Case C-512/18

Request for a preliminary ruling

Date lodged:

3 August 2018

Referring court:

Conseil d'État (France)

Date of the decision to refer:

26 July 2018

Applicants:

French Data Network

La Quadrature du Net

Fédération des fournisseurs d'accès à Internet associatifs

Defendants:

Premier ministre

Garde des Sceaux, Ministre de la Justice

…

The Conseil d'État (Council of State, France) acting in its judicial capacity

(Litigation Section, Combined 9th and 10th Chambers)

…

…

Having regard to the following procedure:

By a summary application, a supplementary statement and four further statements, lodged on 1 September and 27 November 2015, 24 May 2016, 25 July 2016, 7 February 2017 and 10 July 2018 at the Judicial Affairs Secretariat of the Conseil

d'État, French Data Network, La Quadrature du Net and the Fédération des fournisseurs d'accès à Internet associatifs request that the Conseil d'État:

(1) annul, as ultra vires, the implicit decision of rejection resulting from the silence maintained by the Premier ministre (Prime Minister) on their application for the repeal of Article R. 10-13 of the Code des postes et des communications électroniques (Postal and Electronic Communications Code) and of Decree No 2011-219 of 25 February 2011;

(2) order the Prime Minister to repeal those provisions;

(3) ...

Those associations submit that the provisions, the repeal of which has been sought, are unlawful because they were adopted to apply legislative provisions which, falling within the scope of EU law, constitute a disproportionate infringement of the right to respect for private and family life, the right to protection of personal data and the freedom of expression, as guaranteed by Articles 7, 8 and 11 of the Charter of Fundamental Rights, and infringe Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 as interpreted by the Court of Justice of the European Union.

By a defence lodged on 10 June 2016, the Garde des sceaux, ministre de la justice (Minister for Justice) contends that the application should be dismissed. He submits that the pleas in law raised are unfounded. **[Or. 2]**

By a defence lodged on 20 June 2018, the Prime Minister contends that the application should be dismissed. He submits that the pleas in law raised are unfounded.

By a statement in intervention lodged on 8 February 2016, Privacy International and the Center for Democracy and Technology claim that the Conseil d'État should grant the form of order sought in the application. They submit that:

– the contested provisions are incompatible with the Charter of Fundamental Rights of the European Union;

– the contested provisions infringe Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

… ;

Having regard to:

– the Charter of Fundamental Rights of the European Union;

– the European Convention for the Protection of Human Rights and Fundamental Freedoms;

– Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000;

– Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002;

– the Postal and Electronic Communications Code;

– Law No 2004-575 of 21 June 2004;

– Law No 2013-1168 of 18 December 2013;

– Decree No 2011-219 of 25 February 2011;

– the judgment of the Court of Justice of the European Union of 21 December 2016, *Tele2 Sverige AB* v *Post-och telestyrelsen* and *Secretary of State for the Home Department* v *Tom Watson and Others* (C-203/15 and C-698/15);

– the Code de justice administrative (Code of Administrative Justice);

…

Whereas:

1. Privacy International and the Center for Democracy and Technology have an interest in the annulment of the contested decision. Their statement in intervention is therefore admissible.

2. French Data Network, la Quadrature du Net and the Fédération des fournisseurs d'accès à internet associatifs requested that the Prime Minister repeal Article R. 10-13 of the Postal and Electronic Communications Code and the décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Decree of 25 February 2011 on the retention and communication of data allowing for the identification of any person who has contributed to the creation of content posted online). Those three associations contest the implicit decision of rejection stemming from the silence maintained by the Prime Minister with regard to their application. **[Or. 3]**

3. When an application for the repeal of an unlawful regulation is brought before it, the competent authority is required to refer that application if — except in the case of formal and procedural defects vitiating it — that regulation has been unlawful from the date of its signature or if the illegality stems from circumstances of law or of fact arising after that date.

