Court of Justice of the European Union
PRESS RELEASE No 123/20
Luxembourg, 6 October 2020

Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others

Press and Information

The Court of Justice confirms that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security

However, in situations where a Member State is facing a serious threat to national security that proves to be genuine and present or foreseeable, that Member State may derogate from the obligation to ensure the confidentiality of data relating to electronic communications by requiring, by way of legislative measures, the general and indiscriminate retention of that data for a period that is limited in time to what is strictly necessary, but which may be extended if the threat persists. As regards combating serious crime and preventing serious threats to public security, a Member State may also provide for the targeted retention of that data as well as its expedited retention. Such an interference with fundamental rights must be accompanied by effective safeguards and be reviewed by a court or by an independent administrative authority. Likewise, it is open to a Member State to carry out a general and indiscriminate retention of IP addresses assigned to the source of a communication where the retention period is limited to what is strictly necessary, or even to carry out a general and indiscriminate retention of data relating to the civil identity of users of means of electronic communication, and in the latter case the retention is not subject to a specific time limit

***

In recent years, the Court of Justice has ruled, in several judgments, on the retention of and access to personal data in the field of electronic communications. [1] The resulting case-law, in particular the judgment in *Tele2 Sverige* and *Watson and Others*, in which the Court held, inter alia, that Member States could not require providers of electronic communications services to retain traffic data and location data in a general and indiscriminate way, has caused concerns on the part of certain States that they may have been deprived of an instrument which they consider necessary to safeguard national security and to combat crime.

[1] Thus, in the judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12) (see Press Release No 54/14), the Court declared 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), invalid on the ground that the interference with the rights to respect for private life and to the protection of personal data, recognised by the Charter of Fundamental Rights of the European Union ('the Charter'), which resulted from the general obligation to retain traffic data and location data laid down by that directive was not limited to what was strictly necessary. In the judgment of 21 December 2016, *Tele2 Sverige* and *Watson and Others* (C-203/15 and C-698/15) (see Press Release No 145/16), the Court then interpreted 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'). That article empowers the Member States – on grounds of the protection, inter alia, of national security – to adopt 'legislative measures' intended to restrict the scope of certain rights and obligations provided for in the directive. Lastly, in the judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16) (see Press Release No141/18), the Court interpreted Article 15(1) of that directive in a case which concerned public authorities' access to data relating to the civil identity of users of means of electronic communication.

It is against that background that proceedings were brought before the Investigatory Powers Tribunal (United Kingdom) (*Privacy International*, C-623/17), the Conseil d'État (Council of State, France) (*La Quadrature du Net and Others*, Joined Cases C-511/18 and C-512/18) and the Cour constitutionnelle (Constitutional Court, Belgium) (*Ordre des barreaux francophones et germanophone and Others*, C-520/18) concerning the lawfulness of legislation adopted by certain Member States in those fields, laying down in particular an obligation for providers of electronic communications services to forward users' traffic data and location data to a public authority or to retain such data in a general or indiscriminate way.

By two Grand Chamber judgments delivered on 6 October 2020, the Court rules, first of all, that the directive on privacy and electronic communications is applicable to national legislation requiring providers of electronic communications services to carry out personal data processing operations, such as its transmission to public authorities or its retention, for the purposes of safeguarding national security and combating crime. In addition, while confirming its case-law stemming from the judgment in *Tele2 Sverige* and *Watson and Others*, concerning the disproportionate nature of general and indiscriminate retention of traffic data and location data, the Court **provides clarifications**, inter alia, as to **the scope of the powers** conferred on the Member States by that directive in the field of the retention of such data for the purposes mentioned above.

First of all, the Court takes care to allay the doubts as to the applicability of the directive on privacy and electronic communications raised in the present cases. Several Member States that submitted written observations to the Court expressed diverging opinions in that regard. They contended, inter alia, that the directive does not apply to the national legislation at issue, as the purpose of that legislation is to safeguard national security, which is the sole responsibility of the Member States, as attested to by, in particular, the third sentence of Article 4(2) TEU. The Court considers, however, that **national legislation requiring providers of electronic communications services to retain traffic data and location data or to forward that data to the national security and intelligence authorities for that purpose falls within the scope of that directive**.

