtain impunity for their actions. Laws were enacted with the agreement of all political forces, with an obvious sense of reconciliation.[392]

---

[387] See K. Hadjimatheou, "Paper on the ethics of data retention distinguishing between democratic and authoritarian regimes", SURVEILLE Deliverable, D4.4 (forthcoming).

[388] Art. 101 GG prohibits courts of exception and states "nobody can be taken away from a judge"; it protects the right to be heart in a trial, the principle of "*ne bis in idem*", etc.

[389] Art. 10.1 German Constitution.

[390] See *e.g.* R. Warnes, *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, p. 114; T. Würtenberger, "Das Polizei- und Sicherheitsrecht vor den Herausforderungen des Terrorismus" *in* J. Masing and O. Jouanjan (Hg.), *Terrorismusbekämpfung, Menschenrechtsschutz und Föderation*, 2008, s. 27-48; A. Oemichen, *Terrorism and anti-terror legislation: the terrorised legislator? A comparison of counter-terrorism legislation and its implications on human rights in the legal systems of the United Kingdom, Spain, Germany and France*, p. 267 ff.

[391] Tribunal Supremo, sentence 101/2012, 27 February 2012.

[392] See *e.g.* Organic Law 10/1995, 23 November 1995; Law 52/2007, which recognises and extends rights and establishes measures in favor of those who suffered persecution or violence during the civil war and dictatorship, 26 December 2007.

The existence of a former authoritarian regime did not seem to have influenced the issue of data retention and the increased protection of human rights in this context in either Italy or Romania. The ECtHR[393] played a more important role in the so-called democratisation process of the Romanian criminal system. In Italy, the most important influence on criminal procedure in this context results from the implication and alleged abuses of intelligence services during the 1960s and 1970s terrorist attacks. The intelligence services' involvement (and the use of the information they gather) is thus highly framed and scrutinize (*e.g.* by the establishment of a specific Parliamentary Committee).[394]

Conclusion

This deliverable has analysed the issue of data retention in the EU for the purpose of investigation and prosecution of serious crimes. Specific attention was given to the duration of the retention, the authorities who authorise the retention and have access to the data retained as well as the procedure to be followed, and finally the scope of the retention. Further attention has been given to the tests of necessity and proportionality, as well as to the right to privacy and the assessment of the relative intrusiveness of data retention by comparison to other means of investigation.

This deliverable aimed to test the "catalysing effect" of serious crime on the increasing use of data retained by law enforcement officials and intelligence services for the purpose of investigation and prosecution of serious crimes. Indeed, the threat of serious crime was the basis for the adoption of the Data Retention Directive and, because of the lack of a definition on what constituted serious crime at the EU level, Member States extended, on one hand, the scope of the access to these data and, on another hand, the authorities who may have access, including in particular intelligence services. The Directive contributes to the blur of competences between law enforcement authorities and intelligence services in the prevention and investigation of serious crime[395] as well as to a general shift towards prevention, proactive investigations and intelligence-led policing within the criminal justice system.[396]

Finally, despite the fact that data retention has been always considered as a less intrusive means compared to the interception of communications, and was always seen by the Member States as a very valuable means of investigation, the number of data to which authorities have access is extremely high, and the use of data retention is not an alternative but rather an addition to more intrusive means such as interceptions. As a consequence, one cannot really argue that data retention is de facto less intrusive than other means.

---

[393] One of the most important changes of the criminal procedure due to the ECtHR judgments was to subject the acts of the prosecutors gathering evidence and the arrest to the reasoned authorisation of the judge. See ECtHR, *Pantea* v. *Romania,* 2003; *Dumitru Popescu* v. *Romania*, 2007; Grand Chamber judgment, *Rotaru* v. *Roma*nia, 2000.

[394] See *e.g.* Camera dei deputati, Il sistema di informazione per la sicurezza e la disciplina del segreto di Stato, Law 124/2007, n°115, 18 December 2007.

[395] Intelligence agencies would generally provide background information and "advance warnings about people who are thought to be a risk to commit acts of terrorism or other threats to national security", but would – unlike law enforcement agencies – not be actively engaged in investigating acts of terrorism. K. Roach, "Secret evidence and its alternatives" *in* A. Masferrer (ed.), *Post 9/11 and the state of permanent legal emergency. Security and human rights in countering terrorism*, p. 180.

[396] Proactive investigation has been defined as "the prevention of serious crimes that threaten the safety of many citizens, in particular terrorism, and for which reason the traditional criminal investigative functions (evidence gathering) and intelligence investigative functions (the gathering of information about threats to national security for the purpose of prevention) have been merged." M. F.H. Hirsch Ballin, *Anticipative criminal investigation. Theory and counter-terrorism practice in the Netherlands and the United-States*, p. 4.