SECILE

Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness.

# D2.4 The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy

**Chris Jones & Ben Hayes (Statewatch)**

SECILE – Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness

**A Project co-funded by the European Union within the 7th Framework Programme – SECURITY theme**

**This project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 313195.**

## ABSTRACT

SECILE is an EU-funded research project examining the legitimacy and effectiveness of European Union counter-terrorism measures (CTMs). This report examines the implementation of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (the "Data Retention Directive"). The Directive obliges providers of internet and telephony services to keep detailed "traffic data" (or "metadata") regarding the identities and activities of their subscribers for between 6 and 24 months and provide access to police and security agencies for the purposes of investigating serious crime, and has been described as the "the most privacy-invasive instrument ever adopted by the EU". This report explains the policy-making process that resulted in the Directive, the obligations stemming from it, and the way these have been transposed into the national law of the member states with reference to infringement proceedings, legal challenges and the review of the legislation by the European Commission.

# TABLE OF CONTENTS

# 1 Introduction: the Data Retention Directive

The European Union's Data Retention Directive, adopted in 2006, obliges the Member States to ensure that telecommunications and Internet Service Providers (ISPs) retain various types of data generated by individuals through the use of landline phones, fax machines, mobile phones, and the internet, "in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime".[1]

The data that must be retained are:

- The source of a communication;
- The destination of a communication;
- The date, time and duration of a communication;
- The type of a communication;
- Users' communication equipment or what purports to be their equipment; and
- The location of mobile communication equipment.[2]

Data must be retained for a minimum of six months and a maximum of two years; it is left up to the Member States to decide the exact duration as well as the conditions under which it may be accessed. The European Data Protection Supervisor has called the Directive "without doubt the most privacy-invasive instrument ever adopted by the EU in terms of scale and the number of people it affects."[3] The Directive also ranks among the most controversial pieces of counter-terrorism legislation the EU has ever adopted and fierce debate as to its legitimacy and effectiveness has raged since the earliest stages of its drafting to the present day.[4]

An upcoming European Court of Justice decision will assess the extent to which the Directive is compatible with Articles 7 and 8 of the EU's Charter of Fundamental Rights (respect for private and

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[2] Centre for Strategy and Evaluation Services, 'Evidence of potential impacts of options for revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries', November 2012, p.7; see Article 5 of the Directive for full, technical details.

[3] European Data Protection Supervisor, 'The moment of truth for the Data Retention Directive', 3 December 2010, speech given at the conference 'Taking on the Data Retention Directive', https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf

[4] Privacy International and EDRi, 'Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention', 15 September 2004, http://www.statewatch.org/news/2004/sep/data-retention.htm; 'Data Retention Directive receives rubber stamp', *The Register*, 24 February 2006, http://www.theregister.co.uk/2006/02/24/data_retention_directive_ratified/; Joint letter to Cecilia Malmström from 106 NGOs arguing against the Data Retention Directive, 22 June 2010, http://www.statewatch.org/news/2010/jun/ngo-dataret-letter.pdf; AK Vorrat, 'Impossible to Ensure Legality of EU Communications Data Retention Directive says German Parliament', 26 April 2011, http://www.statewatch.org/news/2011/apr/eu-mand-ret-wp-on-dp-prel.pdf

family life and protection of personal data).[5] Privacy advocates and service providers opposed to the legislation are hoping that the Court will declare the Directive incompatible with those rights, following similar rulings in some national courts on legislation transposing the measure.

This report examines the policy-making process and the implementation of the Data Retention Directive at national level across the European Union. Section 2 provides an historical account of the circumstances leading up to the adoption of the Directive. Section 3 provides a clause-by-clause analysis of the Directive. Section 4 examines the data arising from the transposition and review of the Directive by the European Commission. Section 5 provides an overview of the legal action arising from the adoption and transposition of the Directive and Section 6 offers a brief conclusion. An appendix to this report contains an overview of the way the Directive has been transposed in the member states.

[5] European Court of Justice, 'Case C-293/12', 10 August 2012, http://curia.europa.eu/juris/document/document.jsf?text=&docid=125859&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=167537

## 2 The policy-making process

According to the preamble of the Data Retention Directive, the terrorist attacks in Madrid in March 2004 and in London in July 2005 "reaffirmed… the need to adopt common measures on the retention of telecommunications data as soon as possible."[6] However, law enforcement agencies had been seeking data retention legislation since well before the destruction of the World Trade Centre on 11 September 2001, and the Directive did not limit data retention to combating terrorism.

Demands for data retention can be traced back to the "International Law Enforcement and Telecommunications Seminars" (ILETS) held at the FBI academy in Quantico, Virginia, which commenced in 1993 with the aim of developing global "interception requirements" – standards for telephone-tapping by police and security agencies to be provided in all telephone networks.[7] Following the first ILETS meeting, the very first EU Council of Justice and Home Affairs (JHA) Ministers adopted a Resolution in November 1993 – which was not published – calling on experts to compare the needs of the EU vis-à-vis the interception of telecommunications "with those of the FBI".[8]

More 'requirements' formulated by the FBI and adopted by ILETS in 1994 formed the basis of a second EU Resolution on the interception of telecommunications adopted in January 1995. This Resolution introduced obligations on telecommunications companies to cooperate with law enforcement agencies in the "real-time" surveillance of their customers but was never actually discussed by the Council of Ministers; it was adopted instead by "written procedure" (where legislative texts are circulated among ministries and adopted if there are no objections). The Resolution, which was not published in any form until November 1996,[9] formed the basis of the provisions on the interception of telecommunications in the EU Convention on Mutual Legal Assistance of 2000. This Resolution was also cited by *Nokia Siemens Networks* in its response to complaints by human rights organisations that it had assisted the Iranian authorities in the surveillance of dissidents and protestors (NSN argued that it had simply provided the usual "backdoors" set out in the Resolution).[10]

The International Law Enforcement and Telecommunications Seminars continued every year and in 1999 identified a new problem.[11] They suggested that valuable "traffic data" – particularly mobile phone and internet usage records – were being erased by service providers after customers had

[6] Preamble, para. (10), Directive 2006/24/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[7] By 1995 ILETS had expanded to 20 countries: the United States, the 15 EU member states, Canada, Hong Kong, Australia and New Zealand .

[8] Permanent Representatives Committee (Part 2), 'Interception of telecommunications', 10090/93, 16 November 1993, http://database.statewatch.org/e-library/1994-jha-k4-03-06.pdf; held in the Statewatch European Monitoring and Documentation Centre (SEMDOC) JHA Archive, http://www.statewatch.org/semdoc/jha-archive.html

[9] Council Resolution of 17 January 1995 on the lawful interception of telecommunications, OJ 1996 C 329/01, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1996:329:FULL:EN:PDF

[10] 'Provision of Lawful Intercept capability in Iran', NSN Press Statement, 22 June 2009, http://nsn.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran.

[11] 'G8 and ILETS discussed problems of "data retention and implications of data protection legislation" in 1999', *Statewatch News Online*, May 2001, http://database.statewatch.org/article.asp?aid=6289

been billed, a problem that was particularly acute in the EU because of the recently enacted EC Directive on privacy in telecommunications, which obliged service providers to delete traffic data as soon as it had been used for billing purposes (usually within three months).[12] ILETS thus introduced the principle of mandatory data retention regimes that would oblige service providers to keep data for much longer periods.[13] This demand then surfaced in other intergovernmental fora concerned with police and judicial cooperation.[14] The *American Civil Liberties Union*, *Privacy International* and *Statewatch* would later dub this process "policy laundering".[15]

In 2000 the EU decided to update the aforementioned 1997 Directive on privacy in telecommunications to take into account "new technologies" and proposed what would become known as the "e-Privacy" Directive.[16] In line with ILETS and what were by now G8 demands, the draft Directive proposed to scrap the clause obliging service providers to delete traffic data after the "business need" had been met (the major obstacle to data retention). As a First Pillar matter (dealing with the functioning of the internal market), the European Parliament had what was then a rare vote on what was effectively a Justice and Home Affairs or Third Pillar issue (police surveillance).[17] Following an extensive campaign by privacy advocates the proposal was initially rejected out of hand.[18] However in 2002, with the events of 11 September 2001 providing a fresh justification for the proposal, a left-right alliance of the European Socialist Party (PSE) and the European People's Party (PPE) agreed the e-Privacy Directive and the critical "data retention amendment", with the liberals, greens and left parties opposed.[19]

---

[12] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:024:0001:0008:EN:PDF

[13] 'G8 and ILETS discussed problems of "data retention and implications of data protection legislation" in 1999', *Statewatch News Online*, May 2001, http://database.statewatch.org/article.asp?aid=6289

[14] 'Data protection or data retention in the EU?', *Statewatch Bulletin*, Vol. 11 No. 3/4, May-July 2001, http://www.statewatch.org/news/2001/sep/dataprot.pdf; '"Secret plan to spy on all British phone calls": UK fronts G8 plan for records to be kept for 7 years', *Statewatch News Online*, 3 December 2000, http://database.statewatch.org/article.asp?aid=6262; 'Preview of the G8-meeting in Gleneagles', *EDRi*, 2005, http://www.edri.org/book/export/html/616

[15] "Policy laundering", after "money laundering", describes "the use by governments of foreign and international forums as an indirect means of pushing policies unlikely to win direct approval through the regular domestic political process". Under the "war on terror", this technique became a central means by which states seek to overcome civil liberties objections to privacy-invading policies. A critical feature of policy laundering is "forum shifting", which occurs "when actors pursue roles in intergovernmental organisations (IGOs) that suit their purposes and interests, and when opposition and challenges arise, shift to other IGOs or agreement-structures". See the *Policy Laundering Project*, 2005, http://www.policylaundering.org).

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[17] Prior to the Amsterdam treaty, the European Parliament had barely been consulted on JHA policies. After Amsterdam consultation was more structured and co-decision was gradually phased in. See also: Francesca Bignami, 'Protecting Privacy Against the Police in the European Union: The Data Retention Directive' in Yves Bot et al. (eds.), *Melanges en l'Honneu' de Philippe Leger: le droit a la mesure de l'homme 109*, 2006, p.113, http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1340&context=faculty_publications

[18] 'Data protection or data retention in the EU?', *Statewatch Bulletin*, Vol. 11 No. 3/4, May-July 2001, http://www.statewatch.org/news/2001/sep/dataprot.pdf

[19] 'European Parliament caves in on data retention', *Statewatch News Online*, May 2002, http://database.statewatch.org/article.asp?aid=6423

This paved the way for those member states that wished to do so to begin to introduce their own national data retention regimes. Yet no sooner was the ink dry on the e-Privacy Directive than a confidential draft Framework Decision on the compulsory retention of subscriber and traffic data for 12-24 months across the EU was circulated among member states and leaked by *Statewatch*, which published the text on its website.[20] Following widespread criticism of the proposal in European media, the then Danish presidency of the EU was moved to issue a statement saying that the proposal was "not on the table". Although apparently not 'on the table', the proposal appears to have remained close at hand, as indicated by the fact that in the immediate aftermath of the Madrid train bombings in March 2004, the "EU Declaration on combating terrorism" endorsed the principle of mandatory data retention across the EU.[21] The writing was now on the wall and one month later the UK, France, Sweden and Ireland submitted a revised draft Framework Decision on data retention to the Council.[22] By now, a majority of EU member states had also introduced national data retention regimes.[23]

Nevertheless the EU proposal would soon suffer another major setback when *Statewatch* published the confidential legal advice of the EU Council and Commission Legal Services, both of which had been withheld from MEPs and the public despite stating that the Framework Decision was unlawful because it had the wrong legal basis.[24] Data retention, said the EU's lawyers, was a First Pillar issue because it regulated the activities of service providers in the single market. The European Commission, which had previously stated its opposition to data retention, duly redrafted the proposal as a Directive.[25] This complicated things further still because whereas the European Parliament was only consulted on the draft Framework Decision, with the EU Council free to ignore its opinion on the legislation, it would now enjoy full powers of "co-decision". Moreover, during the consultation process on the Framework Decision, the Parliament had voted to reject mandatory data retention because it was "incompatible with Article 8" of the ECHR, stating that:

---

[20] 'EU: data retention to be "compulsory" for 12-24 months - draft Framework Decision leaked to Statewatch', *Statewatch News Online*, July 2002, http://database.statewatch.org/article.asp?aid=6458

[21] 'EU Plan of Action on Combating Terrorism', EU Council document 10586/04, 15 June 2004. See further 'Commentary on the evolution of EU Counter-terrorism' in Deliverable D 2.1.

