THE
NATIONAL LAW REVIEW

The ECJ Rules on the Compatibility with EU Law of Domestic Data Retention Requirements Imposed on Providers of Electronic Communications Services

Article By
Claude-Étienne Armingaud
Alexandre Balducci
K&L Gates
Privacy, Data Protection and Information Management Alert

- Communications, Media & Internet
- Global
- European Union

Thursday, March 16, 2017

ECJ (Grand Chamber), 21 December 2016, Joined Cases C-203/15 and C-698/15

After its invalidation of the data retention requirements imposed by Directive 2006/24/EC in its Digital Rights Ireland decision dated 8 April 2014[1], the ECJ was requested to assess the compatibility with the Directive 2002/58/EC[2] (the "ePrivacy Directive") and the Charter of Fundamental Rights of the European Union (the "CFREU") of a domestic legislation mandating a general and indiscriminate obligation to retain traffic and location data, without prior judicial review, for purposes including the fight against crime.). The ECJ joined the two cases which had been submitted for review and issued its decision on 21 December 2016 (the "Decision").

EU law prohibits general and indiscriminate data retention requirements

Article 15(1) of the ePrivacy Directive requires all providers of electronic communications services to grant national agencies with access to the personal data they retain for limited purposes, including national security and the prosecution of criminal offences.

The ECJ considered that the scope of the ePrivacy Directive with respect to the confidentiality of electronic communications encompassed domestic legislations grounded on this Article. As a result, access to personal data retained by providers of electronic communication services shall remain strictly limited.

In this case, both Swedish and English national laws imposed a similar general obligation to retain communication data bearing on communication service providers, for various purposes other than the fight against crime, and under large access conditions by third parties. In his opinion delivered on 19 July 2016 (the "Opinion"), Advokate General Saugmandsgaard Øe recognized that such a data retention obligation could still comply with EU law, provided that it remained subject to national laws' strict safeguards aimed at protecting the data subject's fundamental rights.

In accordance with the Opinion, the ECJ ruled that EU law precludes national legal frameworks from imposing retention of traffic and location data on providers of electronic communications services which would be both general and indiscriminate. Nevertheless, the ECJ expressly added that the provision of preventive and targeted collection of data remained possible for Member States. However, such retention will need to comply with two cumulative requirements, and be both: (i) proportionate and limited to a strictly necessary extent to limited purposes and (ii) circumscribed by adequate safeguards with respect to data subjects. Both these restrictions are addressing the need for effective protection of personal data against any risk of misuse.

The ECJ imparts restrictive safeguards for domestic data retention requirements

The ECJ noted that general data retention requirements grounded on Article 15(1) of the ePrivacy Directive amount to an authorized interference in the fundamental rights of privacy and protection of personal data provided in Articles 7 and 8 of the CFREU. As a consequence, pursuant to Article 52(1) of the CFREU, and as highlighted in the Opinion, data retention requirements may only be lawful provided that they are proportionate and limited to the strictest extent possible, i.e. for purposes of the "fight against serious crime" or objectives of general interest recognized by the EU. Any domestic legislation to that effect will thus need to be clear and precise, and data subjects will need to be informed about the objective circumstances and conditions under which preventive data retention requirements may be applied.

The ECJ has not precisely defined the scope of the limited purposes for which data may be retained and Member States may have some leeway in this respect.

While the fight against terrorism and organized criminality undoubtedly enter the "serious crime" category, tax fraud may not be a sufficient ground. The notion of "objectives of general interest recognized by the EU" also remains undefined by the

ECJ; nonetheless Member States may refer to the general objectives set forth in the Treaty on the Functioning of the EU in this regard.

In addition, the ECJ added that access to the retained data needed to be governed by strict substantive and procedural requirements set by national legislations in order to limit indiscriminate access to data and further misuse by national authorities.

In particular, access to the retained data shall solely be granted to designated national agencies for the purposes set forth in the ePrivacy Directive and only with regards to individuals suspected of planning, or, more broadly, implicated in a serious crime, save cases where national security is at stake (terrorism, etc.).

The Decision also provided that access to the retained data by national authorities may only occur further to prior review by a judicial or independent administrative authority, safe for urgency matters, and that data subjects must receive information relating to the access to their personal data once such access has been granted.

Having regards to the recent international intelligence scandals, while data subjects may be targeted outside the EU, and having regards to the sensitivity of the retained data, the ECJ added that national legislation had to provide for storage of the retained data within the EU. Consequently, all transfer of such retained data outside of the EU is effectively prohibited. Such safeguard will limit the use of foreign subcontractors by EU national authorities (data analysts, security services, etc.).

The aforementioned safeguards are expected to greatly improve the protection of data subjects' fundamental rights. However, at the same time, they may also create issues in terms of international police cooperation, including cases of cross-border fight against "serious crime".

Expected consequences of the Decision on National laws

The ECJ judgement will impact several national laws relating to "technical" data retention (including traffic and location data), whereas such data became a ubiquitous tool for intelligence agencies and national authorities during the last decade, for various purposes ranging from the fight against crime to economic intelligence.

This judgement may render unlawful some provisions currently set forth under French law and in particular the data retention requirements imposed on providers of electronic communication services. Indeed, the French Code of Post and Electronic Communications relating to the retention of technical communication data by electronic communication providers does notably provide for exceptions to the principle of limited duration for the data retention; furthermore, French law does not provide for the possibility of a prior judicial or administrative review for accesses granted to such data by authorized national agencies.

As a reminder, judicial or administrative review may only intervene today after access has been granted to national authorities, as per the latest Act n°2015-912 dated 24 July 2015 relating to intelligence, which created a commission in charge of controlling intelligence techniques. Nevertheless, such review does not comply as

such with the Decision.

---

[1] ECJ, 8 April 2014, Digital Rights Ireland and Seitlinger and others, Joined cases C-293/12 and C-594/12

[2] 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