JONES DAY

AUGUST 2016

COMMENTARY

The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws

Triggering a landslide of legislative reforms and legal battles, the European Court of Justice's ("ECJ") landmark judgment of April 8, 2014, *Digital Rights Ireland* (C-293/12), invalidated the Data Retention Directive 2006/24/EC, which provided that providers of publicly available communications services must retain certain data. The ECJ considered that such data retention obligations went beyond what was strictly necessary and violated the Charter of Fundamental rights of the European Union. The ensuing national legislative revamps and national court proceedings now seek to draw the line between combating crime and terrorism, and respecting fundamental privacy and data protection rights.[1]

Currently, a pair of national sequels to *Digital Rights Ireland* are pending before the ECJ (Tele2 Sverige AB (C-203/15) and Watson and Others (C-698/15)), which must assess the compatibility of the UK and Swedish national data retention obligations with EU law. A telecom operator in Sweden and several private parties in the United Kingdom challenged their respective national data retention laws, on the same grounds that led the ECJ to annul the Data Retention Directive. Both national laws impose general data retention obligations. The Swedish law, implementing the now-invalidated Directive, provides for a retention period of up to six months. The UK law, adopted after the annulment of the Directive, sets out a retention period of up to 12 months. The Swedish and British courts decided to refer to the ECJ the question of compatibility of these data retention laws with the EU e-Privacy Directive[2] and the Charter of Fundamental Rights of the EU.[3]

On July 19, 2016, Advocate General Saugmandsgaard Øe ("AG") issued an opinion ("Opinion") on these cases, which validates general data retention obligations for electronic communications providers, provided that appropriate safeguards are in place. The Opinion considers that such national legislation imposing general obligations upon service providers to retain so-called "traffic data" (i.e., communications data excluding content) may be compatible with EU law, but only in relation to the fight against serious crimes and if accompanied by appropriate safeguards.

This *Commentary* provides a summary overview of the Opinion and the status of current data retention laws in selected EU Member States.

The AG's Opinion

Drawing on the court's findings in *Digital Rights Ireland*, the Opinion dismissed the parties' claim that national law imposing an obligation of general data retention constitutes a violation of EU law in itself. While emphasizing that general data retention obligations entail a serious interference with the right to privacy and protection of personal data, the Opinion recognizes that such rules also benefit law enforcement. Furthermore, as explicitly provided in the EU e-Privacy Directive, EU Member States have the right to adopt legislative measures providing for the retention of data for limited periods of time.

Accordingly, the Opinion finds that national legislation imposing general data retention obligations may be compatible with EU law, but only in conjunction with the following safeguards:

- Any data retention obligation must have a **proper legal basis** that is adequately accessible and foreseeable and that provides adequate protection against arbitrary interference.

- Such obligation must **observe the rights elaborated in the Charter of Fundamental Rights of the EU**, particularly the right to privacy and the right to the protection of personal data. This requirement is considered to be met as long as the content of the communications is not retained.

- The obligation must pursue an objective of general interest that, according to the Opinion, can be only the **fight against serious crime**, to the exclusion of lower-level offenses or noncriminal proceedings. However, the Opinion does not define "serious crime," other than listing the examples of terrorism, murder, kidnapping, and child pornography, and despite the fact that the UK High Court judgment under appeal at the national level precisely criticized this lack of clarity in what constitutes a "serious crime."

- The obligation must be **appropriate, necessary, and proportionate** to achieve the defined objective of fighting serious crime. Thus, data retention obligations cannot go beyond what is strictly necessary to attain such goal, and where no other less-restrictive but as-effective means are available. In this regard, the Opinion emphasizes that users, geographic areas, and means of communications covered by the law can vary. The Opinion considers it preferable to exclude data from the retention obligation that is particularly sensitive in terms of fundamental rights, such as data that is subject to professional privilege or data enabling the identification of a journalist's source. Nevertheless, it also recognizes that limiting retention obligations to a specific geographic area or a particular means of communication could considerably reduce the utility of the measures.

- All protections stated by the court in the *Digital Rights Ireland* case must be respected, in particular: (i) **prior review** by a court or an independent administrative body before access to data is granted (possibly *ex post facto* in the case of extreme urgency); (ii) data must be **retained within the EU**; and (iii) **strict limitations on the retention period**: the Opinion does not take a final stance on existing national retention periods but indicates that a duration of six months has already been considered as reasonable. The Opinion further requests that national laws expressly lay down an obligation to delete any retained data, once its use is no longer necessary in combating serious crime.