<u>The refusal to repeal Article R. 10-13 of the Postal and Electronic Communications Code:</u>

4. Under Article L. 34-1 of the Postal and Electronic Communications Code, in the applicable version thereof: '*I.- This article shall apply to the processing of personal data in connection with the provision of electronic communications services to the public; it shall apply in particular to the networks which support data collection and identification devices./ II.- Electronic communications operators, and in particular those persons whose activity consists in offering access to online public communications services, shall erase or make anonymous any traffic data, subject to the provisions of paragraphs III, IV, V and VI./ Persons providing electronic communications services to the public shall establish, in accordance with the provisions of the previous subparagraph, internal procedures for responding to requests from the competent authorities./ Persons who, as part of a main or ancillary professional activity, offer to the public a connection enabling online communication by means of network access, including free of charge, shall be subject to compliance with the provisions applicable to electronic communications operators under this article./ III.- For the purposes of investigating, establishing and prosecuting criminal offences or a failure to comply with the obligation laid down in Article L. 336-3 of the Code de la propriété intellectuelle (Intellectual Property Code) or for the purposes of preventing attacks on the automated data processing systems provided for and punishable under Articles 323-1 to 323-3-1 of the Code pénal (Criminal Code), and with the sole aim of allowing, where necessary, provision to the judicial authority or the high authority referred to in Article L. 331-12 of the Intellectual Property Code or the Autorité nationale de sécurité des systèmes d'information (National Cybersecurity Agency) referred to in Article L. 2321-1 of the Code de la défense (Defence Code), the procedures to erase or make anonymous certain categories of technical data may be deferred for a maximum period of one year. A decree of the Conseil d'État, issued after obtaining the opinion of the Commission nationale de l'informatique et des libertés (French Data Protection Authority), shall determine, within the limits laid down in paragraph VI, those categories of data and the period of their retention, according to the activity of the operators and the nature of the communications, as well as the arrangements for offsetting, where necessary, the identifiable and specific additional costs of the services provided in this regard, at the request of the State, by the operators*'. Article R. 10-13 of that same code, the repeal of which is sought by the applicants, implements the provisions of paragraph III of Article L. 34-1, cited above, inter alia by listing the data which must be retained by electronic communications operators and fixing the period for their retention at one year.

5. Firstly, contrary to the interveners' submissions, the fact that the retention obligation described in the previous paragraph is of a general nature and not restricted to particular persons or circumstances is not, in itself, contrary to the requirements arising from the provisions of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

6. Secondly, under Article 4 of the Treaty on European Union, the Union '*shall respect their* [i.e. the Member States'] *essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and*

safeguarding national security. In particular, national security remains the sole responsibility of each Member State'. Article 51 of the Charter of Fundamental Rights of the European **[Or. 4]** Union provides that '*1. The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. ... 2. This Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties*'. Article 54 of the Charter reads: '*Nothing in this Charter shall be interpreted as implying any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms recognised in this Charter ...*'.

7. In addition, 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, which was adopted on the basis of Article 95 of the Treaty establishing the European Community, now reproduced in Article 114 of the Treaty on the Functioning of the European Union, stems from the desire to approximate the laws of the Member States in order to allow the internal market to be established and to function. As stated in Article 3(1) of the Directive, the Directive concerns the '*processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community*'. However, as is made clear in Article 1(3) of the Directive, it '*shall not apply to activities which fall outside the scope of the Treaty establishing the European Community ... and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law*'. Furthermore, Article 15 of the Directive provides that '*Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union*'. The Member States are thus authorised, on grounds relating to State security or in order to prevent criminal offences, to derogate — inter alia — from the obligation to ensure the confidentiality of personal data, and the confidentiality of the related traffic data, laid down in Article 5(1) of the Directive.

<u>The general and indiscriminate retention obligation:</u>

8. By its judgment of 21 December 2016, *Tele2 Sverige AB* v *Post-och telestyrelsen* and *Secretary of State for the Home Department* v *Tom Watson and Others* (C-203/15 and C-698/15), the Court of Justice of the European Union ruled that Article 15(1) of that 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, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic **[Or. 5]** and location data of all subscribers and registered users relating to all means of electronic communication'.

9. First, it is established that such preventative and indiscriminate retention allows the judicial authority to access data relating to the communications that an individual has made before being suspected of having committed a criminal offence. The usefulness of such a retention practice is therefore unparalleled with a view to investigating, establishing and prosecuting criminal offences.

10. Second, as the Court of Justice of the European Union observed in its judgment of 21 December 2016, such a retention approach is not such as to affect adversely the 'essence' of the rights enshrined in Articles 7 and 8 of the Charter, since the content of a communication is not disclosed under that approach. In addition, the Court has since noted, in its Opinion 1/15 of 26 July 2017, that those rights 'are not absolute rights' and that an objective of general interest of the European Union is capable of justifying even serious interference with those fundamental rights, having made the point that 'the protection of public security also contributes to the protection of the rights and freedoms of others' and that 'Article 6 of the Charter states that everyone has the right not only to liberty but also to security of the person'.

