



Press and Information

Court of Justice of the European Union

PRESS RELEASE No 29/21

Luxembourg, 2 March 2021

Judgment in Case C-746/18

H. K. v Prokuratuur

Access, for purposes in the criminal field, to a set of traffic or location data in respect of electronic communications, allowing precise conclusions to be drawn concerning a person's private life, is permitted only in order to combat serious crime or prevent serious threats to public security

In addition, EU law precludes national legislation that confers upon the public prosecutor's office the power to authorise access of a public authority to such data for the purpose of conducting a criminal investigation

Criminal proceedings were brought in Estonia against H. K. on counts of theft, use of another person's bank card and violence against persons party to court proceedings. A court of first instance convicted H. K. of those offences and imposed a custodial sentence of two years. That judgment was then upheld on appeal.

The reports relied upon in order to find H. K. guilty of those offences were drawn up, inter alia, on the basis of personal data generated in the context of the provision of electronic communications services. The Riigikohus (Supreme Court, Estonia), before which H. K. lodged an appeal on a point of law, expressed doubts as to whether the conditions under which the investigating authority had access to those data were compatible with EU law.¹

Those doubts concerned, first, whether the length of the period in respect of which the investigating authority has had access to the data is a criterion for assessing the seriousness of the interference, constituted by that access, with the fundamental rights of the persons concerned. Thus, the referring court raised the question whether, where that period is very short or the quantity of data gathered is very limited, the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference. Second, the referring court had doubts as to whether it is possible to regard the Estonian public prosecutor's office, in the light of the various duties which are assigned to it by national legislation, as an 'independent' administrative authority, within the meaning of the judgment in *Tele2 Sverige and Watson and Others*,² that is capable of authorising access of the investigating authority to the data concerned.

By its judgment, delivered by the Grand Chamber, the Court holds that the directive on privacy and electronic communications, read in the light of the Charter, precludes national legislation that permits public authorities to have access to traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public

¹ To be more precise, with 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) (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 directive on privacy and electronic communications'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

² Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, [C-203/15](#) and [C-698/15](#) paragraph 120; see also Press Release No [145/16](#).

security. According to the Court, the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period are irrelevant in that regard. The Court further holds that that directive, read in the light of the Charter, precludes national legislation that confers upon the public prosecutor's office the power to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation.

Findings of the Court

As regards the circumstances in which access to traffic and location data retained by providers of electronic communications services may, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, be granted to public authorities, pursuant to a measure adopted under the directive on privacy and electronic communications,³ the Court recalls the content of its ruling in *La Quadrature du Net and Others*.⁴ Thus, that directive authorises the Member States to adopt, for those purposes amongst others, legislative measures to restrict the scope of the rights and obligations provided for by the directive, inter alia the obligation to ensure the confidentiality of communications and traffic data,⁵ only if the general principles of EU law – which include the principle of proportionality – and the fundamental rights guaranteed by the Charter⁶ are observed. Within that framework, the directive precludes legislative measures which impose on providers of electronic communications services, as a preventive measure, an obligation requiring the general and indiscriminate retention of traffic and location data.

So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue, in accordance with the principle of proportionality the Court holds that only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to allow precise conclusions to be drawn concerning the private lives of the persons concerned, and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access.

As regards the power conferred upon the public prosecutor's office to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation, the Court points out that it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in their possession. However, in order to satisfy the requirement of proportionality, such legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and must indicate in what circumstances and under which substantive and procedural conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.

According to the Court, in order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data 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. In cases of duly justified urgency, the review must take place within a short time.

³ Article 15(1) of the directive on privacy and electronic communications.

⁴ Judgment of 6 October 2020, *La Quadrature du Net and Others*, [C-511/18](#), [C-512/18](#) and [C-520/18](#), paragraphs 166 to 169; see also Press Release No [123/20](#).

⁵ Article 5(1) of the directive on privacy and electronic communications.

⁶ In particular, Articles 7, 8 and 11 and Article 52(1) of the Charter.

In that regard, the Court states that one of the requirements for the prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access. Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence.

According to the Court, it follows that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings. That is not so in the case of a public prosecutor's office which, like the Estonian public prosecutor's office, directs the investigation procedure and, where appropriate, brings the public prosecution. It follows that the public prosecutor's office is not in a position to carry out the prior review.

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.

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: Jacques René Zammit ☎ (+352) 4303 3355

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