- Finally, the obligation must be **proportionate** to the objective of the fight against serious crime. In line with democratic values, the advantages offered by the data retention obligation must outweigh its inherent risks.

The Opinion considers the above safeguards to be mandatory and cumulative. According to the AG, they constitute a minimum threshold that can be enhanced by additional requirements imposed by EU Member States. However, the Opinion leaves it to national courts to decide whether, in each particular jurisdiction, those safeguards are sufficiently met.

Impact of the Opinion

Although AG opinions are generally nonbinding, the ECJ tends to follow their advice in the majority of cases. AG opinions nevertheless leave scope for further clarification, and in

particular in the present case in relation to what constitutes a "serious crime" and what retention duration is proportionate. Clearly, however, the Opinion calls into question any national legislation of EU Member States that does not adequately cover the list of mandatory safeguards. Final rulings in both the Swedish and UK cases are expected by end-2016.

In the meantime, the EU e-Privacy Directive, which provides for the right to impose data retention obligations, is currently under revision. A consultation was launched in April 2016, and the Commission is expected to prepare a new legislative proposal by the end of 2016, although it remains unclear if and how data retention rights may be amended.

Status of Data Retention Laws in Selected EU Member States

Belgium. In June 2015, the Belgian Constitutional Court annulled the national law implementing the invalidated Data Retention Directive. Subsequently, the Belgian legislature drafted a new law, on the basis of the findings in the *Digital Rights Ireland* judgment. The new law aims to achieve greater proportionality, thereby granting access to retained data only where the pursued objective cannot be achieved by more privacy-conscious means. Although the standard data retention period is 12 months, access is now more restricted and tailored to the severity of the crime. Accordingly, for minor crimes, access to retained data can be granted only for a maximum period of six months. For more severe crimes, access can be requested for nine months, with a maximum period of 12 months for the most serious crimes. Additionally, physicians, lawyers, and journalists receive additional protection in view of their legal privilege. The law was adopted on May 29, 2016, and entered into effect on July 28, 2016.

France. The current French legal framework defining data retention is principally set out in the Code of Posts and Electronic Communications ("CPEC") (Article L. 34-1) and its implementing regulations (Art. R. 10 12 and *seq*. CPEC), and in the Law of June 21, 2004, on confidence in the digital economy (Article 6, II) and its implementing regulation (Decree n°2011-219 of February 25, 2011).

Pursuant to the CPEC, electronic communications operators must retain specific data for judicial authorities in the investigation and prosecution of criminal offenses, as well as for specific administrative or governmental authorities. Such data consists of technical data enabling the identification of the user and the technical aspects of his or her communications (as opposed to the actual content of such communications). The CPEC requires a one-year retention period for such data. Under the Law of June 21, 2004, internet access providers and internet hosting services must also retain, for a one-year period, information on the identity of the subscribers to their services who contribute to online content, as well as related technical data. Such data can be accessed by judicial authorities in the course of legal proceedings.

The above data retention framework is currently under challenge before the *Conseil d'Etat* (French supreme administrative court) by several associations. They contend that the framework does not comply with the Charter of Fundamental Rights of the EU, on grounds similar to those that led to invalidation of the 2006 Data Retention Directive.

Germany. In 2010, the national law implementing the Data Retention Directive 2006/24/EC was declared unconstitutional by the German Constitutional Court. In October 2015, the German Parliament adopted a new law taking a more restrictive and "privacy-conscious" approach in setting conditions for the retention of data, requiring telecommunications operators and ISPs to retain phone/call detail records (including numbers, call times, and text messages) and internet user metadata, such as IP addresses and port numbers, for 10 weeks and cell phone location data for four weeks. After the respective period, all data must be deleted at the latest within one week. The law strictly prohibits retention of data concerning the content of communications, email data, and information regarding visited web pages (URLs). Such prohibition also includes text messages, if these cannot be retained without their content. Location data may not exceed a level of precision beyond that which enables authorities to determine the (general) geographic area from where a signal was emitted.

