Case C-511/18

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:

La Quadrature du Net

French Data Network

Fédération des fournisseurs d'accès à Internet associatifs

Igwan.net

Defendants:

Premier ministre

Garde des Sceaux, Ministre de la Justice

Ministre de l'Intérieur

Ministre des Armées

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

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

…

1. By a summary application, a supplementary statement and three further statements, lodged on 30 November 2015, 29 February 2016, 6 May 2016, 13 November 2017 and 10 July 2018 at the Judicial Affairs Secretariat of the

Conseil d'État under No 394922, La Quadrature du Net, French Data Network and the Fédération des fournisseurs d'accès à internet associatifs request that the Conseil d'État:

(1) annul, as ultra vires, décret nº 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Decree No 2015-1185 of 28 September 2015 designating the specialised intelligence services);

(2) in the alternative, refer a number of questions to the Court of Justice of the European Union for a preliminary ruling;

(3) …

They submit:

– … [plea of formal illegality dismissed by the referring court];

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life and the right to an effective remedy guaranteed, respectively, by Articles 8 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and, accordingly, that that decree has no legal basis;

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life, the right to protection of personal data and the right to an effective remedy guaranteed, respectively, in Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and, accordingly, that that decree has no legal basis; **[Or. 2]**

– that Article L. 851-3 of the Code de la sécurité intérieure (Internal Security Code), which constitutes the legal basis of the contested decree, infringes Directive 2000/31/EC of 8 June 2000 and, accordingly, that that decree has no legal basis;

– that the contested decree must be regarded as having no legal basis because Article 323-8 of the Code pénal (Criminal Code) is incompatible with Articles 6 and 32 of the Convention on Cybercrime of 23 November 2001, and with Articles 8 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms as well as with the provisions of Protocol No 1 to that convention, and, accordingly, that that decree has no legal basis.

By two defences, lodged on 26 April and 4 July 2016, the Ministre de la défense (Minister for Defence) contends that the application should be dismissed. He submits that the pleas in law raised are unfounded.

By three defences, lodged on 27 June 2016 and 26 and 28 June 2018, the Premier ministre (Prime Minister) contends that the application should be dismissed. He submits that the pleas in law raised are unfounded.

2. By a summary application, a supplementary statement and three further statements, lodged on 30 November 2015, 29 February 2016, 6 May 2016, 13 November 2017 and 10 July 2018 at the Judicial Affairs Secretariat of the Conseil d'État under No 394925, La Quadrature du Net, French Data Network and the Fédération des fournisseurs d'accès à internet associatifs request that the Conseil d'État:

(1) annul, as ultra vires, décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Decree No 2015-1211 of 1 October 2015 on litigation concerning the implementation of intelligence techniques subject to authorisation and files involving matters of State security);

2) in the alternative, refer a number of questions to the Court of Justice of the European Union for a preliminary ruling;

3) …

They submit:

– …

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life and the right to an effective remedy guaranteed, respectively, by Articles 8 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and, accordingly, that that decree has no legal basis;

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life, the right to protection of personal data and the right to an effective remedy guaranteed, respectively, in Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and, accordingly, that that decree has no legal basis;

– that Article L. 851-3 of the Internal Security Code, which constitutes the legal basis of the contested decree, infringes Directive 2000/31/EC of 8 June 2000 and, accordingly, that that decree has no legal basis. **[Or. 3]**

By a defence lodged on 13 June 2016, the Garde des Sceaux, Ministre de la Justice (Minister for Justice) contends that the application should be dismissed. He submits that the application is inadmissible because the associations fail to establish an interest which gives them standing to institute proceedings, and that, in any event, the pleas in law raised are unfounded.

By three defences, lodged on 27 June 2016 and 26 and 28 June 2018, the Prime Minister contends that the application should be dismissed. He submits that the pleas in law raised are unfounded.

3. By a summary application, a supplementary statement and two further statements, lodged on 11 March 2016, 6 May 2016, 13 November 2017 and 10 July 2018 at the Judicial Affairs Secretariat of the Conseil d'État under No 397844, the association Igwan.net requests that the Conseil d'État:

1) annul, as ultra vires, décret nº 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 (Decree No 2015-1639 of 11 December 2015 on the designation of the services other than the specialised intelligence services which are authorised to use the techniques referred to in Title V of Book VIII of the Internal Security Code, adopted pursuant to Article L. 811-4);

2) in the alternative, to refer a number of questions to the Court of Justice of the European Union for a preliminary ruling;

3) …

It submits:

– …;

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life and the right to an effective remedy guaranteed, respectively, by Articles 8 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and, accordingly, that that decree has no legal basis;

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life, the right to protection of personal data and the right to an effective remedy guaranteed, respectively, in Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and, accordingly, that that decree has no legal basis;

– that Article L. 851-3 of the Internal Security Code, which constitutes the legal basis of the contested decree, infringes Directive 2000/31/EC of 8 June 2000 and, accordingly, that that decree has no legal basis.

