Alexis FITZJEAN Ó COBHTHAIGH
Lawyer of the Paris Bar
5, rue Daunou – 75002 PARIS
Tel. 01.53.63.33.10 – Fax 01.45.48.90.09
info@afocavocat.eu

COURT OF JUSTICE

OF

THE EUROPEAN UNION

OBSERVATIONS ON

THE QUESTIONS REFERRED FOR A PRELIMINARY RULING

JOINED CASES

C-511/18 and C-512/18

ON BEHALF OF: Center for Democracy and Technology (CDT) (C-511/18 and C-512/18)

DEFENDANTS:
1) The Prime Minister (France)
2) The Minister of Justice (France)
3) The Minister of the Interior (France)
4) The Minister of Defense (France)

APPLICANTS:
1) La Quadrature du Net
2) Fédération des fournisseurs d'access à Internet associatifs
3) igwan.net
4) French Data Network
5) Privacy International

FACTS

1. The Center for Democracy and Technology (CDT), petitioner, is a non-governmental organization that supports online fundamental rights and freedoms and is active in researching possible and technically viable solutions to the most pressing challenges faced by users of electronic communications technologies.

2. Since its establishment, which occurred approximately 25 years ago, CDT has played a primary role in the development of policies, practices and rules so as to allow individuals to effectively take control of technology. Based in Washington, D.C. (United States), CDT is a non-profit organization that is recognized and registered in the United States and has offices in Brussels. CDT actively supports the rigorous development of European laws and rules in compliance with human rights within the domains of privacy and freedom of expression.

3. CDT intervened several times before the European Court of Human Rights (ECHR), notably in one case on governmental access to personal data (see ECHR, 12 January 2017, *Szabo and Vissy v. Hungary*, No. 37138/14) and, more recently, in the case of *Big Brother Watch & Others* (see ECHR, 13 September 2018, No. 58170/13, 62322/14 and 24960/15), concerning the United Kingdom's surveillance practices.

4. CDT intervened before the French *Conseil d'Etat* in Case No. 393099 on the annulment, on the grounds of having exceeded authority, of the implicit dismissal, resulting from the non-response by the Prime Minister, of the request submitted by La Quadrature du Net, Fédération des fournisseurs d'access à Internet associatifs and French Data Network to repeal Article R. 10-13 of the Postal and Electronic Communications Code and Decree No. 2011-219 of February 2011.

5. By decisions No 3933099 and No. 394922, 394925, 397844 and 397851 of 26 July 2018, the French *Conseil d'Etat* submitted a series of requests for a preliminary ruling to the Court of Justice of the European Union.

6. The said requests for a preliminary ruling were registered by the Registry of the Court of Justice of the European Union (hereinafter "the Court") under No. C-511/18 and C-512/18, which were then joined. The Court invited CDT to submit its observations on the questions referred.

7. This brief constitutes CDT's observations on such questions.

ARGUMENTS

8. First, CDT will lay out on the one hand the key provisions of the French rules discussed in the main proceedings (I), and, on the other, the basic principles of EU law that were clarified by the Court in its case law, in relation to the questions referred for a preliminary ruling (II).

9. Secondly, CDT will lay out in detail the legal framework applicable in the United States, where there is no general and indiscriminate obligation to retain connection data, nor is there any mass surveillance program on the territory of the United States, so as to show that, contrary to what the tone of the questions submitted by the *Conseil d'Etat* implies, such a severe interference on the fundamental freedoms of the Union's citizens is not necessary to ensure safety, nor to ensure national security, nor to fight against terrorism or serious crime (III).

I.- The rules discussed in the main proceedings

10. **On the questions relating to the general retention of connection data under general law**

11. The rules discussed in the main proceedings notably consist, on the one hand, in Articles L. 34-1 and R. 10-13 of the Postal and Electronic Communications Code,[1] which apply to operators of electronic communications (providers of electronic networks or communications services) and concerning traffic and location data, and, on the other hand, in Decree No. 2011-219, adopted in application of Article 6, II of the law on confidence in the digital economy, which applies to the persons mentioned under Article 6, I 1 and 2 of the said law (access providers and web hosts) and concerning identifying data, therein including traffic data.

12. In particular, those rules provide that, on the one hand, persons whose activity consists in offering access to online public communications services are obligated to retain the connection identifier, the identifier attributed to the subscriber, the identifier of the device used for the connection, the date and time of start and end of the connection, and the features of the subscriber's line; on the other hand, that those who, even free of charge, for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind, supplied by recipients of those services, are obligated to retain the connection identifier at the beginning of the communication, the identifier assigned by the information system to the content, the subject of the operation, the type of protocols used to connect to the service and to transfer the content, the nature of the operation, the date and time of the operation, and the identifier used by the person from which the operation originates when it was provided by the latter.

