



UNIVERSITY OF LAPLAND
LAPIN YLIOPISTO

Rovaniemi Summer School in Legal Informatics

Surveillance and Data Protection

Why is data retention regulation so relevant?

Rovaniemi, 29/08/2011

Manuel David Masseno



Instituto Jurídico Interdisciplinar
da Faculdade de Direito da Universidade do Porto

A constitutional *pre-understanding*:

- **in the Information Society, the main balance between of Powers, Political or else, and Liberties passes by the consideration of *Informational Self-Determination***
 - **even if, in most cases, the very idea of privacy no longer makes sense**
- **from this came out the need to *constitutionalize data protection*:**
 - **both in **Portugal** (Art. 35) and in **Finland** (§ 10(1) *in fine*) and also at the**
 - **European Union** (Art. 16 of the *EU Treaty* and Art. 8 of *Charter of Fundamental Rights*)

Why is data retention regulation so relevant?

- A legal *Micro-system* based on **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
 - Currently under revision
- in **Portugal**, it was transposed by Act N. 67/98, and
- in **Finland** by Act N. 523/1999

Why is data retention regulation so relevant?

- **access, by Public or Private Powers, to personal data** as one of the most controversial questions regarding the European regulation of the Information Society
 - specially “**traffic data**”
- this is also a **critical issue** concerning the **balance between the effectiveness of criminal investigation and the protection of Fundamental Liberties**, as well as for the effectiveness of other protected interests, such as those related to Intellectual Property
 - **traffic monitoring is basic for HADOPI implementation**
 - *Lex Nokia...*

Why is data retention regulation so relevant?

- **also for Information Services Providers (ISPs), abstaining from having access to personal data is very relevant**
- besides, the **liability exemptions** of Art. 12 to 14 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('**Directive on electronic commerce**') depend on that abstention, according to the EU Court of Justice
 - at **Google France Cases** (C-236/08 to C-238/08, of 23 March 2010) and more recently at
 - at **L'Oréal Case** (C-324/09, of 2011)

Why is data retention regulation so relevant?

Also relevant is the **New Regulatory Framework of Electronic Communications:**

- **Directive 2009/136/EC** of the European Parliament and of the Council of 25 November 2009 amending [...] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [...] (**'Citizens Rights Directive'**)
- “National measures regarding end-users’ access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, including in relation to privacy and due process, as defined in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.”

Why is data retention regulation so relevant?

- “In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. **When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.**” and also
- “Member States shall ensure that **the storing of information, or the gaining of access to information already stored**, in the terminal equipment of a subscriber or **user is only allowed on condition that the subscriber or user concerned has given his or her consent**, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.”

Focusing ...what is our **subject?** We've been discussing what, precisely?

- **“Data’ means traffic data and location data and the related data necessary to identify the subscriber or user” (Art. 2(2) (a) of 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)**

Even more precisely:

- “**traffic data**’ means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof [...]”
- “**location data**’ means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.” (**Art. 2. (b) (c) of 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**

Why is data retention regulation so relevant?

At a **first stage**, the **objective** was to protect people from a private processing of such data:

- “1. **Traffic data** relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service **must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication [...]. and**
- 2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. **Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.” (Art. 6.)**

Why is data retention regulation so relevant?

However, there was a statement regarding the possibility of data retention was previewed:

- **“Member States may adopt legislative measures to restrict the scope of the rights and obligation [...] when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system [...] To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph.”, Art. 15(1)**

But with a special concern in terms of the **respect for Human Rights**:

- “[...] All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.” (**Art. 15(1) of the EU Treaty**)
- However, this possibility **was not used by any Member State**, and **was not even necessary** having in mind the “**Principle of Conferral**” (**Art. 5(1) (2) of EU Treaty**).

Then, a major change occurred. What happened? (the *occasio legis*):

- the **terrorist attacks of Madrid**, 11 March 2004, **and of London**, 7 July 2005
- Police could only succeed because, mostly by hazard, got some connection data from cell phones
- **Pressure from the National Public Opinions and Governments upon the European Parliament**, in order to **put security concerns in the centre**, without such an emphasis in Fundamental Rights, as this was a subject already with the Co-decision Procedure
- So, we should **identify the 2006 Directive as an “Emergency Act”**, with all the due consequences

So, what are the main traits of the Data retention Directive?:

- It “[...] 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.”, **Art. 1(1)**
- And “O Member States shall ensure that **the categories of data specified [...] are retained for periods of not less than six months and not more than two years from the date of the communication.**”, **Art. 6**

These rules have been under a close review by the Judiciary, European but mostly National:

- Due to the **Primacy Principle of EU Law** over National legal systems, **National Courts** only dealt with the transposition acts and found unconstitutional some of its provisions, as it have already happened in **Germany, Romania, Bulgaria** and the **Czech Republic**
- and the **Court of Justice of the European Union** is about to address the issue, in relation to the content of the Directive, as we will see

The Judgement of the German Constitutional Court (N. 10/2010, 2 of March 2010)

Found unconstitutional the Act for the Amendment of Telecommunications Surveillance (*Gesetz zur Neuregelung der Telekommunikationsüberwachung*), of 21 December 2007

The main findings:

- a blanket retention “**constitutes a particularly serious encroachment with an effect broader than anything in the legal system to date**”
- **severely burdens the right to informational self-determination** in terms of scope of application as well as comprehensiveness of information retained (Art. 10)
- so, it **doesn't comply with the Principles of Proportionality and of Purpose-Specification**

Finally, the High Court of Ireland referred the validity of the Directive regarding of the Treaties, the 5th May 2010

- The question is whether a mass surveillance of this sort is compatible with constitutional guarantees of fundamental rights?
 - *id est*, even if not explicitly, the **Principle of Proportionality** is underlying
- Not just in procedural grounds, as before

Why is data retention regulation so relevant?

