Court of Justice of the European Union: Judgment on the processing of personal data and the protection of privacy in the electronic communications sector

IRIS 2018-10:1/3

Mariana Francese Coutinho
Institute for Information Law (IViR), University of Amsterdam

On 2 October 2018, the Grand Chamber of the Court of Justice of the European Union (CJEU) delivered a judgment in the Ministerio Fiscal case (C-207/16) concerning the processing of personal data and the protection of privacy in the electronic communications sector. This judgment concerned the interpretation of Article 15(1) of Directive 2002/58/EC (the e-Privacy Directive) - which allows member states to introduce exceptions to the principles of the confidentiality of personal data - read in light of Articles 7 (respect for private life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union (the Charter).

The judgment addressed a request for a preliminary ruling from the Ministerio Fiscal (Spanish Public Prosecutor's Office) against the decision of a local court of preliminary investigation which had refused to grant the police access to personal data retained by providers of electronic communications services. The investigation concerned the theft of a mobile phone, which had prompted the police to request that the investigating magistrate order electronic communications service providers to reveal telephone numbers that had been activated with the International Mobile Equipment Identity (IMEI) code of the stolen mobile, as well as personal data relating to the identity of the owners or users of such numbers. The magistrate had refused on the grounds that Spanish law at that time limited the communication of the data retained by the providers of electronic communications services to serious offences. The Public Prosecutor's Office appealed this decision before the referring court, which requested a preliminary ruling by the CJEU on whether Article 15(1) of the e-Privacy Directive, read in light of Articles 7 and 8 of the Charter, must be interpreted as meaning that public authorities' access to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone entails a sufficiently serious interference with their fundamental rights so as to limit that access to the objective of fighting serious crime and, if so, by which criteria the seriousness of the offence must be assessed.

The case was stayed pending delivery of the Tele2 Sverige and Watson and Others judgment (C-203/15 and C-698/15 - see IRIS 2017-2/3), in which the CJEU held that Article 15 of the e-Privacy Directive could justify national legislation

© European Audiovisual Observatory (Council of Europe) 2026

requiring targeted retention of traffic and location data for the purpose of fighting serious crime, but proceeded once the referring court stated that the Tele2 Sverige and Watson and Others judgment did not enable it to assess with a sufficient degree of certainty the national legislation in light of EU law.

Based on its case law, with special reference being made to the Tele2 Sverige and Watson and Others judgment, the CJEU clarified that the access by public authorities to personal data retained by providers of electronic communications services constitutes an interference with the fundamental rights of Articles 7 and 8 of the Charter, even if the interference is not serious; and that such access must correspond strictly to one of the objectives set out in Article 15(1) of the e-Privacy Directive. While Article 15(1) of the e-Privacy Directive refers to criminal offenses in general and not only serious crimes, the CJEU held that, due to the principle of proportionality, serious interference can be justified only by the objective of fighting crimes that can qualify as serious as well.

However, seemingly in contrast to the judgment on Tele2 Sverige and Watson and Others, the CJEU decided that, when the interference that such access entails is not serious, access can be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences generally. Therefore, since the data requested by the Public Prosecutor's Office would not allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned, access to the data requested cannot be defined as a serious interference with the fundamental rights of such persons - even though it does constitute an interference - and is justifiable by the objective of preventing, investigating, detecting and prosecuting criminal offences generally, without it being necessary that those offences be defined as serious.

Judgment of the Grand Chamber of the Court of Justice of the European Union in Case C-207/16 Ministerio Fiscal, 2 October 2018

http://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1118868

© European Audiovisual Observatory (Council of Europe) 2026

© European Audiovisual Observatory (Council of Europe) 2026