---

[1] Article R. 10-13 of the Postal and Electronic Communications Code: "*I. – In application of the third paragraph of Article L.34-I, operators of electronic communications shall retain, for the purpose of investigating, determining and prosecuting criminal offences:*

a) Information enabling the identification of the user;
b) The data relating to the terminal devices used for the communication;
c) The technical features, as well as the date, time and duration of each communication;
d) The data relating to supplementary services that were requested or used, and the providers thereof;
e) The data enabling the identification of the recipient or recipients of the communication.

II. – In relation to telephony activities, operators shall retain the data set out under paragraph two and, moreover, those enabling the determination of the origin and localization of the communication.

III. – The data mentioned in this article shall be retained for one year from when they are recorded. (…)"

13. Furthermore, these two categories of persons must retain the information provided at the moment when the user concludes a contract or creates an account, namely, when the account is created, the identifier of that connection, the name and last name or the company name, the associated postal addresses, the pseudonyms used, the associated e-mail or account addresses, telephone numbers, and the password as well as the data that allow it to be verified or modified, in the last updated version. Finally, these two categories of persons must also retain, when the contract or account is subscribed for a fee, the information relating to the type of payment used, the payment reference, the amount, as well as the date and time of the transaction.

14. It follows that the French rules on the retention of traffic and location data and of other data relating to electronic communications mandate the retention of an amount of data that is clearly broader than the Swedish rules in question in the *Tele2* case, and for a duration of one year, that is double the time provided for under the Swedish rules in that case.

15. **On the questions relating to mass intelligence**

16. The connection data that may be collected in the framework of the intelligence techniques are even more significant since, in addition to those data retained "under general law", the second indent of paragraph I of Article R. 851-5 of the Internal Security Code[2] also includes the technical data enabling the localization of terminal equipment, those relating to that equipment's access to networks or online public communications services, those relating to the conveyance of electronic communications through the networks, those relating to the identification and authentication of a user, of a connection, of a network or of a public online communication service and those relating to the features of the terminal equipment and to their software configuration data.

17. The surveillance measures set out under the rules in question may be applied for several purposes, far exceeding the fight against serious crime and by means that interfere in a significant way with the fundamental rights that are protected by the Charter.

18. Oversight of the implementation of the intelligence techniques is subject to a simple opinion by the CNCTR (the National Commission on the Control of Intelligence Techniques), which is not binding on the Prime Minister (see Articles L. 821.3 and 821-4 of the CSI) and that is not necessary in cases of urgency (see Article L.821-5 of the CSI).

---

[2] Article R. 851-5 of the Internal Security Code: "*I.- The information or documents set out under Article L.851-1 shall be, with the exception of the content of the communications or of the information consulted:*

1. *Those laid out under Articles R.10-13 and R. 10-14 of the Postal and Electronic Communications code and under Article 1 of Decree No 2011-219 of 25 February 2011 relating to the retention and communication of data enabling the identification of any person that contributed to the creation of content placed online;*
2. *The technical data, other than those mentioned under paragraph 1:*
   a) *Enabling the localization of the terminal devices;*
   b) *Relating to the access of the terminal devices to networks or public online communications services;*
   c) *Relating to the conveyance of electronic communications through the network;*
   d) *Relating to the identification and authentication of a user, of a connection, of a network or of an online public communications service;*
   e) *Relating to the features of the terminal devices and to their software's configuration data.*

II.- Only the information and documents set out under the first indent of the first paragraph shall be collected in accordance with Article L.851.1. Such collection shall occur at different times.

The information set out under the second indent of the first paragraph shall only be collected in accordance with Articles L.851-2 and L.851-3, within the conditions and limits provided for under those articles and subject to Article R. 851-9."

19. Furthermore, judicial review relating to the implementation of the intelligence techniques does not comply with EU law, since there is no provision requiring, at any time, that the person being the subject of a surveillance measure be duly informed, since there is no possibility, throughout the pre-litigation and litigation procedure, for an *inter partes* procedure, and since no recourse is allowed in relation to international surveillance, as was recognized by the Constitutional Court (see Const. Court, 26 November 2015, Intelligence Law, Decision No. 2015-722 DC) as well as by the specialized chamber of the Conseil d'Etat (see Conseil d'Etat, specialized chamber, 19 October 2016, No 397623). Moreover, the latter clarified that an appeal, on the grounds of excess of power, cannot be submitted in relation to the lack of a referral to the Conseil d'Etat by the President of the CNCTR (see Conseil d'Etat, specialized chamber, 20 June 2018, *Sophie in'T Veld*, No 404012).

