FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency
Collaborative Project

SURVEILLE Deliverable 4.3: Comparative law paper on data retention regulation in a sample of EU Member States

Due date of deliverable: 30.04.2013
Actual submission date: 30.04.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP04 Prof. Martin Scheinin (EUI)

Author(s): Céline Cocq and Francesca Galli (ULB)*

SURVEILLE: Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

* The authors are grateful for the substantial contributions that were provided by EUI researchers Cristina Blasi Casagran, Madalina Moraru, Marta Otto, Mathias Vermeulen and Ben Wagner. All errors or mistakes in this deliverable are our own.

Abstract

Within the context of the SURVEILLE project, which offers a legal and ethical analysis of issues surrounding the use of surveillance technologies in the three phases of countering serious crime (prevention, investigation and prosecution) at the national as well as at the EU level, this deliverable focuses on the use of retained data in the fight against serious crime. This research aims at conducting a comparative study of the use of retained data within selected national jurisdictions for the purpose of investigating and prosecuting serious crime. The authors are testing in this paper a hypothesis, which is used to describe a trend underlying a current evolution in this domain. The hypothesis relates to the so-called catalysing effect of serious crime on the increasing use of data retention for the purpose of investigating and prosecuting serious crime. The catalysing effect of serious crime on the use of such a measure is amplified by the fact that the Data Retention 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. Thus, the access of data retained by the private sector for investigation purposes and the subsequent use for prosecution purposes has been studied in nine EU Member States, namely Belgium, France, Germany, Italy, the Netherlands, Poland, Romania, Spain and the United Kingdom. The comparative analysis of these case studies allow us to highlight potential differences in those legal provisions that regulate the retention and subsequent use of information between European Member States with an authoritarian past and Member States without such a past. The human rights dimension is the normative background of the project as a whole, and thus of the present work.

Executive summary

- National public authorities should undertake a thorough a legal impact assessment before deciding to harmonize legislation supporting the use of data retention in the investigation, detection and prosecution of serious crimes.

- The use of surveillance technologies in order to gather information in the prevention and investigation phase and then to introduce the results of these surveillance technologies as evidence at trial in the prosecution phase must be recognised and better defined by law. This use should always respect the principles of proportionality and necessity to ensure the lowest degree of intrusion into the private life of individuals.

- The core of this study is the assessment of the use of retained data in a country's criminal procedure in order to highlight the similarities and differences between selected Member States namely Belgium, France, Germany, Italy, the Netherlands, Poland, Spain, Romania and the United Kingdom.

- The use of retained data is particularly relevant for the purpose of gathering information to investigate and prosecute, serious crime by intelligence services, law enforcement agencies and judicial authorities.

- This deliverable provides an overview of how access to retained data in the investigation phase and then used as evidence at trial is regulated, by analysing the following elements:
    - the legal basis and purpose of data retention
    - the scope of data retention legislations, including the length of retention
    - the procedure applicable in each country to access retained data, including analysing the authorities that authorize access
    - the procedure to be followed for presenting intelligence/information at trial.

- While data retention was adopted for investigation, detection and prosecution of serious crimes, its scope has extended to the use of such data for prevention purposes and for all kind of (less serious) offences. In this context, the use of data retention must be clearly regulated by European instruments and by the national provisions in the prevention, investigation and prosecution phases.

Table of content

1. 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.[1] 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.[2] Both traffic data and location data have been considered very useful for investigating the terrorist attacks in Europe.[3]

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"[4] 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.[5] Communications data may be defined as the data identifying: who made a communication[6]; 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.[7] More specifically, the Data Retention Directive applies to the fields of fixed network telephony, mobile telephony, Internet access, Internet email and Internet telephony.[8] 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[9], for preventing and investigating serious crimes.[10] Equally, it is often seen as an important tool for the prosecution as it can produce evidence to be brought to trial.

---

[1] 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.
[2] European Council, Declaration on Combating terrorism, 25 March 2004.
[3] Preamble 11 Directive 2006/24/EC.
[4] Art. 2 Directive 2006/24/EC.
[5] Art. 3 Directive 2006/24/EC.
[6] 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.
[7] Art. 5 Directive 2006/24/EC.
[8] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011, p. 12.
[9] 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.
[10] 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.