[22] Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism', EU Council document 8958/04, 20 December 2004.

[23] 'Majority of governments introducing data retention of communications', *Statewatch News Online*, January 2003, http://database.statewatch.org/article.asp?aid=6635

[24] 'Projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme - Base juridique', 7688/05, 5 April 2005, http://www.statewatch.org/news/2005/apr/Council-legal-opinion-data-retention.pdf; see also 'EU: Data Retention proposal partly illegal, say Council and Commission lawyers', *Statewatch News Online*, April 2005, http://www.statewatch.org/news/2005/apr/02eu-data-retention.htm and 'Secret Minutes EU Data Retention Meeting', *EDRi-gram*, 6 April 2005, http://www.edri.org/edrigram/number3.7/retention

[25] European Commission, '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, 21 September 2005, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0438en01.pdf

> "The monitoring and storage of data must be rejected if the measures do not comply with three basic criteria in line with the European Court of Human Rights' interpretation of Article 8(2) of the [ECHR]: they must be laid down by law, necessary in a democratic society and serve one of the legitimate purposes specified in the Convention. As has already been illustrated, it is debatable, to say the least, whether the proposal fulfils all the necessary criteria".[26]

However, between the defeat of the proposal for a Framework Decision and the publication of the proposal for a Directive, the July 2005 London tube bombings happened. These were used as a fresh justification for an EU data retention law, although the UK prime minister suggested at the time that "all the surveillance in the world" could not have prevented the attacks.[27]

The UK then used its presidency of the EU Council to impose a deadline of the end of 2005 for the European Parliament to agree the measure, with Charles Clarke, UK Secretary of State, lecturing the EP on the need to adopt the proposal and Home Office officials were reported to have told MEPs in private that if parliament failed to do this they "would make sure the European Parliament would no longer have a say on any justice and home affairs matter."[28]

Led by *Privacy International* and the *European Digital Rights Initiative*, 90 NGOs and 80 telecommunications service providers wrote to the MEPs, imploring them to reject the measure:

> "The retention of personal data resulting from communications, or of traffic data, is necessarily an invasive act. With the progress of technology, this data is well beyond being simple logs of who we've called and when we called them. Traffic data can now be used to create a map of human associations and more importantly, a map of human activity and intention. It is beyond our understanding as to why the EU Presidency and some select EU Member States insist on increasing the surveillance of traffic data even as this data becomes more and more sensitive, concomitant to a decreasing regard for civil liberties…
>
> "… the European Parliament now faces a crucial decision. Is this the type of society we would like to live in? A society where all our actions are recorded, all of our interactions may be mapped, treating the use of communications infrastructures as criminal activity; just in case that it may be of use at some point in the future by countless agencies in innumerable countries around the world with minimal oversight and even weaker safeguards".[29]

---

[26] European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism', A6-0174/2005, 31 May 2005, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//EN

[27] Simon Davies, 'Unlawful, unworkable, unnecessary', *The Guardian*, 13 July 2005, http://www.theguardian.com/world/2005/jul/13/humanrights.july7

[28] Statewatch Observatory, 'The surveillance of telecommunications in the EU (from 2004 and ongoing), http://www.statewatch.org/eu-data-retention.htm; see also: 'Europarl Protests Against UK Push For EU Data Retention', *EDRi-gram*, 14 July 2005, http://www.edri.org/edrigram/number3.14/retention. The EP was at the time seeking a greater role in decision-making on all aspects of JHA policy.

[29] [29] Privacy International and EDRi, 'Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention', 15 September 2004, http://www.statewatch.org/news/2004/sep/data-retention.htm

The EP finally agreed the measure on 14 December 2005, with another alliance between the PSE and PPE reversing the position on the draft Framework Decision that the parliament had taken just eight months earlier.[30] The Directive then completed its passage through parliament following a single reading to meet the UK's demands. The Council of the EU adopted the legislation by qualified majority, with Ireland and the Slovakia voting against, and the Directive passed into law in March 2006.

Two further observations are relevant to any substantive consideration of the policy-making process. The first concerns the role of the UK government, which took its attempts to enforce data retention to EU institutions after it had been prevented from a domestic mandatory data retention regime by the houses of parliament.[31] In what appears to be a case of "policy laundering", the subsequent EU Directive, championed by the UK government, was binding on the UK and eligible to be implemented by statutory instrument in accordance with the European Communities Act 1972.[32]

The second observation concerns the role played by the US government in pushing for mandatory data retention in Europe, bilaterally in its discussions with the European Commission and EU Presidency,[33] and in multilateral fora like the G8.[34] This is noteworthy because at that time there

[30] For a discussion that argues Parliament's agreement to data retention came about through a desire "to be seen as a 'responsible' legislator", see Ariadna Ripoll Servent, 'Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision', *Journal of European Public Policy*, Vol. 20, No. 7, 2013, pp.972-987

[31] UK police and security agencies are empowered to access data held by telecommunications service providers under the Regulation of Investigatory Powers Act 2000. A statutory basis for extended data retention was established by the Anti-Terrorism, Crime and Security Act 2001 (ATCS), adopted after the 9/11 attacks, but parliament restricted the Home Secretary's powers to a "voluntary" code of practice – which many service providers chose to ignore – and insisted on a five year sunset clause. In 2002 the All Party Internet Group (APIG), comprising over 50 Members of Parliament and the House of Lords, raised "significant doubt that the whole scheme is lawful" and recommended "very strongly" that the Home Office drop its plans on voluntary or mandatory data retention schemes in favour of and "urgently enter into Europe-wide discussions to dismantle data retention regimes and to ensure that data preservation becomes EU policy". See 'U-turn on UK data retention law?', Outlaw.com, 29 January 2003, http://www.out-law.com/page-3277. The government ignored the APIG and enacted the Voluntary Code of Practice on Data Retention on 5 December 2003 by Statutory Instrument 2003/3175.

[32] The Data Retention (EC Directive) Regulations 2007 (http://www.legislation.gov.uk/uksi/2007/2199/contents/made); The Data Retention (EC Directive) Regulations 2009 (http://www.legislation.gov.uk/uksi/2009/859/introduction/made). The Regulations formalised the voluntary code already and extended the retention period from six to 12 months. They were subject to the affirmative resolution procedure, by which instruments "cannot become law unless they are approved by both Houses," i.e. the Commons and the Lords. However, there is no requirement for a parliamentary debate and the only debate that did take place occurred within 18-member Delegated Legislation Committees. The Regulations were "nodded through" both chambers. The transcript of the debate in 2007 is not available online but can be purchased: http://www.tsoshop.co.uk/bookstore.asp?Action=Book&ProductId=9780215785404. The 2009 debate can be found here: http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm. See further Statewatch Analysis, 'Mandatory retention of telecommunications traffic to be "nodded" through in UK', May 2007, http://www.statewatch.org/news/2007/may/uk-data-ret.pdf.

[33] In October 2001 the President of the United States wrote to the European Commission with a further 40 specific requests regarding cooperation on anti-terrorism measures. 'Text of US letter from Bush with demands for EU for cooperation', *Statewatch News Online*, November 2001, http://database.statewatch.org/article.asp?aid=6344. Structured dialogue on counter-terrorism between the EU and USA continued in the framework of the New Transatlantic Agenda.

were no corresponding powers in the USA, nor any intention to introduce them. Even the notorious PATRIOT Act did not go this far. In place of blanket "data retention", US law enforcement and security agencies are obliged to seek "preservation orders" from special surveillance courts. However, recent leaks such as that of the FISA court order imposed on *Verizon*, demonstrate that US agencies and their special "surveillance court" have interpreted these principles so widely as to cover entire telephone networks and all of their users.[35]

Opposition to the Data Retention Directive in Europe included advocacy from civil society organisations for the development of this model as an alternative framework for communications surveillance in the EU, with judicial supervision supposed to ensure that access to private data is necessary and legitimate. This is still the preferred option of the German Ministry of Justice (see further section 5.6, below).

[34] 'G8 and ILETS discussed problems of "data retention and implications of data protection legislation" in 1999', *Statewatch News Online*, May 2001, http://database.statewatch.org/article.asp?aid=6289
[35] 'NSA collecting phone records of millions of Verizon customers daily ', Guardian, 6 June 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order

# 3 Clause-by-clause analysis

Article 1 sets out the subject matter and scope of the Directive covers which covers all legal entities and:

> "aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."

Article 1(1) of the Directive states that serious crime is "as defined by each Member State in its national law". Article 1(2) states that the Directive does not apply to the retention of the content of communications. However, it has long been argued that "retaining traffic data makes it possible to reveal… what websites people have visited", indicating that certain content data can actually be retained under the Directive.[36] The EU's "Article 29 Working Party" on data protection was so concerned that it issued an Opinion in 2008 making it clear that the Directive is "not applicable to search engine providers", as "search queries themselves would be considered content rather than traffic data and the Directive would therefore not justify their retention."[37]

Article 2 contains definitions of the terms used in the legislation, and Article 3 outlines the obligation for telecoms providers to retain data, through derogation from a number of Articles (5, 6 and 9) of the e-Privacy Directive.[38] Article 5 of that Directive obliges Member States to:

> "[E]nsure the confidentially of communications and the related traffic data by means of a public communications network and publicly available electronic communications services" through the prohibition, except when legally authorised, of "listening, tapping, storage or other kinds of interception or surveillance."

Article 6 of the e-Privacy Directive prohibits the retention by telecommunications providers of "traffic data relating to subscribers and users" except if necessary for billing or for marketing (where the subscriber or user has given their consent). Article 9 states that location data that relates to users or subscribers "may only be processed when they are made anonymous, or with the consent of the users of subscribers to the extent and for the duration necessary for the provision of a value added service."

Article 4 of the Data Retention Directive covers access by Member States' competent authorities to retained data, which should only occur "in specific cases and in accordance with national law". The phrase "competent authorities" is undefined in the Directive and it has been left to Member States to decide which of their agencies and institutions should have access to retained data and the ability

[36] Open Rights Group, 'Data Retention Directive', http://wiki.openrightsgroup.org/wiki/Data_retention_directive#Summary_of_issues_with_the_directive

[37] Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, 00737/EN WP 148, 4 April 2008, p.3

[38] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communiations)

to request it from telecommunications providers (see further section 4.2, below). It is also left entirely to Member States to define what procedures the authorities should follow if they are to be given access to retained data. This has led to wide divergence in which authorities can access the retained data, and how they do so. The Directive's failure to stipulate that national law should include judicial scrutiny of requests for retained data allows member states to establish self-regulatory systems that dispense with the traditional use of surveillance "warrants".

Article 5 states in detail the data that must be retained by service providers, as outlined in the introduction of this report. Article 6 covers periods of retention ("not less than six months and not more than two years from the date of the communication"), and Article 7 outlines measures for the protection and security of retained data: it should be "of the same quality and subject to the same security and protection as those data on the network"; it should be protected against "accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure"; should be accessible only by "specially authorised personnel"; and must be destroyed at the end of the retention period unless "accessed and preserved". Compliance with these provisions is to be supervised by "one or more public authorities" in accordance with Article 9.

Article 8 states that the storage of retained data must allow for its transmission to competent authorities, when requested, "without undue delay". Article 10 obliges Member States to provide to the Commission with statistics, excluding personal data, on an annual basis. These should include:

- The cases in which information was provided to the competent authorities in accordance with applicable national law;
- The time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data;
- The cases where requests for data could not be met.