By two defences, lodged on 28 June 2016 and 26 June 2018, the Ministre de l'intérieur (Minister for the Interior) contends that the application should be dismissed. He submits that the application is inadmissible because the associations fail to establish an interest which gives them standing to institute proceedings, and that, in any event, the pleas in law raised are unfounded. **[Or. 4]**

By three defences, lodged on 5 July 2016 and on 26 June and 28 June 2018, the Prime Minister contends that the application should be dismissed. He submits that the pleas in law raised are unfounded.

4. By a summary application, a supplementary statement and two further statements, lodged on 11 March 2016, 19 May 2016, 24 November 2017 and 10 July 2018 at the Judicial Affairs Secretariat of the Conseil d'État under No 397844, La Quadrature du Net, French Data Network and the Fédération des fournisseurs d'accès à internet associatifs request that the Conseil d'État:

1) annul, as ultra vires, décret nº 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Decree No 2016-67 of 29 January 2016 on intelligence gathering techniques);

2) in the alternative, refer a number of questions to the Court of Justice of the European Union for a preliminary ruling;

3) …

They submit:

– …;

– that the legislative provisions constituting the legal basis of the contested decree have been found to be contrary to the Constitution by the Conseil constitutionnel (Constitutional Council) and, accordingly, that that decree has no legal basis;

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life and the right to an effective remedy guaranteed, respectively, by Articles 8 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and, accordingly, that that decree has no legal basis;

– that the legislative provisions constituting the legal basis of the contested decree infringe the right to respect for private life, the right to protection of personal data and the right to an effective remedy guaranteed, respectively, in Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and, accordingly, that that decree has no legal basis;

– that Article L. 851-3 of the Internal Security Code, which constitutes the legal basis of the contested decree, infringes Directive 2000/31/EC of 8 June 2000 and, accordingly, that that decree has no legal basis;

– that the contested decree infringes the provisions of Articles L. 851-1 to L. 851-3 of the Internal Security Code, which the decree is inter alia adopted in order to apply, by extending the scope of the connection data which may be collected.

By a defence lodged on 26 June 2018, the Minister for the Interior contends that the application should be dismissed. He submits that the pleas in law raised are unfounded.

By three defences, lodged on 4 July 2016 and on 26 and 28 June 2018, the Prime Minister contends that the application should be dismissed. He submits that the pleas in law raised are unfounded. **[Or. 5]**

Having regard to:

– the Constitution, in particular the Preamble thereto and Articles 61-1 and 62 thereof;

– the Treaty on European Union;

– the Treaty on the Functioning of the European Union;

– the Charter of Fundamental Rights of the European Union;

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

– the Convention on Cybercrime of 23 November 2001;

– 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 Internal Security Code, in particular Book VIII thereof;

– Decision of the Constitutional Council No 2016-590 QPC of 21 October 2016;

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

…;

Whereas:

1. By three applications, La Quadrature du Net, French Data Network and the Fédération des fournisseurs d'accès à internet associatifs seek the annulment, as ultra vires, of the Decree of 28 September 2015 designating the specialised intelligence services (under No 394922), of the Decree of 1 October 2015 on litigation concerning the implementation of intelligence techniques subject to authorisation and files involving matters of State security (under No 394925), and of the Decree of 29 January 2016 on intelligence gathering techniques (under No 397851). Under No 397844, the association Igwan.net seeks annulment of the Decree of 11 December 2015 on the designation of the services other than the specialised intelligence services which are authorised to use the techniques referred to in Title V of Book VIII of the Internal Security Code, adopted pursuant to Article L. 811-4 of the Internal Security Code. Those applications raise the

same questions. It is appropriate that they be joined so that they may be determined in a single decision.

Pleas of formal illegality:

2. … **[Or. 6]** ... [pleas in law dismissed by the referring court] …

Pleas of substantive legality:

Plea in law alleging infringement of Article L. 851-1 of the Internal Security Code by the Decree of 29 January 2016 on intelligence gathering techniques:

3. …. [plea in law rejected by the referring court]

Pleas in law relied on by way of exception:

4. In support of the forms of order sought by them, the applicants raise pleas in law, by way of exception, against all the provisions of Book VIII of the Internal Security Code, those of Chapter IIIa of Title VII of Book VII of the Code of Administrative Justice and those of Article 323-8 of the Criminal Code.

