



Press and Information

Court of Justice of the European Union

PRESS RELEASE No 141/18

Luxembourg, 2 October 2018

Judgment in Case C-207/16
Ministerio Fiscal

Criminal offences that are not particularly serious may justify access to personal data retained by providers of electronic communications services provided that that access does not constitute a serious infringement of privacy

In the context of an investigation into the robbery of a wallet and mobile telephone, Spanish police requested the investigating magistrate in charge of the case to grant them access to data identifying the users of telephone numbers activated with the stolen telephone during a period of 12 days as from the date of the robbery. The investigating magistrate rejected the request on the ground, *inter alia*, that the acts giving rise to the criminal investigation did not constitute a ‘serious’ offence — that is, an offence punishable under Spanish law by a term of imprisonment of more than five years —, access to identification data being possible only in respect of that category of offences. 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 communications¹ provides that Member States may restrict citizens’ rights when such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society in order to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.

The Audiencia Provincial de Tarragona states that, following the adoption of the investigating magistrate’s decision, the Spanish legislature introduced two alternative criteria for determining the degree of seriousness of an offence in respect of which the retention and communication of personal data are permitted. The first is a substantive criterion, relating to specific and serious criminal offences that are particularly harmful to individual and collective legal interests. The second is a formal normative criterion setting a threshold of three years’ imprisonment which covers the great majority of offences. In addition, the Spanish court takes the view that the State’s interest in repressing criminal conduct cannot justify disproportionate interferences with the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (‘the Charter’). The Audiencia Provincial de Tarragona therefore seeks guidance from the Court of Justice on fixing the threshold of seriousness of offences above which an interference with fundamental rights, such as competent national authorities’ access to personal data retained by providers of electronic communications services, may be justified.

In today’s judgment, the Court recalls that national authorities’ access, in connection with a criminal investigation, to personal data retained by providers of electronic communications services comes within the scope of the directive. In addition, access to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as their surnames, forenames and, if need be, addresses, constitutes an interference with their

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).

fundamental rights enshrined in the Charter. Nevertheless, the Court rules that that interference is not sufficiently serious to entail access being restricted, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.

The Court indicates that national authorities' access to personal data retained by providers of electronic communications services constitutes an interference with the fundamental rights of respect for private life and protection of data enshrined in the Charter, even in the absence of circumstances which would allow that interference to be defined as 'serious', without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way. However, the directive lists objectives capable of justifying national legislation governing public authorities' access to such data and thereby derogating from the principle of confidentiality of electronic communications. The list of objectives is exhaustive, as a result of which that access must correspond, genuinely and strictly, to one of those objectives. The Court observes in that regard that, **as regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the wording of the directive does not limit that objective to the fight against serious crime alone, but refers to 'criminal offences' generally.**

In its judgment in *Tele2 Sverige*², the Court ruled that only the objective of fighting serious crime is capable of justifying public authorities' access to personal data retained by providers of electronic communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned. That interpretation was, however, based on the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails. In accordance with the principle of proportionality, serious interference can be justified in that field only by the objective of fighting crime which must also be defined as 'serious'. **By contrast, when the interference is not serious, that access may be justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally.**

The Court takes the view that **access to only the data referred to in the request at issue in the main proceedings cannot be defined as 'serious' interference with the fundamental rights of the persons whose data is concerned, as those data do not allow precise conclusions to be drawn in respect of their private lives.** The Court concludes that **the interference that access to such data entails may therefore be justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious'.**

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 EU 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.

Unofficial document for media use, not binding on the Court of Justice.

The [full text](#) of the judgment is published on the CURIA website on the day of delivery.

Press contact: ☎ (+352) 4303 3355

Pictures of the delivery of the Judgment are available from "[Europe by Satellite](#)" ☎ (+32) 2 2964106

² Case: [C-203/15 and C-698/15](#), *Tele2 Sverige and Watson and Others*, see Press Release No. [145/16](#).