Some prosecutors even declare that a number of guilty verdicts are almost exclusively based upon such retained data.[11]

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[12] 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.[13]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.[14] However, no definition of what constitutes 'serious crimes'[15] 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.[16] National legislation often gave intelligence services access to retained data, thereby allowing the use of data retention also for preventive purposes.[17]

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[18] as well as to a general shift towards prevention, proactive

[11] See *e.g.* interview with B. Michel, Federal Prosecutor (Brussels, 26 February 2013).
[12] 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).
[13] See preamble 8 of Directive 2006/24/EC.
[14] Art. 1 Directive 2006/24/EC.
[15] 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.
[16] Art. 4 Directive 2006/24/EC.
[17] 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".
[18] 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*, Ius Gentium: Comparative Perspectives on law and justice 14, Springer, 2012, p. 180.

investigations and intelligence-led policing within the criminal justice system.[19] 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[20] 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.[21] 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.[22]

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 lead to difficulties in the implementation of the Data Retention directive.

2. 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).

[19] 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.

[20] 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*).

[21] 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.

[22] 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.[23] 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[24] 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.[25] However, the European Commission urged Romania to fully implement the Data Retention Directive within two months[26] 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 transposition of the Data Retention Directive violated the Constitution.[27] 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.[28] 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.[29] 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, [30] 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

[23] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011.
[24] 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.
[25] Constitutional Court of Romania, Decision n°1258 of 8 October 2009, O.J. n°798, 23 November 2009.
[26] 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.
[27] 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.
[28] 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).
[29] 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).
[30] Evaluation report on the Data Retention Directive, COM(2011) 225 final, 18 June 2011.

Court of Justice of the European Union. On 27 January 2012, the Federal Ministry of Justice addressed[31] a report on the effects of the Constitutional Court's decision in 2010 and asserted the need for retention of 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.[32] 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.[33] These drafts should be discussed in Parliament soon in order to comply with all requirements of the Directive.

3. 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.[34]

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.[35] 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

[31] On the basis of a study carried out by Max Planck Institute.
[32] 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).
[33] 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).
[34] Art.1 Directive 2006/24/EC.
[35] Art. 16 Cybercrime Convention, for a maximum of 90 days.

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.[36]

The Cybercrime Convention of the Council of Europe requires only data preservation.[37] 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[38], DE[39], FR[40], IT[41], PL[42], RO[43]), while one country limits slightly its scope (NL[44]). 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[45], UK[46]). Germany also provides for a general obligation to protect data against unauthorised access and thus potential alteration.[47] 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.

4. 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

[36] European Commission, "Data retention: Commission takes Germany to requesting that fines be imposed", Press Release, IP/12/530, 31 May 2012.
[37] Art. 16-17 Convention on Cybercrime.
[38] 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.
[39] Art. 96 Telekommunikationsgesetz (TKG). Data are preserved for commercial purposes because there is no transposition for judicial purposes.
[40] 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.
[41] Art. 247 (1bis) CCP.
[42] Art. 218a and b CCP. Method of preservation is provided into Regulation of the Minister of Justice, 28 April 2004.
[43] 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.
[44] 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.
[45] 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".
[46] Art. 6 Data Retention (EC Directive) Regulations 2009.
[47] §109 TKG.

- 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]." [48]

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.[49] Italy provides for the destruction of data.[50] France[51] and the United Kingdom[52] have transposed all the four principles.

4.1. 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[53] 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[54] so that the principle of confidentiality it enshrined does not apply to data retention.

Five Member States (DE[55], ES[56], NL[57], RO[58], UK[59]) 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[60], FR[61], IT[62], PL[63]) 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.

[48] 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.
[49] Art. 6 *Arrêté Royal* of 9 January 2003.
[50] Art. 123 and 126 Data protection Code.
[51] 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.
[52] Art. 6 Data Retention Regulation.
[53] Detection could be defined as the fact of the police discovering information about crimes.
[54] 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."
[55] Art. 100a stop (German Code of criminal procedure).
[56] Art. 1(1) Law 25/2007.
[57] Art. 126 CCP.
[58] Art. 2(e) Law 82/2012.
[59] S. 93(4) Police Act 1997.
[60] Art. 126(1) Law of 13 June 2005 concerning electronic communications.
[61] Art. L.34-1(II), CPCE, Law 64/2006 and Law 669/2009.
[62] Art. 132(1) Data Protection Code.
[63] Art. 180a, Telecommunications Law of 16 July 2004 as amended by art. 1 Act of 24 April 2009.

