Telecommunications

Limits to the obligation of telecommunications operators to retain traffic and location data for the purpose of combatting unlawful acts

Telecommunications operators are not required to retain traffic and location data for disciplinary actions against corruption.

ANA I. MENDOZA LOSANA
Associate Professor of Civil Law, University of Castilla-La Mancha
Academic Counsel, Gómez-Acebo & Pombo

The judgment of 7 September 2023 in Case C-162/22, *Lietuvos Respublikos generalinė prokuratūra* (ECLI:EN:EUC:2023:631), joins the long list of Court of Justice of the European Union (CJEU) rulings on the scope of the obligation of telecommunications operators to retain traffic and location data, an obligation that derives from Article 15(1) of 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 ('Directive 2002/58'). The said provision enables States to adopt legislative measures restricting fundamental rights such as the right to the protection of personal data and of the secrecy of communications and requires telecommunications operators to retain data generated by electronic communications for the pursuit of the public interest objectives listed in the Directive, including the prosecution of serious criminal offences.

1. Facts

In the proceedings giving rise to the question referred for a preliminary ruling, an application was made for the quashing of two decisions

of the Lithuanian Prosecutor General's Office sanctioning and suspending a prosecutor from duty for having unlawfully provided information to a suspect and his lawyer in the course of an investigation. The misconduct leading to the disciplinary sanction was established on the basis of data retained by electronic communications service providers; it was also noted that court orders had authorised the interception and recording of information transmitted over electronic communications networks concerning the lawyer in question and the appellant in the main proceedings. However, once these data are obtained, they are used for an administrative procedure other than the criminal proceedings in the context of which the interception of communications and the related retention and transfer of data were ordered.

2. Question referred: access to and use of traffic and location data in non-criminal proceedings

In this case, it was questioned whether data retained and made available by operators in order to prosecute criminal offences could also be used in disciplinary proceedings investigating misconduct in office. Among others, Article 19(1)(5) of the Lithuanian Criminal Intelligence Act, according to which information from criminal investigation operations relating to an event that has the characteristics of a corruption-related infringement may be declassified, subject to the agreement of the Public Prosecutor's Office, and used in the context of an investigation into disciplinary infringement or misconduct in office, is referred to the CJEU for consideration.

In the main proceedings, the appellant (the suspended prosecutor) distinguished between two elements: (a) access to data retained by providers of electronic communications services for purposes other than combatting serious crime and preventing serious threats to public security; (b) once such access had been obtained, the use of those data in investigating corruption-related misconduct in office. According to the appellant, the use of data allowing the identification of the source and destination of a telephone communication from the landline or mobile phone of a person under investigation in proceedings relating to misconduct in office (not in criminal cases, nor directly related to the commission of serious criminal offences) would constitute an unjustified interference with fundamental rights contrary to EU law.

The national court, which must rule on the invalidity of the contested decisions, questions whether Article 15(1) of Directive 2002/58, read in conjunction with Articles 7 (respect for privacy of communications), 8 (protection of personal data), 11 (freedom of expression) and 52(1) (limitations on the exercise of the rights and freedoms subject to the principle of proportionality) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding the use, in connection with investigations into corruption-related misconduct in office, of personal data relating to electronic communications which have been retained, pursuant to a legislative measure adopted under that provision, by providers of electronic communications services and which have subsequently been made available, pursuant to that measure, to the competent authorities for the purpose of combating serious crime.

Note the difference in nuance: it is not the access to the data that is being questioned (which in this case was for the purpose of prosecuting serious criminal offences in the framework of a criminal investigation and with the corresponding authorisation), but the use given

to such data (they have been used to punish corruption-related misconduct in office).

3. Some preliminary considerations on operators' duty to retain (indiscriminately) traffic and location data

Although it is not the subject of the judgment in question, given the numerous doubts that are being raised, in case law and scholarly writings, by the obligation imposed on electronic communications operators to retain traffic and location data for a certain period of time, it is considered necessary to recall here the legal situation in which this issue finds itself. Following the quashing by the CJEU of 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, numerous European laws have been challenged, such as of Spain (Electronic Communications and Public Communications Networks Data Retention Act 25/2007 of 18 October) impose a duty on electronic communications operators to retain traffic data (source and destination of the communication, type of terminal used, identity of the users involved in the communication and IP addresses) and the location data of all electronic communications made by all users of electronic communications services for a specific period of time (in Spain, one year). This type of obligation could, in principle, be characterised as general and indiscriminate retention only limited in time and constituting an unlawful processing of personal data that is not justified by reasons of public interest.