Access to retained data is restricted to law enforcement agencies for the purposes of prosecuting particularly serious crimes and preventing a concrete danger to the state or to the life or liberty of a person. Further restrictions apply with regard to privileged communications. The retained data must

be stored within Germany, and a high standard of data security must be ensured. The German Federal Network Agency is currently drafting guidelines to specify these standards, and these will hopefully set forth practical solutions.

The new data retention law went into effect on December 18, 2015, after publication in the *Federal Law Gazette* on December 17, 2015. The compliance deadline for concerned parties is 18 months. However, the data retention provisions have raised controversy and are currently under review by the Constitutional Court. While the court declined to issue a preliminary injunction against these provisions, a final judgment is still pending.

Italy. Notwithstanding the Italian Data Protection Authority's request for more privacy-conscious retention, the Italian legislator has largely disregarded the *Digital Rights Ireland* judgment. The topic is highly debated because, due to various subsequent acts aimed at anti-terrorism efforts, the retention terms under the Italian Privacy Code (Article 132) have been successively modified. The latest retention terms (24 months for telephone traffic, 12 months for IT traffic, and 30 days for unanswered calls) 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 until June 30, 2017. Retention terms under Article 132 of the Italian Privacy Code will be reinstated as of July 2017, unless such terms are again prolonged or a new law is adopted.

Netherlands. In March 2015, the Dutch provisional judge (*voorzieningenrechter*) of the court in The Hague suspended the Dutch Telecommunications Data (Retention Obligation) Act (*Wet Bewaarplicht Telecommunicatiegegevens*). Following this suspension and the *Digital Rights Ireland* judgment, a member of the Dutch House of Representatives (*Tweede Kamer*) introduced a bill considering the repeal of the Telecommunications Data (Retention Obligation) Act. Furthermore, the Dutch Minister of Security and Justice has announced plans for a legislative proposal to amend the Telecommunications Act (*Telecommunicatiewet*) and the Code of Criminal Procedure (*Wetboek van Strafvordering*) in view of maintaining acceptable retention obligations under national law.

Spain. In Spain, Law 25/2007 of October 18, 2007 ("Spanish Data Retention Law"), which implemented the now-invalidated Data Retention Directive, addresses data retention related to electronic communications and public communications networks. The Spanish Data Retention Law is, however, in line with the Spanish Constitutional Court's rulings regarding the right of secrecy of communications: (i) data retained is only that which is related to the communication, not the content, and (ii) data transfers that affect a communication or specific communications are subject to prior judicial authorization.

As a general rule, the retention period obligation ceases 12 months from the date on which the communication occurred. However, legally and subject to prior consultation with telecom operators, this period can be increased to a maximum of two years and reduced to a minimum of six months, taking into account storage and data retention costs, the interests raised by the investigation, and in relation to only the detection and prosecution of serious crimes.

After the invalidation of the Data Retention Directive, the Spanish Data Retention Law underwent some modifications, e.g., in relation to sanctions and that data transfers must be made in electronic form within seven calendar to the authorized representatives mentioned in the Spanish Data Retention Law, among others. Furthermore, sanctions are categorized according to very serious, serious, and minor infractions in relation to the nonretention of data.

United Kingdom. The United Kingdom implemented the now-invalidated Data Retention Directive in 2009 by way of the Data Retention (EC Directive) Regulations 2009. Following the Directive's invalidation, the United Kingdom passed the Data Retention and Investigatory Powers Act 2014 ("DRIPA") as an emergency measure, providing for varying data retention periods of up to 12 months. However, in July 2015, the UK High Court held that DRIPA was incompatible with human rights legislation. The UK government appealed this decision, resulting in the pending referral to the ECJ discussed in this *Commentary*. The UK government has also introduced the Investigatory Powers Bill into Parliament. This measure will modify UK law on investigations, interception, and data retention, and it currently proposes a 12-month data retention period.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Elizabeth Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Giuseppe Mezzapesa
Milan
+39.02.7645.4001
gmezzapesa@jonesday.com

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

Bastiaan K. Kout
Amsterdam
+31.20.305.4200
bkout@jonesday.com

Endnotes

1 *See* EU Data Retention Directive Declared Null and Void: What is Next and How The Ruling Has Been Received in the Member States.

2 Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, pp. 37–47).

3 Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012, pp. 391–407).