II.- EU Law prohibits, on the one hand, the general and indiscriminate retention of connection data, and, on the other, a mass surveillance system, such as those in question in the main proceedings

20. At the outset, there is no doubt that the general and indiscriminate retention of connection data, as well as a system of mass surveillance and of automated and non-targeted intelligence, such as that implemented in France, "poses the danger of undermining or even destroying democracy on the ground of defending it" (See ECHR, 6 September 1978, *Klass and others v Germany*, Application No. 5029/71, §§ 49-50; ECHR, 4 May 2000, *Rotaru v Romania*, Application No 28341/95, § 49).

II.1.- This dispute clearly falls under the scope of application of the EU Charter of Fundamental Rights (hereinafter "the Charter")

21. By way of introduction, it should be recalled that a law, such as that in question in the main proceedings, which obligates providers of electronic communication services to retain traffic and location data, falls under the scope of application of Directive 2002/58 of 12 July 2002. Similarly, a domestic law, such as that in the main proceedings, on the access by domestic authorities to data retained by those providers, also falls under the scope of application of that Directive (see, *mutatis mutandis*, CJEU, 21 December 2016, *Tele2 Sverige AB and others*, No C-203/15, C-698/15, EU:C:2016:970, hereinafter "*Tele2*", paras. 75-81).

22. In that regard, it should be noted that, having submitted several requests for preliminary rulings in its decision No. 394922, 394925, 397844, 397851 of 26 July 2018, the Conseil d'Etat held, at point 21 of its decision, completely contrary to the Court's settled case law, that "it clearly appears from the Directive of 12 July 2002 that the provisions of Articles L. 851-5 and L. 851-6, as well as chapters II, III and IV of title V of book VIII of the code of internal security, do not fall under its scope of application, since they concern intelligence collection techniques that are directly implemented by the State without requiring any action by providers of electronic communications services by imposing specific obligations upon them. Hence, these provisions should not be considered as implementing EU law and, therefore, the claims relating to the misinterpretation of Directive of 12 July 2002, interpreted in the light of the EU Charter of fundamental rights, cannot be invoked against them."

23. By doing so, the Conseil d'Etat manifestly reduced the scope of application of EU law and deprived it of *effet utile* and of direct effect, unduly restricting the possibility to rely on it. The Court may seize the occasion represented by this case to reiterate its own interpretation, that will surely be radically opposed to that of the Conseil d'Etat on this point.

II.2.- The confidentiality of communications is a fundamental principle of EU law, which only allows for limited exceptions that must be interpreted strictly

24. The principle of confidentiality of communications established, as it is well known, by Directive 2002/58, implies, *inter alia*, as stated in the second sentence of Article 5(1) of that directive, that, as a general rule, any person other than the user is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorized in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication (see *Tele2*, point 85 and CJEU, 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, para. 47).

25. In other words, the system put in place by Directive 2002/57 requires that the retention of traffic and location data be an exception that is strictly regulated and limited (see *Tele2*, para. 104).

26. The processing and storage of traffic data are permitted only to the extent and for the time necessary for the billing and marketing of services and for the provision of value-added services (see *Tele2*, para. 86; *Promusicae*, C-275/06, EU:C:2008:54, paras. 47 and 48). As for, in particular, the billing of services, that processing is permitted only until the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data that was processed and stored must be erased or made anonymous (see *Tele2*, para. 86). As for location data other than traffic data, under Article 9(1) of the said directive that data can only be processed subject to certain conditions and after having rendered it anonymous or having obtained the consent of the users or subscribers (se *Tele2*, para. 86).

27. This case must be interpreted in light of the principle of minimization of personal data collected and processed, recalled in particular by recital 30 of Directive 2002/58 (see *Tele2*, para. 87).

28. Insofar as Article 15(1) of Directive 2002/58 enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision, in accordance with the Court's settled case-law, must be interpreted strictly (see *Tele2*, para. 89; CJEU, 22 November 2012, *Probst*, C-199/12, EU:C:2012:748, para. 23).

II.3.- The interference consisting in the general and indiscriminate retention of connection data is wide-ranging and must be considered to be particularly serious

29. The Court has already held, in a grand chamber judgment, that "data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the

location of mobile communication equipment, data which consist, *inter alia*, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services (…) make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period" (see CJEU, 8 April 2014, *Digital Rights Ireland*, No C-293/12 and C-594/12, EU:C:2014:238, para. 26; see also *Tele2*, para. 96).