And we should not forget the Ruling of the EU Court of Justice of 29 January 2008, Case C-275/06, Productores de Música de España (*Promusicae*) / Telefónica de España SAL

Whose issue was the access to traffic data...

“[...] Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which **allows a fair balance to be struck between the various fundamental rights protected by the Community legal order.** Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the **principle of proportionality.**”

Why is data retention regulation so relevant?

In Portugal, a reasonable transposition took place, by Act N. 32/2008, of 17 July

- Only for **serious crimes**, namely terrorism, organized crime, kidnaping, crimes against State security, **Art.2(2)(g)**
- Data is to be preserved during **one year, Art. 6**
- Severe **procedural restrictions** in order to assure that only if a strictly proportional requirement is present the access to the retained data will be provided to a criminal police organization, and **always by a Court, Art. 9**
- **The New Cybercrime Law, Act N. 109/2009, of 15 September, didn't change any of the requirements, Art. 11(2)**

In Finland, the transposition took place by the Amendment to the Act on the Protection of Privacy in Electronic Communications, 343/2008, of 23 May 2008

- ISPs and phone companies must **retain their customers' traffic data for a period of 12 months** from the date of the communication
- **small ISPs are exempt from obligations to retain data**
- **Such data may be used only for the purposes of investigating and resolving serious crimes**, and the consideration of charges for criminal acts referred to in the Coercive Measures Act of 1987 (450/1987)

Why is data retention regulation so relevant?

But, returning to ***Proportionality***, does it make sense imposing data retention to ISPs?

According to **Heinz Kiefer**, President of Eurocop (European Confederation of Police), “[...] it remains easy for criminals to avoid detection through fairly simple means, for example mobile phone cards can be purchased from foreign providers and frequently switched. The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them. Activities like these are unlikely to boost citizens’ confidence in the EU’s ability to deliver solutions to their demand for protection against serious crime and terrorism.” (2005)

Why is data retention regulation so relevant?

A, likely, **turning point** might be the **Report from the Commission** to the Council and the European Parliament - **Evaluation on the Data Retention Directive** (Directive 2006/24/EC) (COM(2011) 225 final), of 18 April 2011:

- **the European Commission was obliged to submit a report on the evaluation of the Directive** and its impact on economic operators and consumers, until the 15 September 2010, Art. 14
- however, **the Commission assumed the value of the Directive**, and only asked Member States information and supporting data
- a Letter was sent the 15 July, but **got only 10 answers**, from **Finland** but not from Portugal...

Why is data retention regulation so relevant?

“The moment of truth for the Data Retention Directive’ [...] It goes without saying that such a massive invasion of privacy needs profound justification. This justification is not established if the retention of all such information is only considered ‘a useful tool’ for law enforcement authorities or if it just ‘helps’ solving serious crimes.” (**Peter Hustinx** – the European Data Protection Supervisor, at a Conference on the 2006 Directive, Brussels, the 3rd December 2010).

Attention should also be paid to the **“Shadow evaluation report”**, simultaneously published by *European Digital Rights*

Main issues:

- **Legal basis**, regarding the object of the Directive, **Art. 1**
 - Related to “[...] the establishment and functioning of the internal market.”, **Art. 114 of TFEU**
 - **not police cooperation**, or law enforcement in general
- **Access to data**: authorities and procedures and conditions, **Art. 4**
 - in other words, **who may have access to data and in what cases?**

Why is data retention regulation so relevant?

- **Scope of data retention and categories of data covered, Art. 1(2), 3(2) and 5**
 - For instance, how to deal with “anonymizers”
- **Periods of retention, Art. 6 and 12**
- **Data protection and data security and supervisory authorities, Art. 7 and 9**
- **Statistics, Art. 10**
- **Decisions of Courts in transposing laws**
 - National Courts in transposing laws, but also of the ECHR and the CJEU

In short, the **European Commission** seems to be **open to a revision of the Directive:**

- after an assessment of its impact, in terms of effectiveness, changes should be made in order to
 - assure a more consistent harmonization
 - reimburse Operators for the costs they incur

And, above all

- **Ensuring Proportionality** in the end-to-end process of storage, retrieval and use
 - more harmonization of, and possibly shortening, the periods of mandatory data retention
 - ensuring independent supervision of requests for access and of the overall data retention and access regime applied in all Member States
 - limiting the authorities authorized to access the data

Why is data retention regulation so relevant?

- reducing the data categories to be retained
- providing guidance on technical and organizational security measures for access to data including handover procedures
- providing guidance on use of data including the prevention of data mining;
and
- developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument

- Never forgetting the **EU Court of Justice**
 - **Joint Cases Schecke (C-92/09) and Eifert (C-93/09)**, of 9 November 2010
 - data regarding all the beneficiaries of CAP payments
 - as always, the ***Principle of Proportionality***
 - **Case Ireland v. the Parliament and the Council (C-301/06)**, of 10 February 2009
 - **the legal basis of the Directive**

○ Or The **European Court of Human Rights**

- **Case of S. and Marper v. The United Kingdom**, 4 December 2008 (Applications 30562/04 and 30566/04)
 - “In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State [So] **the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.**”

Kiitos paljon!