Court of Justice of the European Union
PRESS RELEASE No 58/22
Luxembourg, 5 April 2022

Press and Information

Judgment in Case C-140/20
Commissioner of An Garda Síochána and others

The Court confirms that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime

The national court may not impose a temporal limitation on the effects of a declaration of invalidity of a national law that provides for such retention

In March 2015, in Ireland, G.D. was sentenced to life imprisonment for the murder of a woman. In the appeal against his conviction, before the Court of Appeal in Ireland, G.D. criticised the first-instance court in particular for having incorrectly admitted as evidence traffic and location data relating to telephone calls. In order to be able to contest, as part of the criminal proceedings, the admissibility of that evidence, G.D. brought civil proceedings before the High Court (Ireland) contesting the validity of some of the provisions of an Irish law of 2011 ('the 2011 Act') which governed the retention of and access to that data, on the ground that that act infringed rights conferred on him by EU law. By decision of 6 December 2018, the High Court upheld G.D.'s submission. Ireland appealed against that decision to the Supreme Court (Ireland), which is the referring court in this case.

By its reference, the Supreme Court seeks clarification as to the requirements under EU law in respect of the retention of those data for the purposes of combating serious crime and as to the necessary safeguards in respect of access to those data. It has doubts, in addition, as to the scope and temporal effect of a possible declaration of invalidity that it may be obliged to make, since the 2011 Act was adopted in order to transpose Directive 2006/24/EC, [1] which was declared invalid by the Court in the judgment of 8 April 2014, *Digital Rights Ireland and Others*. [2]

In its judgment, the Court, sitting as the Grand Chamber, confirms, in the first place, its settled case-law [3] which holds that EU law [4] **precludes national legislative measures which provide, as a preventative measure, for the general and indiscriminate retention of traffic and location data relating to electronic communications, for the purposes of combating serious crime**.

The privacy and electronic communications directive does not merely create a framework for access to such data through safeguards to prevent abuse, but enshrines, in particular, **the principle of the prohibition of the storage** of traffic and location data**.** The retention of traffic and

[1] 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).
[2] Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12, (see, the Press Release No. 54/14).
[3] Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12; judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15 (see the Press Release Noº 145/16); Judgments of 6 October 2020*, Privacy International*, C-623/17, and La Quadrature du Net and Others, C-511/18, C-512/18 *Ordre des barreaux francophones et germanophone and others*, C-520/18 (see the Press Release No 123/20); and judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18 (see the Press Release No 29/21).
[4] 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) ('the privacy and electronic communications directive'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union.

location data thus constitutes, in itself, first, a derogation from the prohibition of the storage of those data, and, second, an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter.

While the privacy and electronic communications directive allows Member States to place limitations on the exercise of those rights and obligations for the purposes inter alia of combating crime, those limitations must comply with the principle of proportionality. That principle requires compliance not only with the requirements of aptitude and of necessity but also with that of **the proportionate nature** of those measures in relation to the objective pursued. Thus, the Court has already held that the objective of combating serious crime, as fundamental it may be, does not, in itself, justify that a measure providing for the general and indiscriminate retention of all traffic and location data, such as that established by Directive 2006/24, should be considered to be necessary. In the same vein, even the positive obligations of the Member States relating to the establishment of rules to facilitate effective action to combat criminal offences cannot have the effect of justifying interference that is as serious as that entailed by legislation providing for the retention of traffic and location data with the fundamental rights of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued.

The Court also recalls that public authorities have various positive obligations pursuant to the Charter, consisting for example of the adoption of legal provisions to protect private and family life, home and communications, and also the protection of the individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment. It is necessary therefore for them to **strike a balance between the various interests and rights in question**. An objective of general interest may not be pursued without, first, having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by **properly balancing** the objective of general interest against the rights at issue, and, second, verifying that the importance of the public interest objective is proportionate to that seriousness of the interference which that measure entails.

Those considerations lead the Court to reject inter alia the submission that particularly serious crime could be treated in the same way as a threat to national security which is genuine and current or foreseeable and could, for a limited period of time, justify a measure for the general and indiscriminate retention of traffic and location data. Such a threat is distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed.

However, the Court held, in the second place, and confirming its earlier case-law, that EU law does not preclude legislative measures that provide, subject to the conditions set out in its judgment, for the purposes of combating serious crime and preventing serious threats to public security, for:

- **the targeted retention of traffic and location data which is limited,** according to the categories of persons concerned or using a geographical criterion;

- **the general and indiscriminate retention of IP addresses assigned to the source of an internet connection**;

- **the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;** and

- the expedited **retention** (*quick freeze*) of traffic and location data in the possession of those service providers.

The Court provides various precisions regarding those different categories of measure.

First of all, the competent national authorities may adopt a targeted measure of retention using a geographic criterion, such as, inter alia, the average crime rate in a particular geographical area,

without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. It adds that such a retention measure covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect information as to the presence, in those places or geographic areas, of all persons using means of electronic communication in one of those places and to draw conclusions as to their presence and activity in those places or geographic areas for the purposes of combating serious crime.

Next, the Court indicates that neither the privacy and electronic communications directive nor any other measure of EU law precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities.

Finally, the Court observes that the privacy and electronic communications directive does not preclude the competent national authorities from ordering a measure of expedited retention at the first stage of an investigation into a serious threat for public security or a possible serious crime, namely from the time when the authorities may, in accordance with the provisions of national law, commence such an investigation. Such a measure may be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle.

Those various measures may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently.

The Court rejects again the argument that the competent national authorities should be able to access, for the purposes of combating serious crime, traffic and location data which have been retained in a general and indiscriminate way, in accordance with its case-law, in order to address a serious threat to national security which is genuine and current or foreseeable. That argument makes that access depend on factors that are unrelated to the objective of combating serious crime. In addition, under that line of argument, access could be justified by an objective of lesser importance than that which justified its retention, namely safeguarding national security, which would be contrary to that hierarchy of public interest objectives in the context of which the proportionality of a retention measure must be assessed. Furthermore, to authorise such access would deprive of any effectiveness the prohibition on carrying out general and indiscriminate retention for the purpose of combating serious crime.

In the third place, the Court confirms that EU law precludes national legislation pursuant to which the centralised processing of requests for access to data retained by the providers of electronic communications, issued by the police in the context of the investigation and prosecution of serious criminal offences, is the responsibility of a police officer, even where that officer is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and that officer's decisions may subsequently be subject to judicial review. The Court confirms in that regard its case law according to which, in order to ensure, in practice, full compliance with the strict conditions of access to personal data such as traffic and location data, access by the competent national authorities to retained data must be subject to a prior review carried out either by a court or by an independent administrative body and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. However, a police officer does not constitute a court and does not have all the guarantees of independence and impartiality required in order to be able to qualify as an independent administrative body.

In the fourth place and finally, the Court confirms its case-law that EU law precludes a national court from limiting the temporal effects of a declaration of invalidity it is required, as a matter of national law, to make in relation to national legislation requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data, owing to the incompatibility of that legislation with the Directive on privacy and electronic communications.

In those circumstances, the Court recalls that the admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

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: Jacques René Zammit ☎ (+352) 4303 3355