30. The Court noted, very rightly so, that "[t]hose data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them" (*Digital Rights Ireland*, para. 27; *Tele 2*, para. 99). In particular, those data provide the means to determine, as the Court has held, following the conclusions of Advocate General M. Henrik Saugmandsgaard Øe at paras. 253, 254 and 257 to 259 of his conclusion on the *Tele2* case, "the profile of the individuals concerned, information that is no less sensitive, having regard to the right of privacy, than the actual content of communications" (see *Tele2*, para. 99).

31. Even if such legislation does not formally permit the retention of the content of a communication, the retention of the traffic and location data affects the use of means of electronic communication and, consequently, the exercise by the users of their freedom of expression, guaranteed in Article 11 of the Charter (see *Digital Rights Ireland*, para. 28; *Tele2*, para. 101).

32. Consequently, "[t]he retention of data for the purpose of possible access to them by the competent national authorities (…), directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article" (*Digital Rights Ireland*, para. 29).

33. As a result, the obligation imposed on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter (see *Digital Rights Ireland*, para. 34).

34. Furthermore, "the access of the competent national authorities to the data constitutes a further interference with that fundamental right", so that "the rules relating to the access of the competent national authorities to the data constitute, in the same way, an interference with the rights guaranteed by Article 7 of the Charter" (see *Digital Rights Ireland*, para. 35). Likewise, such access constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter (see *Digital Rights Ireland*, para. 36).

35. Such interference with the fundamental rights enshrined under Articles 7 and 8 of the Charter is wide-ranging, and must be considered to be particularly serious (see *Digital Rights Ireland*, para. 37; *Tele2*, para. 100). Furthermore, the fact that data are retained and subsequently used

without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (se *Digital Rights Ireland*, para. 37; *Tele2*, para. 100).

36. Under Article 52(1) of the Charter, in particular, any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of other (see *Digital Rights Ireland*, para. 38). This general principle of proportionality is also reiterated in both 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 the free movement of such data, and repealing Directive 95/47/EC (GDPR), under which collected data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (see Article 5(1)(c)), and in Directive 2016/680, according to which those data must be "adequate, relevant and not excessive in relation to the purposes for which they are processed" (see Article 4(1)(c)).

37. Therefore, while it is true that such interference may be capable of meeting an objective of general interest, it is also true that it is radically disproportionate in relation to the objectives pursued.

II.4- <u>The interference by the domestic law discussed in the main proceedings is not only not necessary to achieve the objectives pursued, but is also radically disproportionate</u>

38. First, it must be reiterated that, in accordance with the Court's settled case-law, the principle of proportionality requires that actions that interfere with fundamental rights must be capable of attaining the legitimate objectives pursued by the legislation in question and must not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, *mutatis mutandis*, *Digital Rights Ireland*, para. 46; *Schrems*, para. 92; *Tele2*, paras. 96 and 116).

39. In the present case, taking into account, on the one hand, the essential role played by the protection of personal data in relation to the fundamental right to respect for private life and, on the other hand, the extent and the seriousness of the interference with that right, which results from a system of mass surveillance such as that discussed in the main proceedings, the legislator's discretion is reduced, with the result that review of that discretion should be strict (see *Digital Rights Ireland*, para. 48).

40. It is certainly true that the data that must be retained in accordance with the legislation discussed in the main proceedings may eventually be such as to allow national law enforcement authorities to have additional opportunities to shed light on serious crimes, and may thus constitute a valuable tool for criminal investigations.

41. However, such an objective of general interest, important as it may be, may not in itself justify a retention measure such as that established by the rules discussed in the main proceedings being considered to be necessary for the purpose of that fight (see *Digital Rights Ireland*, para. 51).

42. The protection of the fundamental right to the respect for private life requires, in accordance with settled case-law of the Court, in any event, that derogations and limitations to the protection of personal data must operate within the limits of what is strictly necessary (see CJEU, 26 July 2017, *Opinion 1/15*, para. 140; *Tele2*, paras. 96 and 116; CJEU, 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, para. 92; *Digital Rights Ireland*, para. 52; CJEU, 7 November 2013, *IPI*, C-473/12, EU:C:2013:715, para. 39 and cited case-law).

