Court of Justice of the European Union
PRESS RELEASE No 59/18
Luxembourg, 3 May 2018

Press and Information

Advocate General's Opinion in Case C-207/16
Ministerio Fiscal

Advocate General Saugmandsgaard Øe proposes that the Court should find that even criminal offences that are not particularly serious may justify disclosure of basic electronic communications metadata provided such disclosure does not seriously undermine the right to privacy

In an investigation concerning the robbery of a wallet and a mobile telephone, the Spanish police asked the examining magistrate to grant it access to identification data of users of telephone numbers activated from the stolen telephone for a period of 12 days from the date of the theft. The examining magistrate refused that request on the ground, inter alia, that the facts on which the criminal investigation was based did not constitute a 'serious' offence — that is, under Spanish law, an offence punishable by a term of imprisonment of more than five years – disclosure of identification data being possible in Spain only for that type of offence. The Ministerio Fiscal (Spanish Public Prosecutor's Office) appealed against that decision before the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain).

The Directive on privacy and electronic communications[1] provides that Member States may restrict citizens' rights where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security and the prevention, investigation detection and prosecution of criminal offences or of unauthorised use of the electronic communications system.

In its judgments in Digital Rights[2] and Tele2 Sverige,[3] the Court of Justice used the concept of 'serious offences' to assess the lawfulness and proportionality of interference with the right to respect for private and family life and the right to protection of personal data, both those rights being enshrined in the Charter of Fundamental Rights of the European Union.

The Audiencia Provincial de Tarragona indicates that, after the adoption of the decision of the examining magistrate, the Spanish legislature introduced two alternative criteria for determining the degree of seriousness of an offence in respect of which the retention and disclosure of personal data are permitted. The first is a substantive criterion, relating to terrorism and offences committed

[1] 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 (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).

[2] Case: C-293/12 and C-594/12 Digital Rights Ireland and Others, see Press Release No 54/14. In that judgment, the Court declared invalid Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

[3] Case: C-203/15 and C-698/15 Tele2 Sverige and Watson and Others see Press Release No 145/16. In that judgment, the Court held that EU law precludes, first, 'national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication' and, second, 'national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the EU'.

in the context of organised crime. The second is a formal normative criterion which lays down a minimum threshold of three years' imprisonment. The Spanish court observes that that threshold may encompass the vast majority of criminal categories. The Audiencia Pronvincial de Tarragona has therefore referred questions to the Court concerning the setting of the seriousness threshold for offences beyond which an infringement of fundamental rights may be justified, in the light of the judgments cited above, when the competent national authorities seek access to personal data retained by electronic communications service providers.

In today's Opinion, Advocate General Henrik Saugmandsgaard Øe states, first of all, that a measure such as that requested by the police in the present case constitutes an interference with the right to respect for private and family life and with the right to protection of personal data. Nevertheless, the Advocate General considers that, **in the judgments in Digital Rights and Tele2, the Court established a link between the seriousness of the interference and the seriousness of the reason justifying the interference**. Thus, to require, at the stage of providing justification for such interference, that there should be a 'serious offence' that will justify derogating from the principle that electronic communications are confidential, means that **the interference itself must be serious**. **According to the Advocate General, that essential element is lacking in the present case**.

The Advocate General adds that the nature of the interference in the present case is distinct from that considered by the Court in the two judgments cited above. **It relates to a targeted measure** intended to allow access, by the competent authorities and for the purposes of a criminal investigation, to data held for commercial purposes by service providers which relate solely to the identity (surname, forename and possibly address) of a restricted category of subscribers or users of a specific means of communication, namely those whose telephone number was activated from the mobile telephone the theft of which is being investigated, **for a limited period**, that is, approximately **12 days. The Advocate General is of the view that the potentially harmful effects for the persons concerned by the request for access in question are both slight and limited**, given that the data sought are not intended to be disclosed to the public at large and the right of access enjoyed by the police authorities is accompanied by procedural safeguards as it is subject to review by a court. **As a consequence, the interference entailed by the communication of such civil identity data is not particularly serious**, as, in those particular circumstances, such data do not have a direct or great effect on the privacy of the persons concerned.

The Advocate General states that, according to the Directive, a derogation from the principle that electronic communications are confidential may be justified by the general-interest objective of preventing and prosecuting *criminal offences*, but no further details are provided as to the nature of those offences. It is not therefore essential that the offences justifying the restrictive measure in question may be classified as 'serious' within the meaning of the judgments in Digital Rights and Tele2. According to the Advocate General, **it is only where the interference suffered is particularly serious that the offences capable of justifying such interference must themselves be particularly serious. On the other hand, where the interference is not serious (that is, when the data the disclosure of which is sought do not entail a serious infringement of privacy), even criminal offences which are not particularly serious may justify such interference (that is, disclosure of the data requested)**.

In particular, the Advocate General considers that EU law does not preclude the competent authorities having access to identification data held by electronic communications service providers where such data make it possible to find the presumed perpetrators of a criminal offence that is not of a serious nature. The Advocate General concludes that, in the light of the Directive, the measure requested by the police in the present case entails interference with fundamental rights guaranteed by the Directive and the Charter which does not attain a sufficient level of seriousness for such access to be confined to cases in which the offence concerned is serious.

NOTE: The Advocate General's Opinion is not binding on the Court of Justice. It is the role of the Advocates General to propose to the Court, in complete independence, a legal solution to the cases for which they are

responsible. The Judges of the Court are now beginning their deliberations in this case. Judgment will be given at a later date.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Press contact: Holly Gallagher ☎ (+352) 4303 3355