Plea in law alleging that Article L. 811-5 of the Internal Security Code is incompatible with the Constitution:

5. … **[Or. 7]** … [the referring court finds that the declaration that Article L. 811-5 of the Internal Security Code is unconstitutional (made in the Decision of the Constitutional Council of 21 October 2016) has no bearing on the outcome of these proceedings]

Plea in law alleging that Article 323-8 of the Criminal Code is incompatible with law laid down in conventions:

6. … [plea in law rejected by the referring court]

Pleas in law alleging infringement of the European Convention for the Protection of Human Rights and Fundamental Freedoms:

7. Firstly, the applicant associations submit that the contested decrees were adopted on the basis of, or in order to apply, legislative provisions which infringe the right to an effective remedy guaranteed, inter alia, by Article 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms because of the interference with the right to a remedy, the rights of the defence and the adversarial principle within the context of litigation concerning the implementation of intelligence techniques.

8. The provisions of Articles L. 841-1 and L. 841-2 of the Internal Security Code set out the circumstances in which the Conseil d'État has jurisdiction to hear and determine applications concerning the implementation of intelligence techniques subject to authorisation. The matter may be brought before it either by

any person wishing to ascertain that an intelligence technique has not been implemented lawfully and who demonstrates that he has first brought the matter before the Commission nationale de contrôle des techniques de renseignement (National Commission for the Oversight of Intelligence Techniques) on the basis of Article L. 833-4 of the same code, or by the President of that commission, or three of its members, where the Prime Minister does not follow the advice or the recommendations issued by the commission or where the action taken further to that advice or those recommendations is deemed to be inadequate. With regard to the measures for the surveillance of international electronic communications laid down in Chapter IV of Title V of Book VIII of the Internal Security Code, although a person who believes that he is the subject of such a surveillance measure cannot directly bring the matter before a court in order to **[Or. 8]** challenge the legality of that measure, he can, however, on the basis of the provisions of Article L. 854-9 of that code, lodge a complaint to that end with the National Commission for the Oversight of Intelligence Techniques. In addition, that same article provides that, where the commission identifies a case of infringement, on its own initiative or further to such a complaint, it is to submit a recommendation to the Prime Minister with the aim of ending that infringement and ensuring that the intelligence gathered is destroyed, where appropriate. It may also refer the matter to the Conseil d'État.

9. Where claims are brought before it asking it to check that an intelligence technique is not being implemented unlawfully with regard to the applicant or the individual concerned, it falls to the specialist panel created by Article L. 773-2 of the Code of Administrative Justice to ascertain — in the light of the information communicated to it outside the inter partes proceedings — whether or not the applicant is the subject of such a technique. If that is the case, it is for that panel to assess whether that technique is being implemented in a manner consistent with Book VIII of the Internal Security Code. Where it appears that an intelligence technique has not been implemented with regard to the applicant or where the implementation of such a technique is not vitiated by any illegality, the panel hearing the case is to inform the applicant that those checks have been completed and that an unlawful act has not been committed, without providing any further details. In the event that an intelligence technique is implemented in circumstances which appear to be vitiated by illegality, it is to inform the applicant accordingly, without revealing any information protected on national security grounds. In such cases, by a separate decision addressed solely to the competent authority and the National Commission for the Oversight of Intelligence Techniques, the specialist panel is to annul, where appropriate, the relevant authorisation and order that the intelligence gathered unlawfully is destroyed.

10. The derogation from the adversarial nature of the judicial proceedings introduced by the contested provisions of the Code of Administrative Justice — the sole purpose of which is to make the judges aware of material which is protected on national security grounds and cannot therefore be communicated to the applicant — allows the specialist panel, which hears the parties, to give a

ruling in full knowledge of the facts. The powers conferred on it — the power to investigate applications, to establish of its own motion any illegalities which exist and to order the authorities to take all appropriate steps to remedy the illegalities established — guarantee that the judicial review conducted by it is effective.

11. It follows — contrary to the claims made — that neither the circumstances in which a matter may be brought before the specialist panel nor those in which it performs its judicial function infringe the right to an effective remedy enjoyed by the persons who refer matters to it, a right guaranteed inter alia by Article 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

12. Secondly, the applicant associations submit that the contested decrees were adopted on the basis of, or in order to apply, legislative provisions which infringe the right to respect for private life guaranteed, inter alia, by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms on account of the failure to notify the persons concerned of the surveillance measures once those measures have been lifted.