In order not to make this paper too long, not all CJEU case law that has made a pronouncement on this obligation and its limits is reproduced here. The judgement under discussion contains in its considerations a brief summary of the numerous rulings that add new nuances to the duty to retain and which, in principle, seem to exclude indiscriminate retention (see, for example, CJEU judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 110; of 2 March 2021, *Prokuratuur, Conditions of access to data relating to electronic communications*, C-746/18, EU:C:2021:152, paragraphs 33 and 35; and of 20 September 2022, *SpaceNet and Telekom Deutschland*, C-793/19 and C-794/19, EU:C:2022:702, paragraphs 74 and 131 and case law cited). In any event and in so far as it constitutes an interference with fundamental rights, the duty to retain must be subject to a strict regime of safeguards, must be interpreted restrictively and constitutes an exception which must be justified on grounds of public interest and in accordance with the principle of proportionality (see CJEU judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 40).

In Spain, the issue seems to have been, for now, settled by the Supreme Court (Criminal Division, First Chamber) judgment no. 824/2022 of 19 October. In this ruling, the Supreme Court declines to refer for a preliminary ruling, as requested by the appellant, covers the vast existing case law on the duty to retain, from the CJEU, the European Court of Human Rights and the Supreme Court itself, and concludes that the obligation to retain, generally and indiscriminately, traffic and location data for one year under the terms and with the safeguards laid down in Spanish law does not constitute an unjustified attack on the fundamental rights recognised by EU law. According to the Supreme Court, it is an instrumental and

essential obligation so that, when the time comes and with the due safeguards, including the essential judicial authorisation, access by the competent authorities to the data retained can be facilitated in order to satisfy the public interest objectives mentioned in an exhaustive manner in Directive 2002/58/EC.

4. Legal doctrine: proceedings against non-serious criminal offences or disciplinary infringements does not justify interference with fundamental rights

In this new judgment of 7 September 2023, the CJEU completes its doctrine on the duty to retain traffic and location data in the context of the provision of electronic communications services. In it, the CJEU states that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with fundamental rights, such as that entailed by the retention of traffic and location data. Telecommunications operators are only required to retain and transfer traffic and location data to the competent authorities for the purpose of combatting serious crime.

The following rules can be drawn from the judgment and the case law cited therein:

a) In the hierarchy of public interest objectives listed in Article 15(1) of Directive 2002/58/EC, in accordance with the principle of proportionality, the importance of the objective of safeguarding national security (the exclusive responsibility of each Member State) outweighs that of the other objectives, in particular the objectives of combating crime in general, including serious crime, and preventing non-serious threats to public security (CJEU judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EUC:2022:258, paragraph 99).

b) Correlatively, the objective of safeguarding national security may justify measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (CJEU judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 57 and the case law cited).

c) The objective of preventing, investigating, detecting and prosecuting criminal offences in general may justify non-serious interferences with fundamental rights (CJEU judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 59 and case law cited).

d) Access to and use of traffic and location data retained by providers pursuant to a measure adopted under Article 15(1) of Directive 2002/58 may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective pursued by access is greater than that of the objective which justified retention (CJEU judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 98 and the case law cited).

e) The same view taken in the previous paragraph has to be applied for other possible uses of the retained data: after having been retained and made available to the competent authorities for the

purpose of combatting serious crime, such data may not be transferred to other authorities or used for other purposes, including combatting corruption-related misconduct in office. This other purpose is of lesser importance in the hierarchy of public interest objectives than combatting serious crime and preventing serious threats to public security. In such a case, access to the retained data would be contrary to the hierarchy of public interest objectives referred to in the previous paragraphs (see, in this sense, the CJEU judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 99 and paragraph 41 of the judgment under consideration).

f) Disciplinary proceedings concerning corruption-related misconduct in office could be related to the protection of public security, although this would require the person concerned to prove the existence of a serious threat to public security (see paragraph 42 of the judgment under consideration). However, in the light of Article 15(1) of the Directive, the restriction of fundamental rights resulting from the retention of traffic and location data is only justified in the context of criminal proceedings and not in the context of disciplinary proceedings, however important the role played by these proceedings in combatting serious crime may be (see paragraph 43 of the judgment under consideration).

5. Conclusion

The Court of Justice of the European Union concludes that traffic and location data retained by providers in application of a measure taken pursuant to Article 15(1) of Directive 2002/58/EC for the purpose of combating serious crime cannot be subsequently transferred to other authorities or used in combatting corruption-related misconduct in office, which is of lesser importance than combatting serious crime. In other words, the directive precludes data collected for the purpose of combating serious crime from being used in administrative investigations related to corruption in the public sector.