1.2.2017

Case note on joined cases C-203/15 Tele2 Sverige AB and C-698/15 Tom Watson a.o.

Case facts

On 21 December 2016, the Court of Justice (CJEU) handed down a Grand Chamber judgment in joined cases Tele2 Sverige (C-203/15) and Tom Watson a.o. (C-698/15) concerning the ability of Member States to oblige electronic communications service providers to retain traffic and location data for all subscribers and registered users. The cases arose under an ePrivacy Directive exemption (Art. 15 Directive 2002/58/EC) allowing Member States to restrict the rights on the confidentiality of communications, for instance for reasons of national security.

After the CJEU’s cutting-edge Digital Rights Ireland decision of April 2014, in which it declared the EU Data Retention Directive invalid, courts in several Member States (e.g. Austria, Slovenia and Romania) struck down national data retention laws.¹ In Sweden and the UK, domestic legislation has been challenged before national courts which have referred the matter to the CJEU for preliminary ruling.

The disputes in the two cases are slightly different: In Sweden, Tele2 Sverige, a telecommunications operator, refused to continue sending customer data to the Swedish National Police Authority which then brought proceedings for non-compliance with national law. In the UK, several complaints were lodged asking for the review of the legality of certain parts of the national legislation that permitted indiscriminate bulk collection by electronic communications providers.

Ruling

- Compatibility of general data retention with EU fundamental rights

Against the background of the invalidated Data Retention Directive, the CJEU first considered whether the national law (here, only the Swedish law as the UK Court did not refer a question to this end) fell within the scope of EU law. The Court found that Directive 2002/58/EC (ePrivacy Directive), as last amended in 2009, provides an exception allowing Member States to restrict the rights and obligations as laid down in the Directive on grounds of national security, defence, public security or for criminal law enforcement purposes (Art. 15(1)). It followed that national measures relating to the retention of data for the purpose of fighting serious crime fell within the scope of the ePrivacy Directive.

The Court further examined Art. 15(1) in light of the fundamental rights to privacy (Art. 7), protection of personal data (Art. 8) and the freedom of expression (Art. 11) as guaranteed by the Charter of Fundamental Rights (CFR). While the relevance of Articles 7 and 8 flows from the Court’s previous case law (notably Digital Rights Ireland and Schrems), the Court also specifically highlighted the importance of the freedom of expression.

The CJEU moreover underscored the ePrivacy Directive’s aim of ensuring a high level of protection of users’ personal data and privacy. Since Article 15(1) constitutes an exception to the general principle of confidentiality of communications, it must be interpreted strictly. The Court also clarified that the list of grounds allowing derogation from the general principle was exhaustive.

It further noted that Article 15(1) sets out safeguards for derogations, notably the principle of proportionality, also reflected in Article 52(1) CFR, which sets out the scope and interpretation of the Charter’s fundamental rights. Accordingly, limitations to the exercise of fundamental rights may be made only if “they are necessary and genuinely meet objectives of general interest recognised by the Union”.

The Court held that national legislation that provides for a general and indiscriminate retention of all traffic and location data, of all users of electronic communications services, relating to all means of electronic communications, and imposing a duty on service providers to keep all data without exception went beyond what was necessary and was disproportionate.

The CJEU explained, referring to Advocate General Saugmandsgaard Øe’s opinion of July 2016, that the bulk collection of traffic and location data made it possible to establish an exact profile of individuals. Similar to the data containing the actual content of the communication, location and traffic data were thus to be considered as sensitive data deserving protection under the Charter rights.

Although the Court acknowledged that we increasingly rely on modern investigation techniques to fight against serious crime, including terrorism, this objective did not in and of itself justify the means. This was particularly true since all data of all users was being retained, even of those for whom there was "no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences". It is thus necessary for the data collected to reveal a link with the objective of fighting serious crime.

However, the CJEU considered that Member States were not precluded from introducing national legislation requiring, “as a preventive measure”, targeted retention of traffic and location data provided that “the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted”.
Conditions for data retention

Answering the second preliminary question, the Court reiterated that combating serious crime was the only objective justifying access to the retained data. Given the seriousness of the interference with fundamental rights, access to the data must be proportionate and accompanied by “adequate safeguards”. It was therefore imperative that national legislation lay down the “substantial and procedural conditions” under which electronic communications service providers are required to grant access to competent national authorities.

As a general rule, access can only be granted to the data of those persons who are suspected of planning, committing or having committed serious crimes. It is interesting to note that the CJEU considered that access to data might also be granted where “vital national security, defence or public security interests are threatened by terrorist activities” provided that there was objective evidence that the data contributed to pursuing the objective.

In addition, the Court noted that, except in urgent cases, competent authorities could only access the data if their request was reviewed in advance, either by a court or by an independent administrative body. The person whose data was being processed should be notified and should have appropriate legal remedies. In this context, the CJEU underlined the need for electronic communications service providers to have effective security mechanisms in place to protect the retained data against the risk of misuse and unlawful access. In particular, national legislation should require the data to be retained within the European Union.

The CJEU left it to the Swedish and UK courts to determine whether the national legislation complied with these requirements.

Importance of the case

The CJEU’s decision does not come as a surprise as it confirms and further develops the 2014 Digital Rights Ireland reasoning. With this ruling, the Court establishes specific requirements for national data retention laws that only implicitly derive from the 2014 judgment. The requirements underscore how seriously data retention practices interfere with EU fundamental rights and the need to establish adequate safeguards. These safeguards need to be clearly spelled out in national legislation, and must govern the access of competent authorities to the retained data and be subject to an ex ante review mechanism.

The Court also takes the opportunity to further strengthen the rights to privacy and protection of personal data, as guaranteed by Articles 7 and 8 CFR. What is noteworthy is the fact that the traditional pairing of Articles 7 and 8 CFR is expanded by reference to Article 11 CFR guaranteeing the right to freedom of expression. Echoing the European Court of Human Rights’ well-known Handyside decision of 1976, the Court champions freedom of expression as “one of the essential foundations of a pluralist, democratic society”, reflecting the values
on which the Union is founded (Art. 2 TFEU). The Court’s acknowledgement of this right’s paramount importance for democracy should certainly be welcomed.

The Court elaborates in detail the adverse effects of general data retention, classifying the interference with fundamental rights when subjecting individuals to “constant surveillance” as “particularly serious”. It did not, however, go as far as to confirm that the essence of the fundamental rights was compromised, a finding that it reached in the Schrems decision concerning transfer of personal data to third countries, notably the US. In terms of the seriousness of the breach, the current judgment is just one step below Schrems.

The issue of data retention remains controversial. The ePrivacy Directive is currently being reviewed by the EU institutions. On 10 January 2017, the Commission published a proposal for an ePrivacy Regulation that would continue to allow Member States to adopt restrictions on grounds of national security or criminal law enforcement. Any implementing measures must indeed comply with the Court’s ruling in Tele2 Sverige and Tom Watson.