13. In the light, first, of the powers conferred on the National Commission for the Oversight of Intelligence Techniques, an independent administrative authority responsible for ascertaining, under the supervision of the courts, that the intelligence gathering techniques are implemented within the national territory in accordance with the requirements laid down in the Internal **[Or. 9]** Security Code, and, second, of the effective remedy available — subject to the conditions set out in the previous paragraphs — before the specialist panel of the Conseil d'État, the fact that the contested legislative provisions do not provide for the notification to the persons concerned of the surveillance measures to which they have been subject once those measures have been lifted does not, in itself, constitute excessive interference with the right to respect for private life.

14. It follows from the foregoing that the pleas in law alleging that the contested legislative provisions are contrary to Articles 8 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms must, in any event, be dismissed.

<u>Plea in law alleging infringement of the Directive of 8 June 2000:</u>

15. The provisions of Article L. 851-3 of the Internal Security Code allow electronic communications operators and technical service providers to be required to '*implement automated processing on their networks which is intended, depending on the parameters specified in the authorisation, to detect connections which may indicate a terrorist threat*'. The sole purpose of this technique is to gather, for a limited period of time, and from all the connection data processed by those persons, those data which could be linked to such a serious offence. In those circumstances, those provisions, which do not lay down a general obligation to conduct active surveillance, do not infringe the clear provisions of Article 15 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, in accordance with which '*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*'. It follows that, in any event, the plea in law alleging infringement of the Directive of 8 June 2000 must be dismissed.

Pleas in law alleging infringement of the Directive of 12 July 2002 and of the Charter of Fundamental Rights of the European Union:

16. First, 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 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 ...*'.

17. Second, 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 **[Or. 10]** 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.

The scope of Article 15(1) of the Directive of 12 July 2002:

18. It follows from the provisions of the Directive of 12 July 2002, cited above, and as the Court of Justice of the European Union ruled in 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), that the Directive 'must be regarded as regulating the activities of the providers [of electronic communications services]'. Provisions which lay down obligations on those providers, such as the general and indiscriminate retention of the traffic and location data of their users and subscribers, for the purposes stated in Article 15(1) of the Directive of 12 July 2002, which include safeguarding national security, defence and public security, therefore fall within the scope of that directive since, as the Court of Justice has held, they regulate their activity. Furthermore, as the Court has likewise ruled, the fact that such obligations arise solely for the purposes of making the relevant personal data available to the competent national authorities means that national legislation providing for access to and use of such data likewise falls within the scope of the Directive of 12 July 2002. By contrast, national provisions concerning intelligence gathering techniques directly implemented by the State without regulating the activities of the providers of electronic communications services by requiring them to comply with specific obligations are not covered by that directive. **[Or. 11]**

19. Article L. 851-1 of the Internal Security Code provides that: '*Subject to the conditions laid down in Chapter I of Title II of this Book, the collection of information or documents processed or retained by their networks or electronic communications services, including technical data relating to the identification of the subscription or connection numbers to electronic communications services, the mapping of all the subscription and connection numbers of a specified person, the location of the terminal equipment used and the communications of a subscriber, namely the list of numbers called and calling and the duration and date of the communications ..., may be authorised from electronic communications operators and the persons referred to in Article L. 34-1 of the Code des postes et des communications électroniques* (Postal and Electronic

Communications Code) *as well as from the persons referred to in Article 6(I)(1) and (2) of Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* [Law No 2004-575 of 21 June 2004 to promote confidence in the digital economy]'. For different purposes and in accordance with different rules, Articles L. 851-2 and L. 851-4 of the Internal Security Code organise real-time administrative access to the connection data retained as set out above.

20. It is clear from the foregoing, having regard to the scope of Article 15(1) of the Directive of 12 July 2002 as interpreted by the Court of Justice of the European Union, that both the retention obligation introduced by the provisions of Article L. 851-1 of the Internal Security Code, cited above, and the administrative access to connection data, including real-time access, which justifies that obligation, as provided for in Articles L. 851-1, L. 851-2 and L. 851-4 of that code, fall within that scope. The same likewise applies to the provisions of Article L. 851-3 of the Internal Security Code which, although they do not lay down a prior retention obligation on the operators and persons concerned, do however require them to implement automated processing on their networks which is intended to detect connections which may indicate a terrorist threat.

21. However, it is clear from the Directive of 12 July 2002 that the provisions of Articles L. 851-5 and L. 851-6, as well as those of Chapters II, III and IV of Title V of Book VIII of the Internal Security Code, do not fall within the Directive's scope, since they relate to intelligence gathering techniques which are directly implemented by the State without regulating the activities of the providers of electronic communications services by requiring them to comply with specific obligations. Accordingly, those provisions cannot be regarded as implementing EU law and, therefore, the pleas in law alleging infringement of the Directive of 12 July 2002, as interpreted in the light of the Charter of Fundamental Rights of the European Union, cannot be relied on effectively to oppose the provisions.