11. In those circumstances, the question whether the general and indiscriminate retention obligation imposed on providers on the basis of the permissive provisions of Article 15(1) of the Directive of 12 July 2002 is to be regarded, inter alia in the light of the guarantees and checks to which the collection and use of such connection data are then subject, as interference justified by the right to security guaranteed in Article 6 of the Charter of Fundamental Rights of the European Union and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 of the Treaty on European Union, presents an initial difficulty in interpreting European Union law.

<u>The refusal to repeal the provisions of Chapter 1 of the Decree of 25 February 2011:</u>

12. The first subparagraph of paragraph II of Article 6 of the Loi du 21 juin 2004 pour la confiance dans l'économie numérique (Law of 21 June 2004 to promote confidence in the digital economy) provides that persons whose activity consists in offering access to online public communications services and the natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds

or messages of any kind provided by recipients of those services '*shall hold and retain data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide*'. The third subparagraph of paragraph II provides that the judicial authority may require that those persons communicate the data referred to in the first subparagraph. The final subparagraph of paragraph II provides that a decree of the Conseil d'État '*shall define the data referred to in the first subparagraph and specify the duration of and arrangements for their retention*'. The first chapter of the Decree of 25 February 2011 was adopted to that end.

13. Paragraph II of Article 6 of the Law of 21 June 2004, which lays down an obligation to hold and retain only data relating to the creation of content, does not fall within the scope of the Directive of 12 July 2002, which — in accordance with Article 3(1) thereof — is clearly limited '*to the processing of personal data in connection with* **[Or. 6]** *the provision of publicly available electronic communications services in public communications networks in the Community*'.

14. By contrast, the provisions of paragraph II of Article 6 of the Law of 21 June 2004, cited above, do clearly fall within the scope of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, which — under Article 1 thereof — '*seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States*'. Articles 12 and 14 of that directive concern services provided, respectively, by providers of communication services to the public and by service providers as part of hosting arrangements. Article 15(1) of that directive provides that '*Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity*'. Under paragraph 2 of that same article: '*Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements*'. Thus, the Directive does not establish, on its own, a prohibition in principle vis-à-vis the retention of data relating to the creation of content, from which derogation would be possible only by way of exception.

15. The question whether those provisions of the Directive of 8 June 2000 cited above, read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, are to be interpreted as allowing a State to introduce national legislation requiring the persons identified in paragraph 12 to retain the data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that the judicial authority may, where appropriate,

require the communication of those data with a view to ensuring compliance with the rules on civil and criminal liability, presents a second major difficulty in interpreting European Union law.

16. The two questions set out in paragraphs 11 and 15 are crucial to the resolution of the disputes to be decided by the Conseil d'État. As stated above, they present several major difficulties in interpreting European Union law. It is therefore appropriate to bring the matter before the Court of Justice of the European Union pursuant to Article 267 of the Treaty on the Functioning of the European Union and, until that court gives its ruling, to stay judgment on the application made by the applicant associations.

HAS DECIDED AS FOLLOWS:

Article 1: Privacy International and the Center for Democracy and Technology are granted leave to intervene. **[Or. 7]**

Article 2: Judgment is stayed on the application made by French Data Network, la Quadrature du Net and the Fédération des fournisseurs d'accès à Internet associatifs until the Court of Justice of the European Union has given a ruling on the following questions:

1. Is the general and indiscriminate retention obligation imposed on providers on the basis of the permissive provisions of Article 15(1) of the Directive of 12 July 2002 to be regarded, inter alia in the light of the guarantees and checks to which the collection and use of such connection data are then subject, as interference justified by the right to security guaranteed in Article 6 of the Charter of Fundamental Rights of the European Union and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 of the Treaty on European Union?

2. Are the provisions of the Directive of 8 June 2000, read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, to be interpreted as allowing a State to introduce national legislation requiring the persons whose activity consists in offering access to online public communications services and the natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services to retain the data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that the judicial authority may, where appropriate, require the communication of those data with a view to ensuring compliance with the rules on civil and criminal liability?

Article 3: … **[Or. 8]**

…