Article 11 makes an amendment to Article 15 of the e-Privacy Directive, paragraph 1 of which permits Member States to enact their own data retention measures if they consider them:

> "[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."

The Data Retention Directive supplemented this by stating that: "Paragraph 1 shall not apply to data specifically required by [the Data Retention Directive] to be retained for the purposes referred to in Article 1(1) of that Directive." The confusion caused by this overlap in the two pieces of legislation has been problematic and the European Commission, which is now reviewing the Data Retention and e-Privacy Directives in parallel, has suggested that:

> "Any revision of the Data Retention Directive should ensure that retained data will be used exclusively for the purposes foreseen in this Directive, and not for other purposes as currently allowed by the e-Privacy Directive."[39]

[39] 'Revision of Data Retention Directive put on hold with "no precise timetable" for a new proposal, *Statewatch News Online*, August 2012, http://database.statewatch.org/article.asp?aid=31781

Article 12 permits Member States to extend the period of retention for "a limited period" if they face "particular circumstances", subject to the *post-facto* approval of the Commission. Article 13 obliges Member States to ensure that provisions of EU data protection law dealing with judicial remedies, liabilities and sanctions[40] apply to the measures enacted by Member States to transpose the Data Retention Directive. It also requires the punishment by "penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive," of any illegal access to or transfer of retained data.

Article 14 obliged the Commission to undertake "an evaluation of the application of this Directive and its impact on economic operators and consumers" and present it to the European Parliament and the Council no later than 15 September 2010. The evaluation, which is examined in the following section, was produced in April 2011. Article 14 also obliged the Commission to determine at this time "whether it is necessary to amend the provisions of this Directive", a decision that the Commission has deferred leaving no precise timetable for a new proposal.[41]

Articles 15-17 require Member States to transpose the Directive into national law by 15 September 2007 (it was agreed on 15 March 2006 and entered into force 20 days later), with sub-section (3) of Article 15 allowing member states to "postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail" for up to three years.

[40] Chapter III, 'Judicial remedies, liability and sanctions', Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[41] 'Revision of Data Retention Directive put on hold with "no precise timetable" for a new proposal', *Statewatch News Online*, 13 August 2012, http://database.statewatch.org/article.asp?aid=31781

# 4 Transposition and review

Member States were required to ensure their national law complied with the requirements of the Data Retention Directive by 15 September 2007, with the option of extending that period until 15 March 2009 with regard to the retention of internet access, internet telephony and internet email. Austria, Belgium, Cyprus, Czech Republic, Estonia, Finland, Germany, Greece, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Slovenia, Sweden and the UK all took up this option. The specific legislation through which Member States transposed the Directive is listed in the EUR-Lex register.[42]

The process of transposing the Directive has been lengthy and controversial in many member states, not least because of the various legal challenges to the implementing legislation brought on procedural, constitutional and human rights grounds detailed in the following section. Six years after the deadline for implementation, the Directive has still not been implemented by all the states it covers and genuine "harmonisation" appears a remote prospect.

Even with the extra room for manoeuvre on internet data retention, six member states still found themselves subjected to infringement proceedings brought by the Commission after failing to implement national legislation in the allotted timeframe. The Commission initiated infringement proceedings against Austria, the Netherlands and Sweden in May 2009, Greece and Ireland in November 2009, and Germany in May 2012. Austria,[43] Greece,[44] the Netherlands,[45] Ireland[46] and Sweden[47] subsequently adopted the requisite legislation; Germany has still failed to introduce legislation and an infringement action is pending at the European Court of Justice (see further section 5.6 below).

In Norway (which is not an EU Member State but is obliged to implement the Directive as a member of the European Economic Area) legislation is yet to be adopted, and there is an on-going campaign

[42] Data Retention Directive National Execution Measures, *EUR-Lex*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:EN:NOT

[43] Jan Libbenga, 'Sweden postpones EU data retention directive, faces court, fines', *The Register*, 18 March 2011, http://www.theregister.co.uk/2011/03/18/sweden_postpones_eu_data_retention_directive/

[44] Transposition in Greece was completed with the passing of Law 3917/2011 after an ECJ ruling imposing a fine (Case C-211/09). All data retained under the law is to be held for 12 months and a court order is required for access. For more information see: Karageorgiou & Associates, 'Data protection in Greece – key issues', May 2011, http://www.kalaw.gr/wmt/userfiles/File/Overview_Greece_2011.pdf

[45] The Netherlands introduced transposing legislation on 1 September 2009 with the *Wet bewaarplicht telecommunicatiegegevens*. Amending legislation passed in July 2011 shortened the retention period for data on Internet access, email and Internet telephony to six months. All other data is retained for 12 months. For more information see: Law Library of Congress, 'Netherlands: Mandated Period of Provider Retention of Internet Data Shortened', 25 July 2011, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205402757_text

[46] The relevant Irish legislation is the Communications (Retention of Data) Act 2011. This legislation, as well as the Data Retention Directive, was the subject of a subsequent court challenge, discussed in section 3.8. The full text of the Communications (Retention of Data) Act 2011 is available at: http://www.irishstatutebook.ie/2011/en/act/pub/0003/index.html

[47] See section 3.9 below.

by civil society organisations to try and prevent its adoption by the parliament.[48] The Commission also recently demanded that Belgium "change its data retention laws to comply with the provisions of the European legislation",[49] and a draft bill aimed at ensuring full implementation through modification of the Electronic Communications Act of 13 June 2005 was subsequently introduced into the Belgian Parliament in July of 2013.[50]

The Directive required the European Commission to undertake "an evaluation of the application of this Directive and its impact on economic operators and consumers" and present it to the European Parliament and the Council of the EU no later than 15 September 2010. A conference entitled "Taking on the Data Retention Directive", at which different "stakeholders" were invited to give their views, was held in December 2010.[51] The evaluation report was finally published in April 2011.[52] To the disappointment of civil liberties and privacy groups, the Commission concluded that:

> "Overall, the evaluation has demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU. The contribution of the Directive to the harmonisation of data retention has been limited, in terms of, for example, purpose limitation and retention periods, and also in the area of reimbursement of costs incurred by operators, which is outside its scope."[53]

[48] Lyndsey Smith and Michael Sandelson, 'Norway oppositions fights EU Data Retention Directive', *The Foreigner*, 25 July 2013, http://theforeigner.no/pages/news/norway-opposition-fights-eu-data-retention-directive/

[49] Frédéric Donck, 'EU Issues Overview – 25-31 May 2013 Edition', *Internet Society*, 3 June 2013, http://www.internetsociety.org/doc/eu-issues-overview-%E2%80%93-25-31-may-2013-edition

[50] 'Belgium – Further proposals to implement the EU Data Retention Directive', *Linklaters*, 18 July 2013, http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-News-18-July-2013/Pages/Belgium-Further-proposals-implement-EU-Data-Retention-Directive.aspx

[51] 'Note on the consultation meeting', 3 December 2010, http://www.statewatch.org/eu-data-retention.htm

[52] European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', COM(2011) 225 final, 18 April 2011, http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf

[53] European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', p.2

## 4.1 Retention period and scope

That the Directive failed to harmonise retention periods is hardly surprising given that it allowed member states to choose from anywhere between 6 and 24 months. In the absence of an EU definition of "serious crime", the requirement that retained data be used for "the investigation, detection and prosecution of serious crime" was unlikely to achieve harmonisation either. According to the Commission's evaluation:

> "Ten Member States (Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, Netherlands, Finland) 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. Eight Member States (Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, Slovenia) 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 for crime prevention, or on general grounds of national or state and/or public security. The legislation of four Member States (Cyprus, Malta, Portugal, UK) refers to 'serious crime' or 'serious offence' without defining it."[54]

The Commission also noted that most member states "allow the access and use of retained data for purposes going beyond those covered by the Directive, including preventing and combating crime generally and the risk of life and limb".[55]

## 4.2 Access to retained data

The authorities permitted to access retained data differ significantly from state to state. Every member state allows their police forces access and all member states except the UK and Ireland give access to prosecutors.[56] Fourteen states provide access to their security and intelligence services (although only twelve are easily identifiable in the report);[57] six to tax and/or customs authorities;[58] four to border police (the Commission claims three despite the information it provides showing otherwise);[59] while the UK allows other public authorities to access data retained by telecoms providers if "authorised for specific purposes under secondary legislation."[60]

The type of authorisation required for access by these authorities is similarly uneven across the EU: "Eleven Member States require judicial authorisation for each request for access to retained data. In three Member States judicial authorisation is required in most cases".[61] A senior authority, but not a

[54] Ibid., p.6
[55] Ibid., p.8
[56] Ibid., p.9
[57] The twelve identifiable states are Bulgaria, Estonia, Spain, Latvia, Lithuania, Luxembourg, Hungary, Malta, Poland, Portugal, Slovenia and the UK. See tables in pages 10-12 of the Commission report.
[58] Finland, Hungary, Ireland, Poland, Spain, UK.
[59] Estonia, Finland, Poland, Portugal.
[60] European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', p.12
[61] Ibid., p.9. The information provided in the report is not specific enough to make it possible to identify exactly which states these are.

judge, must give authorisation in four other Member States[62] while in two Member States, "the only condition appears to be that the request is made in writing."[63]

## 4.3 Necessity and effectiveness

The European Commission's review declared the Data Retention Directive "a valuable tool for criminal justice systems and for law enforcement in the EU"[64] while acknowledging that the civil society groups who took part in its consultation considered the policy "in principle… unjustified and unnecessary".[65] In spite of the pending judgment of the European Court of Justice (see section 5.10, below), EC Home Affairs Commissioner Cecilia Malmström has stated that "data retention is here to stay".[66] This has not, however, allayed concerns about either the legitimacy or effectiveness of the Directive.

In May 2011 the European Data Protection Supervisor issued a formal Opinion on the Commission's evaluation report, stating that, amongst other things, before proposing a revised Directive the Commission needed to "invest in collecting further practical evidence from the Member States in order to demonstrate the necessity of data retention as a measure under EU law", and that all those Member States in favour of data retention should "provide the Commission with quantitative and qualitative evidence demonstrating it".[67] This demand has also come from European Court of Justice in its review of the Directive.[68]

In December 2011 the European Commission wrote to the EU Council's Working Party on Data Protection and Information Exchange (DAPIX), to inform member states' representatives as to the results of the consultation undertaken by the Commission from May to December 2011 on the reform of the Data Retention Directive. The Commission explained:

> "[T]here are serious shortcomings with the EU framework – including retention periods, clarity of purpose limitation and scope, lack of reimbursement of cost to industry, safeguards for access and use – which must be addressed."[69]

[62] Information provided by *five* states – Cyprus, France, Hungary, Italy and Poland – would appear to fit this description.
[63] Information provided by three states fits this description: Ireland, Malta and Slovakia.
[64] European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', p.1
[65] Ibid., p.29
[66] Cecilia Malmström, 'Taking on the Data Retention Directive', 3 December 2010, http://europa.eu/rapid/press-release_SPEECH-10-723_en.htm
[67] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May 2011, http://www.statewatch.org/news/2011/may/edps-opinion-eu-mand-ret-opinion.pdf
[68] Monika Emert, 'Data retention might not be proportional to risks', *Policy Review*, 9 July 2013, http://policyreview.info/articles/news/data-retention-might-not-be-proportional-risks/170
[69] Commission Services, 'Consultation on reform of Data Retention Directive: emerging themes and next steps', 18620/11, 15 December 2011, p.8, http://www.statewatch.org/news/2012/jan/eu-mand-ret-com-consult-18620-11.pdf

The Commission argued that it was necessary to "explain better the value of data retention" due to "a continued perception that there is little evidence at an EU and national level on the value of data retention in terms of public security and criminal justice":

> "We have received strong views from law enforcement and the judiciary from all Member States that communications data are crucial for criminal investigations and trials, and that it was essential to guarantee that these data would be available if needed for at least 6 months or at least… 1 year. We have also received strong qualitative evidence of the value of historic communications data in specific cases of terrorism, serious crime and crimes using the internet or by telephone – but only from 11 out of 27 Member States."[70]