The general and indiscriminate retention obligation:

22. By its judgment of 21 December 2016, 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 and location data of all subscribers and registered users relating to all means of electronic communication'.

23. First, it is established that such preventative and indiscriminate retention allows the intelligence services to access data relating to the communications that an individual has made before the reasons for believing that he presents a threat to public security, defence or State security are identified. Against a **[Or. 12]** background of serious and persistent threats to national security, and in particular the terrorist threat, the usefulness of such a retention practice is unparalleled as compared with the collection of those same data solely from the point at which the

individual in question has been identified as liable to pose a threat to public security, defence or State security.

24. 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'.

25. 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 — mentioned in paragraphs 7 to 13 — to which the administrative access to connection data and the use of such data are 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 other obligations which may be imposed on the providers of an electronic communications service:</u>

26. The provisions of Article L. 851-2 of the Internal Security Code authorise, for the sole purpose of preventing terrorism, the collection of the information or documents provided for in Article L. 851-1 from the same persons. Such collection, which concerns only one or more individuals previously identified as being potentially linked to a terrorist threat, is conducted in real time. The same applies to the provisions of Article L. 851-4 of the same code, which authorise the real-time transmission by operators solely of the technical data relating to the location of the terminal equipment. It follows that those techniques do not impose on the providers concerned a retention requirement going beyond what is required in order to invoice for their services, market those services and provide value-added services. Furthermore, as has been observed in paragraph 15, the provisions of Article L. 851-3 of the Internal Security Code do not entail more general and indiscriminate retention.

27. In addition, first, it is established that real-time access to connection data makes it possible to monitor, with a high level of responsiveness, the conduct of individuals who may represent an immediate threat to public order. Second, the technique provided for in Article L. 851-3 of the Internal Security Code makes it

possible to identify, on the basis of criteria specifically defined for that purpose, those individuals whose conduct, in particular in view of their methods of communication, may point to a terrorist threat. Against a background of serious and persistent threats to national **[Or. 13]** security, and in particular the terrorist threat, the usefulness of those techniques for operational purposes is thus unparalleled.

28. 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'.

29. In those circumstances, a second major difficulty in interpreting European Union law arises: is the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, to be interpreted as authorising legislative measures which fall within the scope of activities concerning public security, defence and State security, such as the real-time measures for the collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data?

Access of the competent national authorities to the retained data:

30. In its judgment of 21 December 2016, the Court of Justice of the European Union also ruled that Article 15(1) of the Directive of 12 July 2002 'must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the territory of the European Union'. In that judgment, the Court found that 'the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read

together with Article 22 of Directive 95/46, where their rights have been infringed'.

31. A third major difficulty in interpreting European Union law is raised by the question whether the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, is to be interpreted as making the legality of the procedures for the collection of connection data subject in all cases to a requirement that the persons concerned are duly informed once such information is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or whether such procedures may be regarded as lawful taking into account all the other **[Or. 14]** existing procedural guarantees, since those guarantees ensure that the right to a remedy is effective.

32. The three questions set out in paragraphs 25 to 31 are crucial to the resolution of the disputes to be decided by the Conseil d'État concerning the four contested decrees in so far as they were adopted to implement Articles L. 851-1 to L. 851-4 of the Internal Security Code. 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, to that extent and without it being necessary to rule on the pleas of inadmissibility raised in defence, on the applications made by the applicant associations and to reject the remainder of the forms of order sought by them.

HAS DECIDED AS FOLLOWS:

Article 1 The applications are rejected in so far as they are directed against Decrees Nos 2015-1185 of 28 September 2015, 2015-1211 of 1 October 2015, 2015-1639 of 11 December 2015 and 2016-67 of 29 January 2016 to the extent that they implement the provisions of Articles L. 851-5 and L. 851-6 and those of Chapters II, III, and IV of Title V of Book VIII of the Internal Security Code.

Article 2: Judgment is stayed, to that extent, on the applications made by the applicant associations 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, against a background of serious and persistent threats to national security, and in particular the terrorist threat, 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. Is the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, to be interpreted as authorising legislative

measures, such as the real-time measures for the collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data?

3. Is the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, to be interpreted as making the legality of the procedures for the collection of connection data subject in all cases to a requirement that the persons concerned are duly informed once such information is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or may such procedures be regarded as lawful taking into account all the other existing procedural guarantees, since those guarantees ensure that the right to a remedy is effective? **[Or. 15]**

Article 3: … **[Or. 16]**

…