4.2. 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.[64] The United Kingdom does not require small operators to retain data[65] 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, ES[66]) 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.[67] 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.[68]

4.3. 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

[64] See *e.g.* in Sweden, the *Stadsnatsforeningen och Stadsnat* is negotiating a hosted third-party storage service for 150 network operators.
[65] 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.
[66] 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.
[67] 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).
[68] Cecilia Malmström, "Taking on the Data Retention Directive", SPEECH/10/723, European Commission conference, Brussels, 3 December 2010.

	services. No provision for internet-related data.[69]
France	The period of data retention is of **one year**.[70] 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[71].
Germany	Telecommunications companies store traffic data for commercial purposes up to **six months**[72]
Italy	The period of data retention depends on the different categories of data.[73] 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**[74], and traffic data and subscribers' data in relation to Internet access services must be retained for **6 months**[75].
Poland	**One year**[76]
Romania	**Six months**[77]
Spain	**One year**[78]
United Kingdom	**One year** as of the date of the communication[79]

4.4. Access to data: authorities and procedure

Most Member States under analysis, both national police forces and prosecutors may access retained data.[80]

States	**Competent authorities to access**	**Procedure**

[69] 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 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.
[70] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 13.
[71] Art. 60-2 CCP.
[72] §97 TKG.
[73] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011, p. 14.
[74] Art. 13.2a(3)(a) Telecommunications Act.
[75] Art. 13.2(3)(b) Telecommunications Act.
[76] "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.
[77] Art. 3(2) Law 82/2012.
[78] Law 25/2007.
[79] §5 Data Retention Regulations 2009.
[80] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 9.

Belgium	Prosecutor, judge (*juge d'instruction*); police [81] ; intelligence services[82]	Access must be authorised either by a judge or prosecutor. Upon request, operators must provide, without delay, subscriber data and traffic and 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[83], police under the prosecutor's warrant after prior authorisation of the judge (JLD)[84]; 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[85] can have access to traffic data; Prosecutor[86] in case of emergency; in specific cases, the Federal Network Agency (*Bundesnetzagentur* [87]) (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[88].
Italy	Prosecutor, judge[89], Police, defence counsel for the defendant or the person under investigation [90] ; intelligence services[91]	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.[92]
Netherland	Prosecutor[93]	Access must be given by a warrant of the

[81] Law of 21 March 2007 (*réglant l'installation et l'utilisation de caméras de surveillance*).
[82] Law 4 February 2010 (*Méthodes de Recueil des Données)*.
[83] Art. 60-1 CPP as modified by the Law 2004/204 of 9 March 2004 and the Law 2007/297 of 5 March 2007.
[84] Art. 6 Law 2004/575.
[85] § 100g StPO.
[86] "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.
[87] Federal Authority within the scope of the German Federal Ministry of Economics and Technology
[88] § 112(1) TKG.
[89] 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.
[90] Art. 132(3) Data Protection Code ; art. 15 Italian Constitution.
[91] Art. 26 §1 Law 124/2007 only for security purposes.
[92] Art. 132(3) Data Protection Code.
[93] Art. 126ni CCP.

		prosecutor or the investigative judge
Poland	Police, Border control officers, Treasury Intelligence, Military Gendarmerie, Customs Service, Internal Security Agency, Central Anti-Corruption Bureau, Military Counter-Intelligence Services[94]	Access to data is subject to a written request[95] or an oral request.[96] 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[97], the police (under the supervision of the Prosecutor for data retention)[98]	Requests of the prosecution, the courts and State authorities in charge of national security will be made on the basis of legal provisions[99] 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[100] in order to avoid any modification of these data.
Spain	Court warrant[101]; director of State Security[102]	Once the judge has issued his/her decision, the prosecutor will be informed[103]; the director of State Security communicates it to the competent judge immediately.[104]
United Kingdom	Serious Organised Crime Agency, the Scottish Crime and Drug Enforcement Agency, Her Majesty's Revenue and Customs, any	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

[94] 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.

[95] 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.

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

[97] Art. 16 Law 82/2012.

[98] Art. 18 Law 82/2012.

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

[100] Art. 16 Law 82/2012.

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

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

[103] Art. 306 LECr (CCP).

[104] 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.

	of the intelligence services and some other public authorities [105] ; intelligence services [106]	procedures have been agreed with operators.

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.[107]

4.5. Scope of data retention and access

The retention applies to the source of communications[108], the destination of communications, the data, time and duration of communications, [109] type of communications, user's [110] communication equipment or what purports to be their equipment, and, finally, the location of mobile communication equipment[111]. 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[112], ES[113]), 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[114], DE[115], UK[116]). In any case, each request to access data or images must be justified.