Furthermore, "[t]he statistics required under Article 10 do not, as it is currently interpreted, enable evaluation of necessity and effectiveness". Therefore, the Commission concluded, "all Member States – not just a minority – need to provide convincing evidence of the value of data retention of security and criminal justice".[71] Member States' delegations in DAPIX had already discussed the need for further evidence of the "necessity" of data retention at a meeting in May 2011. They concluded that the need for the policy:

> "[C]ould not be argued on the basis of statistical data… the gravity of the offences investigated thanks to traffic data, rather than the mere number of cases in which traffic data were used should receive due attention. Quantitative analysis should be complemented with qualitative assessment."[72]

In March 2013 the Commission published a report that attempted to draw together "Evidence which has been supplied by Member States and Europol in order to demonstrate the value to criminal investigation and prosecution of communications data retained under Directive 2006/24/EC."[73] The report contains an overview of the ways in which communications data are used in criminal investigations and judicial proceedings; the sorts of cases in which retained data are important; the "consequences of absence of data retention"; and then comes to a section on statistics and quantitative data. This notes that 23 Member States have provided "some statistics since 2008", and that since 2009 these have mostly been submitted in line with a template drawn up the Commission's "expert group" on data retention[74] in November 2008 and presented to Member States in January 2009. Nevertheless, the Commission found that member states "interpret in

[70] Ibid., p.2-3
[71] Ibid., p.8
[72] Working Party on Data Protection and Information Exchange, 'Summary of discussions', 30 May 2011, 10806/11, p.3, http://register.consilium.europa.eu/pdf/en/11/st10/st10806.en11.pdf
[73] European Commission, 'Evidence for necessity of data retention in the EU', March 2013, p.2, http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf
[74] From March 2008 to December 2012 this group's mandate came from Commission Decision 2008/324/EC of 25 March 2008 setting up the 'Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime' group of experts, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:111:0011:0014:EN:PDF; in April 2013 a new basis was established through a Commission Decision of 18 April 2013 on setting up an experts group on best practice in the implementation of electronic communications data retention for the investigation, detection and prosecution of serious crime ('the data retention experts group'), http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/20130418_data_retention_expert_group_decision_en.pdf

different ways terms from the DRD such as 'case' and 'request', and statistics vary in format which limits their comparability".[75]

Statistics published by the Commission on the application of the Directive in 2010, the latest year for which figures are available, suggests that even with the template, only eight of the 27 member states are able to provide data in anything like the requested format, with twelve states providing no data at all and one providing a single "approximate number" for the entire exercise.[76] What the statistics do show is massive variation in the extent that member states are using their data retention powers, with total annual requests ranging from 23 (Portugal) to 777,040 (UK).[77] In November 2012 – six years after the adoption of the Directive – the expert group adopted and disseminated "more comprehensive guidance on provision of statistics under Article 10, which the Commission encourages all Member States to follow".[78]

In its 2013 report on "Evidence demonstrating the value of data retention,[79] the Commission suggested that "an undue focus on such statistics can be counterproductive to the effectiveness of law enforcement" and that in any case it would be "impossible to identify meaningful statistical trends… only a few years after the DRD entered into force."[80] The majority of the report (20 of 30 pages) was therefore given over to anecdotal evidence, submitted in line with a February 2012 request from the Commission which set out "specific guidance – consistent with the deliberations of the expert group – on qualitative and quantitative evidence to be provided."[81] The report includes 91 reported cases from across Europe in which retained data assisted in finding the perpetrators of a variety of serious crimes.

## 4.4 Alternative approaches

"Data preservation" regimes offer an alternative means of communications surveillance to data retention, by limiting the data that service providers are forced to collect data to specific investigations. This system has been under consideration in Germany following difficulties in transposing the Directive.

In November 2012 the European Commission published a report it had commissioned on "current approaches to data preservation in EU Member States and third countries".[82] Data preservation was defined as the "expedited preservation of stored data or 'quick freeze'" in:

[75] European Commission, 'Evidence for necessity of data retention in the EU', March 2013, p.7, http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf
[76] 'Data Retention Statistics 2010', European Commission, undated, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/publication_data_retention_statistics_20120228_without_es_en.pdf
[77] Ibid, p.5.
[78] Ibid., p.9
[79] European Commission, 'Evidence for necessity of data retention in the EU', March 2013, p.2, http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf
[80] European Commission, 'Evidence for necessity of data retention in the EU', March 2013, p.8, http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf
[81] Ibid., p.9
[82] Centre for Strategy & Evaluations Services, 'Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries', November

> "situations where a person or organisation (which may be a communications service provider or any physical or legal person who has the possession or control of the specified computer data) is required by a state authority to preserve specified data from loss or modification for a specific period of time".

The report explained that data preservation is already mandated by the Council of Europe Convention on Cybercrime (also known as the "Budapest Convention"),[83] which entered into force on 1 July 2004 and is open for worldwide signature. All EU Member States have signed the Convention although Greece, Ireland, Luxembourg, Poland and Sweden still need to ratify it (as of 29 November 2012).[84] Under the Convention data may be preserved "for the purpose of specific criminal investigations or proceedings".[85] The Convention, unlike the Data Retention Directive, explicitly permits the storage of communication content.

While the German Ministry of Justice believes that data preservation is fundamentally an alternative to mandatory retention (see further section 5.6, below), the report concludes that "data retention and data preservation are complementary rather than alternative instruments… data retention plays a role in ensuring that data is kept and that this is sometimes a prerequisite for data preservation, as data may have already been deleted before a data preservation order is issued."[86]

## 4.5 Revision of the Directive

Article 14 requires the European Commission to determine, on the basis of its review, whether it is necessary to amend the provisions of the Data Retention Directive. In August 2012 the Commission announced that it was postponing the revision of the Data Retention Directive with "no precise timetable" for a new proposal. The Commission spokesperson cited the need to review the "e-Privacy" Directive to "ensure that retained data will be used exclusively for the purposes foreseen in this Directive, and not for other purposes as currently allowed by the e-Privacy Directive."[87]

Before the revision of either of these two Directives takes place, however, the Commission wants to see its draft data protection package agreed by the Council and the Parliament. At present the two institutions disagree significantly on the proposal, with further disagreement amongst the member states in the Council.[88] By this time the Court of Justice will also have ruled on the fundamental rights challenge to the Data Retention Directive.

---

2012, p.4, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf

[83] Council of Europe Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[84] Council of Europe, 'Convention on Cybercrime', http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

[85] Ibid., p.7

[86] Ibid., p.23

[87] 'Revision of Data Retention Directive put on hold with "no precise timetable" for a new proposal', *Statewatch News Online*, 13 August 2012, http://database.statewatch.org/article.asp?aid=31781

[88] John Burn-Murdoch, 'Europe deadlocked over data protection reform', *The Guardian*, 12 August 2013, http://www.theguardian.com/news/datablog/2013/aug/12/europe-data-protection-directive-eu

# 5 Legal challenges

## 5.1 EU Court of Justice legal basis challenge

The first legal challenge to the Data Retention Directive came when Ireland, supported by Slovakia, asked the EU Court of Justice to annul the Directive on the grounds that it had not been adopted on an appropriate legal basis. Ireland had been a signatory to the original draft Framework Decision on data retention (see section 2, above) and with the Slovak republic had voted against the draft Directive during the legislative proceedings in the Council. They argued that the EU's lawyers had been wrong in their advice that the issue was matter for EC law on the functioning of the internal market and submitted that correct legal basis for data retention resided "in the provisions of the EU Treaty concerning police and judicial cooperation in criminal matters".[89] The ECJ dismissed the case in February 2009, stating that:

> "Directive 2006/24… regulates operations which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonises neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities…
>
> "It follows that the substantive content of Directive 2006/24 is directed essentially at the activities of the service provides in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty."[90]

## 5.2 Bulgaria

The first ruling on national laws transposing the Data Retention Directive came from Bulgaria in proceedings launched by the NGO *Access to Information Program*. In December 2008 the country's Supreme Administrative Court annulled an article of the transposing legislation permitting the Ministry of Interior "passive access through a computer terminal" to retained data, as well as providing access without judicial permission to "security services and other law enforcement bodies".[91] The court found that:

---

[89] ECJ press release No 70/08, 'Advocate General Bot considers that the Directive on Data Retention is founded on an appropriate legal basis', 14 October 2008, http://www.statewatch.org/news/2008/oct/eu-data-ret-ag-ecj-opinion.pdf

[90] Judgment of the Court(Grand Chamber), Ireland v Parliament and Council, C-301/06, 10 February 2009, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5ef438a96eaae4a758e64c4539c3fa658.e34KaxiLc3eQc40LaxqMbN4OahmTe0?text=&docid=72843&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=615870. See also ECJ press release No 70/08, 'Advocate General Bot considers that the Directive on Data Retention is founded on an appropriate legal basis', 14 October 2008, http://www.statewatch.org/news/2008/oct/eu-data-ret-ag-ecj-opinion.pdf and Opinion of Advocate General Bot, Case C-301/06, 14 October 2008, http://curia.europa.eu/juris/document/document.jsf?text=&docid=66649&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=170367

[91] According to an EDRi report: 'Bulgarian Court Annuls A Vague Article Of The Data Retention Law', *EDRi-gram*, 17 December 2008, http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

> "[T]he provision did not set any limitations with regard to the data access by a computer terminal and did not provide for any guarantees for the protection of the right to privacy stipulated by Art. 32, Para. 1 of the Bulgarian Constitution. No mechanism was established for the respect of the constitutionally granted right of protection against unlawful interference in one's private or family affairs and against encroachments on one's honour, dignity and reputation."[92]

The court also found the legislation failed to make reference to other relevant laws – the Penal Procedure Code, the Special Surveillance Means Act and the Personal Data Protection Act – "which specify conditions under which access to personal data shall be granted."[93] The court ruled that:

> "[N]ational legal norms shall comply with that established principle [limitations on rights permitted by Article 8(2) of the European Convention Human Rights] and shall introduce comprehensible and well formulated grounds for both access to the personal data of citizens and the procedures for their retention. Article 5 of the Regulation lacks clarity in terms of protection of the right of private and family life which contradicts the provision of Article 8 of the ECHR, the texts of the Directive 2006/24/EC, and Articles 32 and 34 of the Bulgarian Constitution."[94]

## 5.3 Hungary

In June 2008, three months after *Access Information Program* filed their complaint in Bulgaria, the *Hungarian Civil Liberties Union* (HCLU or TASZ, *Társaság a Szabadságjogkért*) took similar action when it requested "the ex-post examination" by the Hungarian Constitutional Court of the amendment of Act C of 2003 on electronic communications, "for unconstitutionality and the annulment of the data retention provisions." According to the HCLU, Act C "already comprised numerous restrictive data retention provisions prior to the directive. The only changes brought in by the amendments were the retention of Internet communications data and the elimination of the lax – but at least pre-defined – legal purposes of the data processing". The HCLU argued that "the amendments completely disregarded the provisions of the directive [stating] that data should be 'available for the purpose of investigation, detection and prosecution of serious crimes'."[95] Despite being filed in 2008, the case is yet to be heard. According to Fanny Hidvégi of the Hungarian Civil Liberties Union, this is because as of 1 January 2012 the ability to request that the Constitutional Court initiative an investigation as to whether a law complies with the constitution has been "reduced dramatically". At the same time, "every pending case submitted by a person or institution which no longer has the right to do so were automatically terminated". The HCLU has begun a new and lengthy procedure that requires the exhaustion of all other remedies before the Constitutional Court can examine the Hungarian data retention measures.