Next, the Court recalls that the directive on privacy and electronic communications [2] does not permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and the related data and to the prohibition on storage of such data to become the rule. This means that the directive **does not authorise the Member States to adopt, inter alia for the purposes of national security, legislative measures intended to restrict the scope of rights and obligations provided for in that directive, in particular the obligation to ensure the confidentiality of communications and traffic data, [3] unless such measures comply with the general principles of EU law, including the principle of proportionality, and the fundamental rights guaranteed by the Charter**. [4]

In that context, the Court holds, first, in the *Privacy International* case, that the directive on privacy and electronic communications, read in the light of the Charter, **precludes national legislation requiring providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security**. Secondly, in Joined Cases *La Quadrature du Net and Others* and in *Ordre des barreaux francophones et germanophone and Others*, the Court finds that the directive **precludes legislative measures requiring providers of electronic communications services to carry out the general and indiscriminate retention of traffic data and location data as a preventive measure**. Those obligations to forward and to retain such data in a general and indiscriminate way constitute **particularly serious interferences with the fundamental rights guaranteed by the Charter**, where there is no link between the conduct of the persons whose data is affected and the objective pursued by the legislation at issue.

---

2 Article 15(1) and (3) of Directive 2002/58.

3 Article 5(1) of Directive 2002/58.

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

Similarly, the Court interprets Article 23(1) of the General Data Protection Regulation, [5] read in the light of the Charter, as precluding national legislation requiring providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services.

By contrast, the Court holds that, **in situations where the Member State concerned is facing a serious threat to national security that proves to be genuine and present or foreseeable**, the directive on privacy and electronic communications, read in the light of the Charter, **does not preclude recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic data and location data**. In that context, the Court specifies that the decision imposing such an order, for a period that is limited in time to what is strictly necessary, must be subject to **effective review either by a court or by an independent administrative body** whose decision is binding, in order to verify that one of those situations exists and that the conditions and safeguards laid down are observed. In those circumstances, that directive also does not preclude the automated analysis of the data, inter alia traffic and location data, of all users of means of electronic communication.

The Court adds that the directive on privacy and electronic communications, read in the light of the Charter, does not preclude legislative measures that allow recourse to the **targeted retention, limited in time to what is strictly necessary, of traffic and location data, which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion**. Likewise, that directive does not preclude legislative measures that provide for the general and indiscriminate retention of IP addresses assigned to the source of a communication, provided that the retention period is **limited to what is strictly necessary**, or measures that provide for such retention of data relating to the civil identity of users of means of electronic communication, the Member States not being required in the latter case to limit the retention period. Moreover, that directive does not preclude a legislative measure that allows recourse to the expedited retention of data available to service providers, where **situations arise in which it becomes necessary to retain that data beyond statutory data retention periods in order to shed light on serious criminal offences or attacks on national security**, where such offences or attacks have already been established or where their existence may reasonably be suspected.

In addition, the Court rules that the directive on privacy and electronic communications, read in the light of the Charter, **does not preclude national legislation which requires providers of electronic communications services to have recourse to real-time collection**, inter alia, **of traffic data and location data**, where that collection is **limited to persons in respect of whom there is a valid reason to suspect that they are involved** in one way or another **in terrorist activities** and is subject to a **prior review carried out either by a court or by an independent administrative body whose decision is binding**, to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In urgent cases, the review must take place promptly.

Lastly, the Court addresses the issue of maintaining the temporal effects of national legislation held to be incompatible with EU law. In that regard, it rules that a national court **may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make in respect of national legislation imposing on providers of electronic communications services an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with the directive on privacy and electronic communications**, read in the light of the Charter.

That being said, in order to give a useful answer to the referring court, the Court of Justice recalls that, **as EU law currently stands, it is for national law alone to determine the rules relating to**

---

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of information and evidence obtained by the retention of data in breach of EU law. However, the Court specifies that the directive on privacy and electronic communications, interpreted in the light of the principle of effectiveness, requires national criminal courts to **disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law**, in the context of such criminal proceedings, where those persons suspected of having committed criminal offences are not in a position to comment effectively on that information and evidence.

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