[105] S. 25 RIPA 2000.
[106] S. 7 Data retention Regulation and 22 RIPA.
[107] 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.
[108] 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.
[109] '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.
[110] 'User' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.
[111] '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.
[112] 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.
[113] Spanish law 25/2007 permits access to law enforcement authorities as long as it is for the investigation of a serious crime.
[114] Art. 19/1 Law 2010 MRD.
[115] Art. 100a and g StPO, art. 113 TKG.
[116] S. 7 Data retention Regulation and s. 22(2) of RIPA.

5. 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.[117] 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.[118]

Data that needs to be retained under the Data Retention Directive has been essential in the investigation of a number of serious crimes.[119] In Belgium, for example, one may refer to the 2008 conviction of the perpetrators of a so-called tiger kidnapping[120] 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.[121] 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.[122]

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

[117] 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.
[118] *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.
[119] 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.
[120] The kidnapping of a person in order to compel him/her or a third person to commit another crime.
[121] National Policing Improvement Agency, United-Kingdom, *The journal of Homicide and Major Incident Investigation*, vol.5, issue 1, Spring 2009, pp. 39-51.
[122] 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

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.[123] On the EU level, the effectiveness of Operation Rescue (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.[124]

5.1. 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.

5.1.1. 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 (BE[125], ES[126], FR, PL[127]). This principle may considerably hamper the effect of irregular evidence*, i.e.* evidence collected in violation of procedural or substantial evidence gathering rules.[128] Yet, in some countries, such evidence may be admitted if its irregular nature does not harm the interests of the party (BE[129], FR, NL).[130] 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).[131]

(2) The freedom in the types of evidence employed[132] (BE[133], DE[134], ES, FR, NL, PL,

[123] 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.
[124] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p. 24.
[125] *e.g.* art. 18/3 and art. 18/9 Law 4 February 2010.
[126] Art. 11(1) LOPJ; art. 15 Spanish Constitution.
[127] Art. 170 CCP.
[128] 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.
[129] Cass. 14 October 2003, *Antigone* case; see also, M. Delmas-Marty and J.R. Spencer (eds), *European Criminal Procedures* (CUP, Cambridge, 2006), p. 122.
[130] 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.
[131] *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.
[132] Evidence may be supplied in any appropriate form except where the law provides otherwise.
[133] Cass., 27 February 2002, *Pas*., 2002, p. 598; Cass. 5 March 2002, *Pas*., 2002.
[134] Art. 261 CCP.

RO[135], UK)

However, some countries limit the types of evidence, which could be presented at trial by specific rules (DE[136], RO).

(3) And, its corollary, the discretion of the judge to assess it.[137]

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[138], IT[139], UK[140]).

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.[141]

5.1.2. The exclusion of evidence: irregularity and illegality

Irregularly obtained evidence can be withdrawn from the case file directly by the prosecutor (BE[142], FR, RO) or later in court by the judge (DE, ES[143], NL[144], 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.[145]

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.[146] In some countries, the court has a discretionary power to reject (*inter alia*) evidence that has been illegally or improperly obtained (NL, UK[147]). Some countries explicitly prohibit the "fruit of the poisonous tree"[148] (ES[149], PL) while others do not (IT[150]). 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,[151] including through contradiction in court (BE[152], ES, PL, RO, UK).[153]

---

[135] Art. 741 CCP.
[136] Art. 244 (II) StPO.
[137] See *e.g.* M. Delmas-Marty and J.R. Spencer (eds), *European Criminal Procedures*.
[138] 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.
[139] Art. 192 CPP.
[140] 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.
[141] *e.g.* in BE, Cass. 14 October 2003, *Antigone* case
[142] 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.
[143] Art. 658 and 659 (I) CCP. See *escritos de calificación provisional.*
[144] Art. 359a CCP.
[145] 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).
[146] C. Ambroise-Castérot, P. Bonfils, *Procédure pénale,* Paris, PUF, 2011, 190f.
[147] S. 78 PACE 1984.
[148] 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.
[149] STC n°114/1984, 29 November 1984.
[150] According to case law, it could be applied in Italy but the decisions of the judges on this matter are neither frequent nor clear.
[151] See *e.g.* ECtHR, *Lee Davies* v. *Belgium*, 18704/05, 28 July 2009, §42; applied by Cass., *Antigone* case, 14 October 2003.

