Looking for the best period of Data Retention

In April 2014, the European Court of Justice (ECJ) declared Directive 2006/24/EC invalid on the ground that European Union legislators had exceeded the limits of proportionality in forging the Directive. The ECJ did not specify otherwise, so the Data Retention Directive is void "ab initio", and EU Members who have transposed the Directive into their national legal systems must ensure compliance with the ECJ's judgment.
Following that judgment, two cases were referred to the ECJ on the general obligation imposed, in Sweden and in the UK, on telecommunication service providers to retain data relating to electronic communications. In Sweden, the telecommunications undertaking Tele2 Sverige notified the Swedish post and telecommunications authority of its decision to cease retaining the data and of its proposal to delete the data already registered (Case C-203/15). In UK, Tom Watson, Peter Brice, and Geoffrey Lewis brought actions against the British data retention rules, which authorize the Home Secretary to require public telecommunications operators to retain all communications data for a maximum period of 12 months (Case C-698/15).

In his opinion read on July 16, 2016 the Advocate General affirms that ***a general obligation to retain data may be compatible with EU law. The action by Member States against the possibility of imposing such an obligation is, however, subject to satisfying strict the following requirements****:*

- *the data retention obligation must have a legislative or regulatory basis possessing the characteristics of accessibility, foreseeability, and adequate protection against arbitrary interference;*
- *the obligation must respect the essence of the right to respect for private life and the right to the protection of personal data;*
- *the obligation of retained data must aim to fight against "serious" crime (however the Advocate General does not define "serious" crime) and must be proportionate to this objective;*
- *the judgment in Digital Rights Ireland must be case must be respected.*

The obligation must be accompanied by all the safeguards described by the Court in paragraphs 60-68 of Digital Rights Ireland, in particular: (i) prior review by a Court or an Independent Administrative Body before access to data is granted; (ii) data must be retained within the EU; (iii) strict limitations on the retention period. The Advocate General indicates that a duration of 6 months has already been considered as reasonable.

In the meantime we are in the absence of a valid Data Retention Directive and Member States may still provide for a data retention scheme. Governments are looking to protect internal security and efficiently to prosecute crimes by ***revising*** *their data retention regimes. Other Member States that annulled data retention laws are actively considering replacement measures.*
In contrast to this, in ***Italy*** *nothing has changed, and the data retention time is actually increased. The topic is highly debated because, due to various subsequent acts aimed at anti-terrorism efforts. The latest retention terms have been replaced - in connection with investigations for serious crimes such as terrorism, mass murder, civil war, organized crime, etc. - by an obligation for telecom operators to retain "already" collected data from April 21, 2015 until June 30, 2017 without making any distinction between traffic type. Retention terms under Article 132 of the Italian Privacy Code will be reinstated as of July 2017 - 24 months for telephone traffic, 12 months for telematic traffic, and 30 days for unanswered calls - unless such terms are again prolonged or a new law is adopted (this means that June 30, 2017 will be available over* ***4 years*** *of telephone traffic).*

In other EU Member States the situation is different. For example, in ***Belgium*** *the new law on data retention was adopted on May 29, 2016 and entered into effect on July 28, 2016. For minor crimes, access to retained data can be granted only for a maximum period of 6 months. For more severe crimes, access can be requested for 9 months with a maximum period of 12 months for the most serious crimes. In* ***France****, the legal framework defining data retention is principally set out in CPEC, Code of Posts and Electronic Communications (Article L. 34-1), and in the Law of June 21, 2004. The CPEC requires 12 months of retention period for such data. In* ***Germany****, in October 2015 the Parliament adopted a new law - published in the Federal Law Gazette on January 4, 2016 - requiring telecommunications operators and ISPs to retain phone/call detail records such as phone numbers, the date/ time of phone calls and the content of text messages (if these cannot be retained without their content), and internet user metadata such as IP addresses, port numbers and the date/time of Internet access, for* ***10 weeks*** *and cell phone location data for* ***4 weeks*** *(113b §). After the respective period, all data must be deleted at the latest within 1 week. The law strictly prohibits retention of data concerning the content of communications, email data, and information regarding visited web pages (urls). In* ***Spain****, Law 25/2007 of October 18, 2007 (the Data Retention Law) is in line with the Spanish Constitutional Court's rulings, regarding the right of secrecy of communications. As a general rule, the retention period is 12 months from the date on which the communication occurred but, subject to prior consultation with telecom operators, this period can be increased to a maximum of 2 years and reduced to a minimum of 6 months, taking into account storage and data retention costs.*

In some European States where data retention regimes are in place, capital and operational costs incurred in compliance are reimbursed by the government. More difficult is the situation in those States, such as in Italy, where law does not provide refund. ***Most EU Governments see data retention as an efficient way to protect national security, public safety, and address crime. This issue is the challenge of the future*** *by introducing stricter access controls, specifying what types of crime permit access to retained data, delineating "appropriate" retention periods - the retention time is closely related to maintenance costs - and requiring data to be retained within the EU. ©*

Giovanni Nazzaro