---

[92] Ibid.
[93] Ibid.
[94] According to an article by the NGO that initiated the legal challenge: Access Information Program, 'The Bulgarian Supreme Administrative Court (SAC) repealed a provision of the Data Retention in the Internet Regulation', 11 December 2008, http://www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm
[95] 'Constitutional Complaint Filed by HCLU Against Hungarian Telecom Data Regulations', *Hungarian Civil Liberties Union*, 2 June 2008, http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention

## 5.4 Romania

In October 2009, the Romanian Constitutional Court found that the proposed national legislation implementing the EU Data Retention Directive violated articles of the Romanian constitution protecting freedom of movement; the right to intimate, private and family life; secrecy of correspondence; and freedom of expression.[96] Article 8 of the European Convention on Human Rights (right to respect for private and family life), Article 12 of the Universal Declaration of Human Rights, and Article 17 of the International Covenant on Civil and Political Rights (both of which forbid arbitrary interference with privacy, family, home, and correspondence) were all invoked by the court, which found that the government's attempt to justify the mandatory retention of telecommunications data by invoking undefined "threats to national security" was unlawful.[97] The Court also made reference to the European Court of Human Rights 1978 ruling in *Klass v Germany*,[98] which stated that "taking surveillance measures without adequate and sufficient safeguards can lead to 'destroying democracy on the ground of defending it'."[99]

In October 2011 the European Commission asked the Romanian government to bring forward new laws transposing the Directive into national law, issuing a "reasoned opinion" under Article 258 of the Lisbon Treaty which carries the threat of full infringement proceedings at the European Court of Justice if the request is not met. A new law was duly drafted but this was rejected by the Romanian Senate. The law had been heavily criticised in the media prior to the vote and the country's Data Protection Authority had refused to endorse it, claiming that articles relating to the security services were "still vague".[100] Civil society organisations also opposed it and even the government refused to sponsor it, leaving the Minister of Communications and Information Society to propose it in his role as MP rather than minister.[101] The Minister of European Affairs offered strong support for the law, fuelling criticism that it was motivated solely by the need to escape sanction by the European Court of Justice.

Ultimately the Senate vote was not decisive and the law continued its journey to the Chamber of Deputies, where at the end of May 2012 it was adopted with 197 votes for and 18 against, with many abstentions among the Chamber's 332 Deputies. There was no substantive discussion of fundamental rights issues in the Chamber of Deputies or the main two committees that debated the law[102] and critics have argued that the provisions on access to retained data are even more

[96] Constitutional Court of Romania, Decision no.1258, 9 October 2009, http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf
[97] Statewatch briefing, 'Mandatory data retention in the EU', March 2011, http://www.access-info.org/documents/chris-mandret-draft.pdf
[98] European Court of Human Rights, 'Klass and others v Germany', 6 September 1978, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510#{%22itemid%22:[%22001-57510%22]}
[99] 'Romanian Constitutional Court Decision Against Data Retention', *EDRi-gram*, 2 December 2009, http://www.edri.org/edrigram/number7.23/romania-decision-data-retention
[100] 'Romanian Senate Rejects The New Data Retention Law', *EDRi-gram*, 18 January 2012, http://www.edri.org/edrigram/number10.1/romanian-senate-rejects-data-retention
[101] Ibid.
[102] 'Romanian Parliament Adopts The Data Retention Law. Again', *EDRi-gram*, 23 May 2012, http://www.edri.org/edrigram/number10.10/romanian-parliament-adopts-data-retention-law-again

problematic than the original statute.[103] On 21 February 2013 the European Commission withdrew the infringement procedure that it had opened in 2011.[104]

## 5.5 Cyprus

In February 2011 the Supreme Court of Cyprus ruled that certain aspects of the legislation transposing the Data Retention Directive breached the Cypriot constitution and case law on surveillance. The case was brought by individuals whose telecommunications data had been disclosed to the police in accordance with District Court orders. The complainants argued that the laws on which the orders were based (Articles 4 and 5 of Law 183(I) 2007, that sought to harmonise Cypriot law with the Data Retention Directive), and therefore the District Court orders themselves, "were in breach of the Constitution as they violated their rights of privacy and family life (Art. 15.1) and of secrecy of communications (Art. 17.1)." The Supreme Court found that petitioners had indeed been subject to a violation of their rights and annulled provisions it said went beyond the requirements by the Data Retention Directive. The legality of the Directive itself was not called into question.[105]

[103] Ibid. While "the text of 2008 stated clearly that only a judge could allow the access to the data," the new law – which so far has remains unchallenged – merely contains "a reference to the Penal Procedure Code that, in fact, says nothing on the matter".

[104] 'EC drops case against Romania as data retention law passes', *telecompaper*, 22 February 2013, http://www.telecompaper.com/news/ec-drops-case-against-romania-as-data-retention-law-passes--926708

[105] Christophoros Christophorou, 'Provisions of the Law on Retention of Telecommunications Data Declared Unconstitutional', Council of Europe IRIS database, 2011, http://merlin.obs.coe.int/iris/2011/4/article14.en.html; see also the ruling (Greek only): Cyprus Supreme Court (Civil applications 65/2009, 78/2009, 82/2009 and 15/2010-22/2010), http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf

## 5.6 Germany

Legislation transposing the Data Retention Directive into the Telecommunication Act and Code of Criminal Procedure was passed by the Bundestag on 9 November 2007 and entered into force on 1 January 2008. The day before, 31 December 2007, 35,000 German citizens (represented by the NGO *AK Vorrat*) filed a complaint against the legislation at the Federal Constitutional Court.

On 2 March 2010 the Court ruled that the provisions of § 113a and § 113b Telecommunication Act and § 100g Code of Criminal Procedure were a disproportionate interference with Article 10 (privacy of correspondence, posts and telecommunications) of the Basic Law (*Grundgesetz*). However, the Court made no ruling on the actual Directive, stating that data retention is in principle proportionate to the aim of investigating serious crime and preventing imminent threats against life, body, freedom of persons, and the existence and security of the Federal Republic or one of its states. The Court found that the new domestic law failed to comply with legal standards on purpose limitation (restrictions on use of the retained data), data security, transparency and legal remedies.[106]

In January 2011 the Ministry of Justice (MoJ) presented a paper proposing an alternative to data retention in the form of a "quick freeze" system of limited data preservation for criminal investigations.[107] The police and/or public prosecutors would issue a "quick freeze" order seeking access to metadata already held by telecommunications providers, for example for billing purposes. To actually access the "frozen"' data would require the approval of a judge. In addition, the MoJ proposed an obligation for ISPs to store internet traffic data for seven days, allowing criminal investigators to identify persons behind (already known) IP addresses in particular in cases of child pornography. Criminal investigators would request the traffic and communications data via service providers without having direct access to these traffic data.[108] This paper reflected proposals made in June 2010 by the Federal Commissioner for Data Protection, as well as the suggestions of more pragmatic privacy advocates. More radical activists claim that any mandatory storage of communications data should be prohibited.[109]

The Interior Ministry rejected the MoJ's proposals and insisted on full implementation of the Data Retention Directive instead, including the minimum storage retention period of six months, arguing that the Constitutional Court has already shown that it is possible to implement the Directive and ensure individual privacy through high data security standards, including encryption and the "four eyes principle" (approval by at least two people) as prerequisite for accessing data and log files;

[106] 'Leitsätze zum Urteil des Ersten Seants vom 2. März 2010 – 1 BvR 256/08 – 1 BvR 263/08 – 1 BvR 586/08', *Bundesverfassungsgericht*, 2 March 2010, https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html; see also 'German Federal Constitutional Court Rejects Data Retention Law', *EDRi-gram*, 10 March 2010, http://www.edri.org/edrigram/number8.5/german-decision-data-retention-unconstitutional

[107] See section 5 for more information on the differences between 'quick freeze' data preservation and data retention.

[108] 'Eckpunktepapier zur Sicherung vorhandener Berkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet', *Bundesministerium der Justiz*, January 2011, http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/eckpunktepapr_zur_sicherung_vorhandener_verkehrsdaten.pdf;jsessionid=2E7C449846360716899A599AF0A357FC.1_cid324?__blob=publicationFile

[109] 'Bundesdatenschützer plädiert für "Quick Freeze" statt Vorratsdatenspeicherung', *Heise Online*, 15 June 2010, http://www.heise.de/newsticker/meldung/Bundesdatenschuetzer-plaediert-fuer-Quick-Freeze-statt-Vorratsdatenspeicherung-1021967.html

strict purpose limitation; and the protection of professions whose confidentiality must be ensured.[110]

The MoJ produced a "quick freeze" bill in April 2012 but continued opposition from the Interior Ministry meant that it was never tabled in Parliament. The Interior Ministry was unhappy with the length of the proposed freezing periods, demanding three months instead of the one month suggested by the Ministry of Justice. Moreover, where the MoJ wanted to restrict the authorisation for freezing orders to the investigation of serious crimes, the Interior Ministry wanted broader powers to include crimes such as fraud and hacking.[111] The proposed bill also aimed to amend the Telecommunications Act in order to make the storage of identities behind assigned IP addresses mandatory for seven days, with an exemption for internet service providers (ISPs) providing services to less than 100,000 people on cost grounds.[112] The controversy continues and no new legislation has yet been introduced: the Interior Ministry wants the law to cover all ISPs and reiterated its demand for a six month retention period in line with the provisions of the Data Retention Directive.[113]

By this time the European Commission had initiated infringement proceedings and took its case to the European Court of Justice in July 2012 in a case that has yet to be decided.[114] The Commission is seeking to impose a daily fine of €315,000 for failure to implement transposing legislation. The Commission noted that following the Constitutional Court's ruling in March 2010 the German government had promised a replacement law to transpose the provisions of the Directive but:

> "Since the draft has not, as yet, been adopted, it is, according to the Commission, not open to dispute that the Federal Republic of Germany has failed to meet its obligation to transpose the directive in full. The abovementioned partial transposition is, in the Commission's view, insufficient to attain the objectives of the directive under Article 1. Finally, the Commission points out that, in its opinion, the draft Law notified to it by Germany is insufficient for purposes of full implementation of the directive."[115]

## 5.7 Czech Republic

On 13 March 2011 the Constitutional Court of the Czech Republic also declared national legislation implementing the Data retention Directive unconstitutional. The Court found that the retention

[110] Interestingly Clerics were mentioned but not journalists or lawyers. See Häufig gestellte Fragen zur Mindestspeicherfrist', *Bundesministerium des Innern*, undated, http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/Sicherheit/SicherheitAllgemein/8.html

[111] Kai Bierman, 'Wie umfangreich wird die Vorratsdatenspeicherung?', *Zeit Online*, 19 April 2012, http://www.zeit.de/digital/datenschutz/2012-04/vorratsdaten-gesetzentwurf/komplettansicht

[112] The exclusion of smaller service providers was identified by the European Commission as one reason for the uneven implementation of the Directive across the EU – see section 5.