5.1.3. 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[154], 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[155]) but this information cannot always be shown in court. This is the case for instance in France and the United Kingdom.[156]. In France, intelligence is assessed by the Prosecutor, who decides whether the information is admissible to be submitted in Court.[157]
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. [158]

5.1.4. Procedure for intelligence to become evidence

The centralisation, coordination and exploitation of intelligence is increasingly organised and institutionalised (*e.g.* DE, ES, FR, IT[159]).

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.[160] The national and central organisation that the *DCRI*[161] 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.[162] 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.

---

[152] Cass. 18 January 1971, Pas. 1971 I. 459; Cass. 10 June 1974, 1974 I. 1040.
[153] See *e.g.* ECtHR, 10 March 2009, *Bykov* v. *Russia*, req. n°4378/02, §95.
[154] M. Trévidic, parliamentary committee of inquiry, "Fonctionnement des services de renseignement", National Assembly, 14 February 2013.
[155] HR 5 September 2006, NJ 2007, 336.
[156] A. Masferrer (ed.), *Post 9/11 and the State of Permanent Legal Emergency. Security and Human Rights in countering Terrorism*, p. 180-182.
[157] M. Trévidic, parliamentary committee of inquiry, "Fonctionnement des services de renseignement", National Assembly, 14 February 2013.
[158] *e.g.* arts. 203 and 240(2) CPP.
[159] Art. 2 Decree 2008/609.
[160] 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.*
[161] Gathering of the *Direction de la surveillance du territoire* (DST) and of the *Direction centrale des Renseignements Généraux* (RG).
[162] Interview with P. Caillol, Deputy Director of the *Institut national des hautes études de la sécurité et de la justice* (Paris, 28 November 2012).

In Germany, legislative and institutional reforms occurred to improve the coordination between the two bodies, including the Act on Joint Databases,[163] which promotes the collaboration of the 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.[164] With this database, the principle of the separation of police and intelligence services, the German *Trennungsprinzip*[165]*,* is further weakened. Intelligence and police forces now share the same data.[166]

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.[167]

Depending on the country, intelligence obtained by administrative warrants (administrative police and intelligence services) may be officially recorded in a statement (BE[168], FR, NL[169]) 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.[170] In some countries, evidence can only be disclosed in court so there is no specific procedure to be followed beforehand (DE, NL, PL[171], ES, UK[172]).

---

[163] *Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des 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).

[164] §2 first sentence, sub-paragraphs (1a) - (3).

[165] 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.

[166] 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.

[167] 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)

[168] 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).

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

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

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

5.2. Assessment of evidence: prosecution and trial

5.2.1. 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[173]). 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.[174] In The Netherlands, for instance, from January to July 2010, historical traffic data has been a decisive factor in 24 court judgments.[175] 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.[176]

5.2.2. 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[177], DE, FR[178], RO[179], UK). In some countries, intelligence must always be corroborated by other evidence (BE[180], ES[181]); it does not have any evidentiary value if it is presented as sole source of evidence.

---

[172] 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.
[173] CCTV information, CCTV Advisory Service, http://www.cctv-information.co.uk/i/Digital_Images_as_Evidence (accessed on 4 February 2013).
[174] *e.g.* interview with the Prosecutor B. Michel (BE), (Brussels, 26 February 2013).
[175] Evaluation report on the Data Retention Directive, COM(2011) 225 final, Brussels, 18 April 2011, p.25.
[176] *Ibid*.
[177] *e.g.* art. 29 CCP.
[178] M. Trévidic, parliamentary committee of inquiry, "Fonctionnement des services de renseignement", National Assembly, 14 February 2013.
[179] Art. 7 CCP.
[180] Art. 19/1 §4 Law 2010 MRD. C. Constit., *Loi du 4 février 2010*.
[181] 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.

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.[182] Intelligence is then taken into account by the judge, but it is not a decisive element (BE, DE, ES[183], FR, NL[184], RO[185]). The judge may even decide not to consider such evidence at all (ES[186], RO). In some countries, evidence presented by police agencies has a higher value (ES[187]) 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[188], UK[189]). 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.

6. Implications of data retention for fundamental rights

6.1. Protection of privacy vs. intrusiveness

6.1.1. 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[190]. Such intrusiveness must be 'provided for by law and respect the essence of those rights, subject to the principle of proportionality'[191], and justified as necessary and meeting the objectives of general interest. This means that any limitation must[192] (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.