[113] Kai Biermann, 'Wie umfangreich wird die Vorratsdatenspeicherung?', *Zeit Online*, 19 April 2012, http://www.zeit.de/digital/datenschutz/2012-04/vorratsdaten-gesetzentwurf/komplettansicht

[114] Action brought on 11 July 2012 – European Commission v Federal Republic of Germany(Case C-329/12), InfoCuria, http://curia.europa.eu/juris/document/document.jsf?text=&docid=126495&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1218677

[115] Ibid.

period required by the national legislation exceeded the requirements of the Directive, and that use of the data was not restricted to cases of serious crime and terrorism.[116] "The national legislation lacked, according to the constitutional court, clear and detailed rules for the protection of personal data as well as the obligation to inform the person whose data has been requested."[117]

As in Germany, the Court stated that it could not review the Directive itself, while noting that there was nothing in principle preventing implementation in conformity with constitutional law. A second Constitutional Court decision in December 2011[118] examined the procedures put in place for obtaining access to retained data and found the "procedure in question to be too vague, in breach of [the] proportionality rule (its second step) and thus unconstitutional due to interference with right to privacy and informational self-determination."[119]

In the meantime the Czech government revised the implementing legislation with modifications that took effect on 1 October 2012.[120] These included "[T]he introduction of the obligation to inform people whose data have been requested under the Criminal Code and to obtain court permission when such data is requested by intelligence service or the Czech National Bank."[121] The NGO *Iuridicum Remedium* has lodged fresh proceedings against the revised legislation on the grounds that regulation remains inadequate and that the new decree could provide for the "monitoring of contents of Internet communications".[122]

## 5.8 Slovakia

In August 2012 a group of Slovakian MPs, supported by the *European Information Society Institute*, lodged a legal complaint against the legislation implementing the Data Directive. The complaint asks the Slovak Constitutional Court to examine whether the laws implementing the Directive in Slovakia and dealing with access by the authorities to retained data are compatible with constitutional provisions on proportionality, the rights to privacy and protection against unlawful data collection, the right to private correspondence, and the provision granting freedom of speech.[123] It also argues that the measures infringe provisions guaranteeing privacy, data protection and freedom of expression in Slovakian human rights law, the European Convention on Human Rights and the

[116] 'The English translation of the Czech Constitutional Court decision on Data Retention', 22 March 2011, http://www.slidilove.cz/sites/default/files/dataretention_judgment_constitutionalcourt_czechrepublic.pdf
[117] 'Czech Constitutional Court Rejects Data Retention Legislation', *EDRi-gram*, April 2011, http://www.edri.org/edrigram/number9.7/czech-data-retention-decision
[118] The link provided to the judgment by Martin Husovec (see footnote 117) no longer works (http://www.concourt.cz/soubor/6113) and the current English website of the Czech Constitutional Court (http://www.usoud.cz/en/) does not contain the text of the December 2011 ruling.
[119] Martin Husovec, 'Czech Constitutional Court Gives Another Decision on Data Retention, *Hut'ko's Technology Law Blog*, 5 January 2012, http://www.husovec.eu/2012/01/czech-constitutional-court-gives.html
[120] Czech Telecommunication Office, 'The Annual Report of the Czech Telecommunication Office for 2012', p.12, http://www.ctu.eu/164/download/Annual_Reports/annual_report-2012.pdf
[121] Ibid. at 17
[122] 'Czech Republic: Data Retention – Almost Back In Business', *EDRi-gram*, 1 August 2012, http://www.edri.org/edrigram/number10.15/czech-republic-new-data-retention-law
[123] The provisions covered by the challenge are § 58(5), (6), (7)(a), § 63(6) Act No. 351/2011 Coll. on Electronic Communications - data retention; § 116 Penal Procedure Act (Act No. 301/2005 Coll.) - access to retention data; and § 76(a)(3) Police Corps Act (Act No. 171/1993 Coll.) - access to retention data.

Charter of Fundamental Rights of the European Union.[124] The complaint has not yet been resolved.

[124] The European Information Society Institute twice previously attempted to file their own complaints about the country's data retention measures before the Constitutional Court, but both cases were rejected. Martin Husovec from the Institute told Statewatch in October 2012 that this left the organisation with "no other option than to prepare the template submission before the Constitutional Court ourselves and address the MPs." He noted that "data retention is an unfortunate experiment with the privacy of European citizens." There is no defined time limit in which the Constitutional Court is required to rule on the complaint, but given that no procedural issues have been raised with the application it is expected that a judgment will be delivered by the end of 2014 at the latest. See 'Slovakian data retention law faces challenge before Constitutional Court', *Statewatch News Online*, October 2012, http://database.statewatch.org/article.asp?aid=31892

## 5.9 Sweden

In Sweden, the European Commission has engaged in a lengthy battle to try to bring Sweden's domestic legislation into line with the Data Retention Directive. After the country missed the initial September 2007 deadline, the Commission brought infringement proceedings, with the European Court of Justice finding Sweden guilty of failing to fulfil its obligations to the EC in February 2010.[125]

A proposal for transposing legislation was put forward in December 2010[126] and finally adopted in In March 2012.[127] Johan Linander, an MP for the Centre Party, told *EU Business* that "the need for, and the benefits of, the directive do not compensate for the invasion of privacy." The police were not happy either, although for rather different reasons: the law made it more difficult for them to access historical traffic data. Chief of police Klas Freiberg was quoted as saying that the six month retention period would make police work more difficult: "The time period is too short. Today we're able to access information that is older than six months."[128]

The new law should have taken effect in May 2012 but despite an overwhelming vote in favour of the new measures in the Swedish parliament (233 MPs voted in favour with 41 against and 19 abstaining), the Left Party and the Greens invoked a constitutional provision allowing the entry into force of new measures to be delayed by a motion of one sixth of its members.[129] In May 2013, the European Court of Justice ordered Sweden to pay a €3 million fine for its delay in implementing the legislation in accordance with its earlier ruling. The Commission rejected Swedish pleas regarding the domestic controversy over the implementation of the law:

> "Regarding the Kingdom of Sweden's conduct in respect of its obligations under Directive 2006/24, the justifications put forward by that Member State pursuant to which the delay in complying with that judgment was attributable to extraordinary internal difficulties connected with specific aspects of the legislative procedure, to the extensive political debate on the transposition of Directive 2006/24, and to the issues raised in terms of difficult choices involving weighing the protection of privacy against the need to combat crime effectively cannot be upheld. As the Court has repeatedly emphasised, a Member State cannot plead provisions, practices or situations prevailing in its domestic legal order to justify failure to observe obligations arising under European Union law (see, inter alia, Case C-407/09 *Commission* v *Greece* [2011] ECR I-2467, paragraph 36). The same is true of a decision, such as the one made by the Swedish Parliament, to which paragraph 8 of this judgment makes reference, to postpone for a year the adoption of the draft bill intended to transpose that directive."[130]

---

[125] Judgment of the Court (Sixth Chamber) of 4 February 2010 – European Commission v Kingdom of Sweden (Case C-185/09), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:080:0006:0006:EN:PDF

[126] 'Regeringens proposition 2010/11:46, Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG', 3 December 2010, http://www.regeringen.se/content/1/c6/15/74/33/3dc07bbd.pdf

[127] 'Swedish parliament passes controversial data storage bill', *EU Business*, 21 March 2012, http://www.eubusiness.com/news-eu/sweden-telecom.frt

[128] Ibid.

[129] Jan Libbenga, 'Sweden postpones EU data retention directive, faces court, fines', *The Register*, 18 March 2011, http://www.theregister.co.uk/2011/03/18/sweden_postpones_eu_data_retention_directive/

[130] Paragraph 54, Judgment of the Court (Fourth Chamber) of 30 May 2013 – European Commission v Kingdom of Sweden (Case C-270/11),

## 5.10 The Court of Justice (EU)

The most serious challenge to the implementation of the Data Retention Directive has come from a challenge made initially by the NGO *Digital Rights Ireland*, whose complaint to the ECJ has now been joined by the plaintiffs in a case referred from the Austrian Constitutional Court. The joined cases[131] were heard by the Grand Chamber of the ECJ on 9 July 2013 and "adamantly asked for proof of the necessity and efficiency of the EU Data Retention Directive".[132] The Advocate General is scheduled to produce their opinion on the case on 7 November 2013.

The case focuses on the compatibility of the Directive with Articles 7 (respect for private and family life) and 8 (protection of personal data) of the European Charter of Fundamental Rights. Prior to the oral hearing the Court sent out a series of questions to the parties involved. These asked:

- Whether the measures contained within the Directive "can serve the purpose of detection and prosecution of serious crime", in particular in the light of the possibilities for communicating anonymously through electronic means;
- To what extent profiling of individuals is possible based on the data retained under the Directive;
- How the interference with the rights guaranteed by Articles 7 and 8 should be characterised;
- The objective criteria and data that served as the basis for the adoption of the Directive and certain of its provisions, i.e. a minimum retention period of six months;
- Whether the legislature achieved "a proper balance of the requirements bound up with the protection of fundamental rights and the public interest objective at issue in these cases";
- Whether the Directive contains sufficient provisions on "the security of retained data as are necessary and sufficiently precise in order to avoid the possibility of abuse" and whether the interference with fundamental rights was restricted "strictly to what was necessary".[133]

At the hearing the representatives of those who initiated the cases domestically in Ireland and Austria argued that the Data Retention Directive is fundamentally incompatible with the Charter and that there is still no evidence to demonstrate that "the excessive collection of communication data is a necessary and proportionate measure for combating organised crime and terrorism in the EU."[134] On behalf of Austrian privacy group *AK Vorrat*, Edward Scheucher argued that:

---

http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=137828&occ=first&dir=&cid=1133353

[131] Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012 — Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General (Case C-293/12), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62012CN0293:EN:NOT and Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 — Kärntner Landesregierung and Others (Case C-594/12), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62012CN0594:EN:NOT

[132] Monika Emert, 'Data retention might not be proportional to risks', *Policy Review*, 9 July 2013, http://policyreview.info/articles/news/data-retention-might-not-be-proportional-risks/170

[133] '"As large a charter as the wind? ECJ to hold hearing in data retention cases, focusing on Charter of Fundamental Rights', *Content and Carrier*, 15 June 2013, http://www.contentandcarrier.eu/?p=435

[134] 'Data Retention: "We Ask The Court To Rule In Favour Of Freedom"', *EDRi-gram*, 17 July 2013, http://www.edri.org/edrigram/number11.14/data-retention-hearing-ecj-2013

> "[T]he cumulative effect of fundamental rights restrictions need to be taken into consideration when judging the legitimacy of a single measure. Given the revelations regarding PRISM, this cumulative effect now clearly provides a different result [than] at the time when the German [Constitutional] Court took its decision [to annul certain provisions of German transposing legislation]. Furthermore, he stated that the Austrian implementation of the directive clearly showed that a Charter-compatible national implementation of the Data Retention Directive is not possible. This argument is bolstered by the fact that the main author of the Austrian implementation is among the 11,139 Austrian plaintiffs who challenged data retention before the Austrian Constitutional Court."[135]

In response to requests for evidence demonstrating the necessity of the Directive, the Austrian and Irish governments presented new statistics on the use of retained data at the hearing. They were joined in arguments in favour of the Directive by representatives of Italy, Spain and the UK, as well as the Commission, the Council and the Parliament. Despite the new information from Austria[136] and Ireland,[137] the Directive's advocates still "had to acknowledge a lack of statistical evidence", with the UK admitting that "there was no 'scientific data' to underpin the need" for data retention.[138] Judge Thomas von Danwitz, the Court's main rapporteur for the hearing, was moved to ask what information had led to the adoption of the Directive in 2006, given that "the Commission in 2008 claimed not to have enough information for a sound review".[139] The Council's lawyers "implored the Court not to take away instruments from law enforcement".[140]

Von Danwitz also questioned the legitimacy of excluding detailed fundamental rights protections from the legislation after European Data Protection Supervisor's office argued that the Directive "did not provide enough protection for privacy. It just passed the blindspot onto Member States".[141] The storage by telecoms providers of retained data in third countries was also raised in the context of the revelations about mass internet surveillance by the USA's National Security Agency and the UK's Government Communications Headquarters (GCHQ). Thirty-six per cent of retained traffic data is apparently stored in third countries or by service providers based in third countries, but "it had become clear that this data in fact was not stored according to the legal obligation, calling into question the legality of the storage obligation in general, von Danwitz warned."[142]

---

[135] Ibid.

[136] Austrian law enforcement authorities requested 326 sets of data between 1 April 2012 and 31 March 2013, and of the 139 procedures that have been closed, retained data "helped to solve" 56 of the cases – 16 thefts, 12 drugs cases, 12 cases of stalking, 7 frauds and 9 others. Judge Thomas von Danwitz subsequently asked: "Was there a terrorist case"? See: Monika Emert, 'Data retention might not be proportional to risks' *Internet Policy Review*, 9 July 2013, http://policyreview.info/articles/news/data-retention-might-not-be-proportional-risks/170

[137] The Irish authorities apparently make "6,000 to 10,000" requests every year according to the government's lawyer in the ECJ case, although statistics from 2010 show 14,928 requests, and from 2011 12,675 requests. See: Karlin Lillington, 'State agencies target Irish phone and Internet records', *The Irish Times*, 25 July 2013, http://www.irishtimes.com/business/sectors/technology/state-agencies-target-irish-phone-and-internet-records-1.1473739

[138] Monika Emert, 'Data retention might not be proportional to risks' *Internet Policy Review*, 9 July 2013, http://policyreview.info/articles/news/data-retention-might-not-be-proportional-risks/170

[139] Ibid.

[140] Ibid.

[141] Ibid.

[142] Ibid.

# 6 Conclusion

The legitimacy of the EU's Data Retention Directive has been a matter if dispute since legislation was first proposed in 2002. Adopted soon after the terrorist attacks in Madrid and London, some member states appear to have extended the scope of its application beyond even the "serious crimes" mandated by the Directive. In principle and in practice the implementation of the Directive has had a tremendous impact on fundamental rights and other constitutional protections. By establishing the principle that data must be retained for long periods in case police and security agencies need to access it later, the EU has crossed the Rubicon into mass surveillance.

The Directive has failed to harmonise data retention regimes for law enforcement purposes because of the wide margin of discretion given to member states when transposing its provisions. By giving Member States the scope to choose their own retention periods and to decide which authorities should have access under what type of authorisation, and by failing to include a list of crimes for which retained data can be retrieved or specific data protection provisions, the legislative situation is arguably now only slightly less uneven than before the Directive was adopted. But given the law was primarily a response to demands for mandatory data retention across the EU from law enforcement and security agencies, "harmonisation" does not appear to have been the primary purpose of a measure that does little more than provide a generous EU legal basis for communications surveillance.

It appears that states are not prepared to concede to the suggestion that a mandatory data retention system per se may simply not be appropriate. Thus, debates about its legitimacy have come to rest on whether the practical experience of using it justifies keeping it. In respect to the "evidence" presented to justify the Directive, it is sufficient to note that the plural of anecdotes is not "data". And even to the extent that case studies can be seen to objectively demonstrate the Directive's effectiveness, it does not necessarily follow that they justify the Directive's scope, application, or absence of protection for due process and fundamental rights.

# Appendix

The tables below contain a variety of information on the provisions and procedures governing access to telecommunications data retained under national laws implementing the EU Data Retention Directive. Due to the amount of information contained in the tables it has only been possible to include three member states per page; they are listed in the traditional order provided for in EU publications[143] and not for any particular comparative purpose. The tables have been compiled from a number of different sources of data:

- EUR-Lex database:[144] links to national implementing measures;
- European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, 18 April 2011:[145] retention periods, purpose limitation, authorities with access, procedures for access, statistics on requests for access to retained data for 2008 and 2009, data protection safeguards, data protection authority, relevant law, reimbursement of costs (operational), reimbursement of costs (capital);
- Céline Cocq and Francesca Galli, 'Comparitive law paper on data retention regulation in a sample of EU Member States', SURVEILLE project, 30 April 2013: further information on authorities with access and procedures for access
- European Commission, 'Data Retention Statistics 2010':[146] statistics on requests for access to retained data for 2010

Some other sources used for information on statistics for access to retained data for 2011 (Poland) and 2012 (Ireland) are noted in the text.

[143] This is determined by the alphabetical order of the native names of each member state transliterated into English.
[144] http://eur-lex.europa.eu/RECH_legislation.do
[145] http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf
[146] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/publication_data_retention_statistics_20120228_without_es_en.pdf

| | Belgium | Bulgaria | Czech Republic |
|---|---|---|---|
| National law | Three acts: EUR-Lex entry | Four acts: EUR-Lex entry | Fourteen acts: EUR-Lex entry |
| Retention period | Between 1 year and 36 months for 'publically available' telephone services. No provision for internet-related data. | 1 year. Data which has been accessed may be retained for a further 6 months on request. | Information unavailable |
| Purpose limitation | For the investigation and prosecution of criminal offences, the prosecution of abuse of emergency services telephone number, investigation into malicious abuse of electronic communications network or service, for the purposes of Intelligence-gathering missions undertaken by the intelligence and security services. | For 'discovering and investigating severe crimes and crimes under Article 319a-319f of the Penal Code as well as for searching persons'. | Information unavailable |
| Authorities with access | Judicial coordination unit, examining magistrates, public prosecutor, criminal police. | Certain departments of the State Agency for National Security, the Ministry of the Interior, Military Information Service, Military Police Service, Minister of Defence, National Investigation Agency; the court and pre-trial authorities under the conditions. | Information unavailable |
| Procedures for access | Magistrate or prosecutor authorisation. Upon request, operators must provide in 'real time' subscriber, traffic and location data for calls made within the last month. Data for older calls must be provided as soon as possible. | Access only possible on the order of the Chairperson of a Regional Court. | Information unavailable |
| **Total number of requests made for telephony and internet data, successful (unsuccessful)** | | | |
| 2008 | - | - | 131,560 (2,490) |
| 2009 | - | - | 280,271 (10,446) |
| 2010 | - | 38,861 (920) | 289,169 (10,194) |
| Data protection safeguards | Operators must ensure transmission of data cannot be intercepted by third parties and complies with ETSI standards. Principle of obligatory destruction of data at the end of retention period does not seem to be addressed. | Transposing law includes requirement to implement the four principles. | Information unavailable |
| Data protection authority | Institute for Postal Services and Telecommunications | Commission for Personal Data Protection (processing and storing of data obligations); Parliamentary Commission in the National Assembly (procedures for authorisation | Information unavailable |

| | | | |
|---|---|---|---|
| | | and access to the data) | |
| Relevant law | Article. 6, Royal Decree of 9 January 2003 | Article 4 (1), Law on Electronic Communications 2010 | Information unavailable |
| Reimbursement of costs (operational) | Yes | No | Information unavailable |
| Reimbursement of costs (capital) | No | No | Information unavailable |
| | **Denmark** | **Germany** | **Estonia** |
| National law | Three acts: EUR-Lex entry | One act (suspended): EUR-Lex entry | Two acts: EUR-Lex entry |
| Retention period | 1 year. | - | 1 year. |
| Purpose limitation | For investigation and prosecution of criminal acts. | - | May be used if collection of the evidence by other procedural acts is precluded or especially complicated and the object of a criminal proceeding is a criminal offence [in the first degree or an intentionally committed criminal offence in second degree with a penalty of imprisonment of at least three years]. |
| Authorities with access | Police. | Prior to suspension of law: Police and Border Guard Board, Security Police Board and, for objects and electronic communication, the Tax and Customs Board. | |
| Procedures for access | Access requires judicial authorisation; court orders are granted if application meets strict criteria on suspicion, necessity and proportionality. | | Access requires permission of a preliminary investigation judge Operators must 'provide [retained data] in urgent cases not later than 10 hours and in other cases within 10 working days [of receiving a request].' |
| **Total number of requests made for telephony and internet data, successful (unsuccessful)** | | | |
| 2008 | 3,599 (5) | 12,684 (931) | 4,490 (1,526) |
| 2009 | 4,066 (11) | - | 8,410 (2,768) |
| 2010 | 4,235 | - | 4,173 (98,408) |
| Data protection safeguards | Four principles are provided for. | | |
| Data protection authority | National IT and Telecom Agency monitors the obligation for providers of electronic communications networks and services to ensure that technical equipment and systems allow police access to information about telecommunications traffic. | Information unavailable | Transposing law provides for three of the four principles. No explicit provision for the fourth principle though any persons whose privacy has been infringed by surveillance-related activities may request the destruction of data, subject to a court judgement. |
| Relevant law | Act on Processing Personal Data; Executive Order No.714 of 26 June 2008 on Provision of | Information unavailable | Technical Surveillance Authority is the responsible authority. |

| | | | |
|---|---|---|---|
| | Electronic Communications Networks and Services | | |
| Reimbursement of costs (operational) | Yes | Information unavailable | Yes |
| Reimbursement of costs (expenditure) | No | Information unavailable | No |

| | Ireland | Greece | Spain |
|---|---|---|---|
| National law | Three acts: EUR-Lex entry | One act: EUR-Lex entry | One act: EUR-Lex entry |
| Retention period | 2 years for fixed telephony and mobile telephony data, 1 year for internet access, internet email and internet telephony data. | 1 year. | 1 year. |
| Purpose limitation | For prevention of serious offences [i.e. offences punishable by imprisonment for a term of 5 years or more, or an offence in schedule to the transposing law], safeguarding of the security of the state, the saving of human life. | For the purpose of detecting particularly serious crimes. | For the detection, investigation and prosecution of the serious crimes considered in the Criminal Code or in the special criminal laws. |
| Authorities with access | Members of Garda Síochána (police) at Chief Superintendent rank or higher; Officers of Permanent Defence Force at colonel rank or higher; Officers of Revenue Commissioners at principal officer or higher. | Judicial, military or police public authority. | Police forces responsible for detection, investigation and prosecution of the serious crimes, National Intelligence Centre and Customs Agency. |
| Procedures for access | Requesting to be in writing. | Access requires judicial decision declaring that investigation by other means is impossible or extremely difficult. | Access to these data by the competent national authorities requires prior judicial authorisation. |
| **Total number of requests made for telephony and internet data, successful (unsuccessful, if provided)** | | | |
| 2008 | 14,095 (97) | 584 | 53,578 (0) |
| 2009 | 11,283 (92) | - | 70,090 (0) |
| 2010 | 14,928 | - | - |
| 2012 | Approx. 9,000[147] | - | - |
| Data protection safeguards | Transposing law includes requirement to implement the four principles. | Transposing law includes requirement to implement the four principles, with further requirement for operators to appoint a data security manager to prepare and apply a plan for ensuring compliance. | Data security provisions cover three of the four principles (quality and security of retained data, access by authorised persons and protection against unauthorised processing). |
| Data protection authority | Designated judge has power to investigate and report on whether competent national authorities comply with provisions of transposing law. | Personal Data Protection Authority and Privacy of Communications Authority | Data Protection Agency is the responsible authority. |
| Relevant law | Sections 4, 11 and 12, Communications (Retention of Data) Bill 2009 | Article 6 of Law 3917/2011 | Article 8, Law 25/2007; Article 38(3) General Telecommunications Law; Art 22 and 23 Organic Law 15/1999 on personal data protection |

[147] A spokesperson for the Irish Department of Justice told *The Irish Times* that "The communications data retention statistics for Ireland for 2012 are in the order of 9,000 requests." Source: Karlin Lillington, 'State agencies target Irish phone and internet records', *The Irish Times*, 25 July 2013**,** http://www.irishtimes.com/business/sectors/technology/state-agencies-target-irish-phone-and-internet-records-1.1473739

| | | | |
|---|---|---|---|
| Reimbursement of costs (operational) | No | No | No |
| Reimbursement of costs (expenditure) | No | No | No |

| | **France** | **Italy** | **Cyprus** |
|---|---|---|---|
| National law | Two acts: EUR-Lex entry | One act: EUR-Lex entry | One act: EUR-Lex entry |
| Retention period | 1 year. | 2 years for fixed telephony and mobile telephony data, 1 year for internet access, internet email and internet telephony data. | 6 months. |
| Purpose limitation | For the detection, investigation, and prosecution of criminal offences, and for the sole purpose of providing judicial authorities with information needed, and for the prevention of acts of terrorism and protecting intellectual property. | For detecting and suppressing criminal offences. | For investigation of a serious criminal offence. |
| Authorities with access | Public prosecutor, police officers authorised by a judge, Minister of the Interior, and gendarmes. | Public prosecutor; police; defence counsel for either the defendant or the person under investigation, intelligence services. | The courts, public prosecutor, police |
| Procedures for access | Police must provide justification for each request for access to retained data and must seek authorisation from 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. | Access requires 'reasoned order' issued by the public prosecutor. | Access must be approved by a prosecutor if he considers it may provide evidence of committing a serious crime. A judge may issue such an order if there is a reasonable suspicion of a serious criminal offence and if the data are likely to be associated with it. |
| **Total number of requests made for telephony and internet data, successful (unsuccessful)** | | | |
| 2008 | 503,437 | - | 34 (5) |
| 2009 | 514,813 | - | 40 (3) |
| 2010 | - | - | 79 (8) |
| Data protection safeguards | Transposing law includes requirement to implement the four principles. | No explicit provisions on security of retained data, although there is a general requirement for destruction or anonymisation of traffic data and consensual processing of location data. | Transposing law provides for each of the four principles. |
| Data protection authority | National Commission for Information Technology and | Data protection authority monitors operators' | Commissioner for Personal Data Protection monitors |