---

[182] SN judgment of 20 February 2002, V KKN 586/99, Prok. i Pr. 2002, supplement "Orzecznictwo", n°11, item 10, LEX 53048.
[183] STS 31.03.2010; Raquel Castillejo Manzanares, 2012, p. 4.
[184] Art. 359a CCP.
[185] Art. 410 CCP.
[186] 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.
[187] Raquel Castillejo Manzanares, 2012, p. 6.
[188] 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.
[189] 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.
[190] 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".
[191] Art. 52(1) Charter for Fundamental Rights.
[192] 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'.

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 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.[193] 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.[194]

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. [195] 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.[196]

6.1.2. 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*)

[193] 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.
[194] ECtHR, *Schenk* v. *Switzerland*, §§47-51; *Heglas,* §§89-93.
[195] 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.
[196] 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).

Italy	Garante della Privacy	Code of privacy
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[197]	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,[198] nor handles citizens' complaints about unlawful storage of their data[199]. His/her only possible control focuses on the gathering and processing of the crime-related information by law enforcement agencies.[200] 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.[201]

6.2. Current issues under discussion within Member States selected

[197] 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.
[198] Art. 43 s. 1 and 1a Personal Data Protection Act.
[199] Art. 43 s. 2 Personal Data Protection Act.
[200] Art. 18(1) Law of 6 July 2001 on gathering, processing, and transfer of criminal information.
[201] 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.

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

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[202], NL, RO[203]) 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[204]). 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.

7. 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.

7.1. 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.[205] 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[206],

[202] "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.

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

[204] 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.

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

[206] 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".

PL and the UK.[207] For instance, in Belgium, article 46bis §1 authorises the prosecutor, which acts before seizing of the investigative judge[208], to access retained data in the case of crimes and misdemeanours. Belgium has therefore 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.[209]

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.[210] In Spain, the law implementing the Data Retention Directive also extends access to intelligence services.[211]

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.[212] 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).[213] 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.[214] 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[215], 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.

---

[207] 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.

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

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

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

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

[212] *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.

[213] 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.

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

[215] 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.

7.2. 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 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.[216]

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.[217] 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.[218] 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.

[216] 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.

[217] 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.

[218] 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*.

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[219], DE, FR, PL, RO, ES[220]). Law sometimes restricts the use of new powers by intelligence services (BE[221], FR, RO[222]), 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).[223] 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.

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.[224] 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.

7.3. 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.[225] 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.[226]

---

[219] The theoretical prohibition to present intelligence in court alleviate recently.
[220] Art. 5(5) Law 11/2002.
[221] Art. 18/9 Law 4 February 2010.
[222] Serious crime as defined in art. 2(e) Law 82/2012.
[223] 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.
[224] 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.
[225] 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.
[226] See *e.g.* ECtHR, *M.M.* v. *the United Kingdom*, 24029/07, 13 November 2012.

In order to prevent such abuses, in **Poland**, a "Report on the retention of telecommunications data"[227] 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.[228] 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.[229] Similar concerns and attempts to find a proper solution have been discussed in **Spain.**

8. 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[230].

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,[231] including the confidentiality of the contents of communication and of the specific circumstances of communications discoveries.[232]

Germany developed an intelligence structure based on numerous independent intelligence agencies reflecting the federal structure with 16 *Länder.* This system of decentralisation to the

[227] Raport dotyczący retencji danych telekomunikacyjnych opracowany przez sekretarza stanu ds. bezpieczeństwa w Kancelarii Premiera Jacka Cichockiego, 8 June 2011.
[228] Założenia projektu ustawy o zmianie niektórych ustaw, w związku z pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych, 28 May 2012.
[229] Letter of Fundacja Panoptykon to the Minister of Internal Affairs, 13 June 2012, p.5 and 7
[230] See K. Hadjimatheou, "Paper on the ethics of data retention distinguishing between democratic and authoritarian regimes", SURVEILLE Deliverable, D4.4 (forthcoming).
[231] 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.
[232] Art. 10.1 German Constitution.

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.[233]
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[234], 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.[235]

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[236] 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).[237]

9. 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

[233] 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.
[234] Tribunal Supremo, sentence 101/2012, 27 February 2012.
[235] 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.
[236] 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.
[237] 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.

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[238] as well as to a general shift towards prevention, proactive investigations and intelligence-led policing within the criminal justice system.[239]

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.

[238] 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.

[239] 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.