| | | | |
|---|---|---|---|
| | Freedom supervises compliance with obligations | compliance with the Directive. | application of transposing law. |
| Relevant law | Article D.98-5, CPCE; Article L-34-1(V), CPCE; Article 34, Act n° 78-17; Article 34-1, CPCE; Article 11, Law no.78-17 of 6 January 1978 | Article 123, 126, Data Protection Code | Articles 14 and 15, Law 183(I)/2007 |
| Reimbursement of costs (operational) | Yes | - | No |
| Reimbursement of costs (expenditure) | No | - | No |

| | Latvia | Lithuania | Luxembourg |
|---|---|---|---|
| National law | Six acts: EUR-Lex entry | Six acts: EUR-Lex entry | Five acts: EUR-Lex entry |
| Retention period | 18 months. | 6 months. | 6 months. |
| Purpose limitation | To protect state and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings. | For the investigation, detection and prosecution of serious and very serious crimes, as defined by the Lithuanian Criminal Code. | For the detection, investigation, and prosecution of criminal offences carrying a criminal sentence of a maximum one year or more. |
| Authorities with access | Authorised officers in pre-trial investigation institutions; persons performing investigative work; authorised officers in state security institutions; the Office of the Public Prosecutor; the courts. | Pre-trial investigation bodies, the prosecutor, the court (judges) and intelligence officers. | Judicial authorities (investigating magistrates, prosecutor), authorities responsible for safeguarding state security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences. |
| Procedures for access | Authorised officers, public prosecutor's office and courts are required to assess 'adequacy and relevance' of request, to record the request and ensure protection of data obtained. Authorised bodies may sign agreement with an operator e.g. for encryption of data provided. | Authorised public authorities must request retained data in writing. For access for pre-trial investigations a judicial warrant is necessary. | Access requires judicial authorisation. |
| **Total number of requests made for telephony and internet data, successful (unsuccessful)** | | | |
| 2008 | 16,892 (696) | 85,315 (5,729) | - |
| 2009 | 26,096 (560) | 72,473 (6,580) | - |
| 2010 | 34,467 (560) | 105,118 (31,140) | - |
| Data protection safeguards | Transposing law provides for two of the principles: confidentiality of and authorised access to retained data, and destruction of data at the end of the period of retention | Transposing law provides for the four principles. | Transposing law provides for the four principles. |
| Data protection authority | The State Data Inspectorate supervises the protection of personal data in the electronic communications sector, but not access and processing of retained data. | State Data Protection Inspectorate supervises the implementation of the transposing law, and is responsible for providing the European Commission with statistics. | Data protection authority |
| Relevant law | Article 4(4) and Article 71(6-8), Electronic Communications Law | Articles. 12(5), 66(8) and (9) Electronic Communications Law as amended on 14 November 2009 | Article 1 (5), Law of 24 July 2010 |
| Reimbursement of costs (operational) | No | Yes, if requested and justified. | No |
| Reimbursement of costs | No | No | No |

| | | | |
|---|---|---|---|
| (expenditure) | | | |

| | Hungary | Malta | Netherlands |
|---|---|---|---|
| National law | 24 acts: EUR-Lex entry | Two acts: EUR-Lex entry | Three acts: EUR-Lex entry |
| Retention period | 6 months for unsuccessful calls and 1 year for all other data. | 1 year for fixed, mobile and internet telephony data, 6 months for internet access and internet email data. | 1 year. |
| Purpose limitation | To enable investigating bodies, the public prosecutor, the courts and national security agencies to perform their duties, and to enable police and the National Tax and Customs Office to investigate intentional crimes carrying a prison term of two or more years. | For investigation, detection or prosecution of serious crime. | For investigation and prosecution of serious offences for which custody may be imposed. |
| Authorities with access | Police, National Tax and Customs Office, national security services, public prosecutor, courts. | Malta Police Force; Security Service | Investigating police officer, prosecutor. |
| Procedures for access | Police and the National Tax and Customs Office require prosecutor's authorisation. Prosecutor and national security agencies may access such data without a court order. | Requests must be in writing. | Access must be by order of a prosecutor or an investigating judge. |
| **Total number of requests made for telephony and internet data, successful (unsuccessful)** | | | |
| 2008 | - | 869 (133) | 85,000 |
| 2009 | - | 4,023 (902) | - |
| 2010 | 130,000 | - | - |
| Data protection safeguards | Transposing law provides for the four principles. | Transposing law provides for the four principles. | Transposing law provides for the four principles. |
| Data protection authority | Parliamentary Commissioner for Data Protection and Freedom of Information | Data Protection Commissioner | Radio Communications Agency supervises obligations of internet access and telecom providers; data protection authority supervises general processing of personal data; a protocol details their cooperation between the two authorities. |
| Relevant law | Article 157 of Act C/2003, as amended by the Act CLXXIV/2007; Article 2 of Decree 226/2003; and Act LXIII/1992 on Data Protection. | Article 24, 25 Legal Note 198/2008; Article 40(b) Data Protection Act (Cap.440). | Article 13(5), Telecommunications Act; the long title of the cooperation protocol is *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht* |

| | | | |
|---|---|---|---|
| | | | *telecommunicatiegegevens* |
| Reimbursement of costs (operational) | No | No | Yes |
| Reimbursement of costs (expenditure) | No | No | No |

| | Austria | Poland | Portugal |
|---|---|---|---|
| National law | Two acts (currently suspended): EUR-Lex entry | Six acts: EUR-Lex entry | One act: EUR-Lex entry |
| Retention period | Information unavailable | 2 years. | 1 year. |
| Purpose limitation | Information unavailable | For prevention or detection of crimes, for prevention and detection of fiscal offences, for use by prosecutors and courts if relevant to the court proceedings pending, for the purpose of the Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, Military Counter-intelligence Services and Military Intelligence Services to perform their tasks. | For the investigation, detection and prosecution of serious crime. |
| Authorities with access | Information unavailable | Police, border guards, tax inspectors, Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, military counter-intelligence services, military intelligence services, the courts and the public prosecutor. | Criminal Police, National Republican Guard, Public Security Office, Military Criminal Police, Immigration and Borders Service, Maritime Police |
| Procedures for access | | Requests must be in writing and in case of police, border guards, tax inspectors, authorised by the senior official in the organisation. | Transmission of data requires judicial authorisation on grounds that access is crucial to uncover the truth or that evidence would be, in any other manner, impossible or very difficult to obtain. The judicial authorisation is subject to necessity and proportional requirements. |
| **Total number of requests made for telephony and internet data, successful (unsuccessful)** | | | |
| 2008 | 3,093 | - | - |
| 2009 | - | 1,048,318 | - |
| 2010 | - | - | 23 (3) |
| 2011 | - | 1,856,888[148] | - |
| Data protection safeguards | Information unavailable | Transposing law provides for the four principles. | Transposing law provides for the four principles. |
| Data protection authority | Information unavailable | Data protection authority. | Portuguese Data Protection Authority. |
| Relevant law | Information unavailable | Article 7(1), (5) and 11, Law 32/2008; Articles 53 and 54, Personal Data Protection Act. | Article 7(1), (5) and 11, Law 32/2008; Articles 53 and 54, Personal Data Protection Act. |
| Reimbursement | Information unavailable | No | No |

[148] 'How many times did the state authorities reach out for our private telecommunications data in 2011? We publish the latest research', Panoptykon Foundation, 3 April 2012, http://panoptykon.org/wiadomosc/how-many-times-did-state-authorities-reach-out-our-private-telecommunications-data-2011-we

| | | | |
|---|---|---|---|
| of costs (operational) | | | |
| Reimbursement of costs (expenditure) | Information unavailable | No | No |

| | Romania | Slovenia | Slovakia |
|---|---|---|---|
| National law | Two acts: EUR-Lex entry | Five acts: EUR-Lex entry | 13 acts: EUR-Lex entry |
| Retention period | Information unavailable (6 months under annulled law). | 14 months for telephony data and 8 months for internet related data. | 1 year for fixed telephony and mobile telephony data, 6 months for internet access, internet email and internet telephony data. |
| Purpose limitation | Information unavailable | For ensuring national security, constitutional regulation and the security, political and economic interests of the state … and for the purpose of national defence. | For prevention, investigation, detection and prosecution of criminal offences. |
| Authorities with access | Prosecutor, courts, and State authorities with responsibilities in national security, the police (under the supervision of the Prosecutor for data retention). | Police, intelligence and security agencies, defence agencies responsible for intelligence and counter-intelligence and security missions. | Law enforcement authorities, courts. |
| Procedures for access | Requests of the prosecution, the courts and State authorities in charge of national security will be made on the basis of legal provisions99 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 in order to avoid any modification of these data. | Access requires judicial authorisation. | Requests must be in writing. |
| **Total number of requests made (telephony and internet, successful and unsuccessful)** | | | |
| 2008 | - | 2,821 | - |
| 2009 | - | 1,918 (48) | 5,214 (157) |
| 2010 | - | 1,728 (18) | 7,125 (291) |
| Data protection safeguards | Information unavailable | Transposing law provides for the four principles. | Transposing law provides for the four principles. |
| Data protection authority | Information unavailable | Information Commissioner. | The national regulator and pricing authority in the area of electronic communications supervises the protection of personal data |
| Relevant law | Information unavilable | Article 107a(6) and 107c, Electronic Communications Act. | Article 59a, Electronic Communications Act; Article S33, Act No 428/2002 on the protection of personal data. |
| Reimbursement of costs (operational) | Information unavailable | No | No |
| Reimbursement of costs (expenditure) | Information unavailable | No | No |

| | Finland | Sweden | UK |
|---|---|---|---|
| National law | Two acts: EUR-Lex entry | Five acts: EUR-Lex entry | Three acts: EUR-Lex entry |
| Retention period | 1 year. | Information unavailable. | 1 year. |
| Purpose limitation | For investigating, detecting and prosecuting serious crimes as set out in Chapter 5a, Article 3(1) of the Coercive Measures Act. | Information unavailable | For the investigation, detection and prosecution of serious crime. |
| Authorities with access | Police, border guards, customs authorities (for retained subscriber, traffic and location data).<br>Emergency Response Centre, Marine Rescue<br>Operation, Marine Rescue Sub-Centre (for identification and location data in emergencies) | Information unavailable | Police, intelligence services, tax and customs authorities, Scottish Crime and Drug Enforcement Agency, other public authorities designated in secondary legislation. |
| Procedures for access | Subscriber data may be accessed by all competent authorities without judicial Authorisation. Other data requires a court order. | Information unavailable | A 'designated person' and necessity and proportionality test, in specific cases and in circumstances in which disclosure of the data<br>is permitted or required by law. Specific procedures have been agreed with operators. |
| **Total number of requests made for telephony and internet data, successful (unsuccessful)** | | | |
| 2008 | 4,008 | - | 470,222 (0) |
| 2009 | 4,070 | - | - |
| 2010 | 5,588 | - | - |
| Data protection safeguards | Transposing law only explicitly provides for the requirement to destroy data at the end of the period of retention. | Information unavailable | Transposing law provides for the four principles. |
| Data protection authority | Finish Communications Regulatory Authority supervises operators' compliance with data retention regulations.<br>Data Protection Ombudsman supervises general legality of personal data processing. | Information unavailable | Information Commissioner supervises the retention and/or processing of communications data (and any other personal data) and appropriate controls around data protection. The Interception Commissioner (an acting or retired senior judge) oversees the acquisition of communications data under RIPA by public authorities. Investigatory Powers Tribunal investigates complaints of misuse of their data if acquired under the transposing legislation (RIPA). |
| Relevant law | Article 16 (3), Electronic Communications Act | Information unavailable | Article 6, Data Retention Regulation |
| Reimbursement of costs (operational) | Yes | Information unavailable | Yes |

| | | | |
|---|---|---|---|
| Reimbursement of costs (expenditure) | Yes | Information unavailable | Yes |