43. In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter (see *Digital Rights Ireland*, para. 53).

44. Consequently, in order to comply with EU law and in particular with the Directive of 12 July 2002 interpreted in the light of the Charter and the Directive of 8 June 2000, interpreted in the light of Articles 6, 7, 8 and 11, as well as Article 52(1), of the Charter, the rules discussed in the main proceedings 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 data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see *Digital Rights Ireland*, para. 54; by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, No. 58243/00, §§ 62 and 63; ECHR, 1 July 2008, *Rotaru v. Romania [GC]*, No. 28341/95, §§ 57 to 59; *S. and Marper v. the United Kingdom*, § 99).

45. The need to provide for such safeguards is all the greater where, as laid down in the legislation discussed in the main proceedings, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see *Digital Rights Ireland*, para. 55; by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103; ECHR, 18 April 2013, *M. K. v. France*, No. 19522/09, § 35).

46. The interference resulting from the legislation discussed in the main proceedings is far from being limited to what is strictly necessary, since, in particular, those rules impose the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mails, internet telephony as well as all connection data retained by the web hosts. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, those rules cover all subscribers and registered users. They therefore entail an interference with the fundamental rights of all users of those services, regardless of their nationality (see *Digital Rights Ireland*, para. 56).

47. **First**, the legislation in question in the main proceeding covers, in a generalized manner, all persons and all means of electronic communication as well as all traffic data, without any distinction, limitation or exception being made in the light of the objective of fighting against serious crime (see *Digital Rights Ireland*, para. 57).

48. On the one hand, those rules affect, in a comprehensive manner, all persons using electronic communications services, without, however, the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. They therefore apply even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, they do not provide for any exception, with the result that they apply even to persons whose

communications are subject to the obligation of professional secrecy (see *Digital Rights Ireland*, para. 58; *Tele2*, para. 105).

49. On the other hand, while the justification provided for these rules is the fight against serious crime, it is particularly astonishing to note that they do not require any relationship between the data whose retention is provided for and a threat to public security. In particular, they are not restricted to a retention in relation to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences (see *Digital Rights Ireland*, para. 59; *Tele2*, para. 106, in which these three elements are included under the general notion of "*fighting crime*").

50. **Next**, in addition to this general absence of limits is the fact that the rules in question in the main proceedings fail to lay down any objective criterion by which to determine the limits of the access by the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference (see *Digital Rights Ireland*, para. 60).

51. In particular, these rules do not lay down any objective criterion that is capable of limiting the number of persons authorized to access and subsequently use the data retained to what is strictly necessary in light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not subject to a prior review carried out by a court or by an independent administrative body under EU law whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions (see *Digital Rights Ireland*, para. 62).

52. **Finally**, as regards the data retention period, the rules in question in the main proceedings require that those data be retained for a period of one year, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned (see *Digital Rights Ireland*, para. 63).

53. That very long retention period is set in a completely arbitrary way, without being based on objective criteria in order to ensure, in particular, that it is limited to what is strictly necessary (see *Digital Rights Ireland*, para. 64).

54. It follows from the above that the legislation in question in the main proceedings does not lay down sufficiently clear and precise rules that are capable of limiting the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that those rules entail a wide-ranging and particularly serious interference with those fundamental rights, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary (see *Digital Rights Ireland*, para. 65).

55. Moreover, the legislation in question in the main proceedings do not provide for sufficient safeguards, such as those required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that

data. Indeed, those rules do not lay down rules which are specific and adapted to the vast quantity of data whose retention is required by those rules, the sensitive nature of that data and the risk of unlawful access to that data, rules which would serve, in particular, to ensure the full integrity and confidentiality of the data in question (see *Digital Rights Ireland*, para. 66).

56. In particular, the rules in question do not lay down the conditions under which providers of electronic communications services must grant competent national authorities access to data retained, in a way that strictly restricts access to the objectives set out under Article 15(1) of Directive 2002/58, nor does it lay down sufficiently precise substantive and procedural conditions governing such access (see *Digital Rights Ireland*, para. 61; *Tele2*, para. 118). They also do not lay down sufficiently precise substantive and procedural conditions governing the use of those data (see *Opinion 1/15*, para. 192).

57. Furthermore, the rules in question do not impose on the competent national authorities to whom access to the retained data has been granted an obligation to notify the persons affected, as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities (see *Tele2*, para. 121), even though that notification is 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 (see *Opinion 1/15*, para. 220; *Tele2*, para. 121; *Schrems*, para. 95; CJEU, 7 May 2009, *Rijkeboer*, No. C-553/07, EU:C:2009:293, para. 52). Indeed, "the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively" (see ECHR, 4 December 2015, *Zakharov v. Russia*, No 47143/06, § 234).

58. It should be noted that, after having annulled 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 (see *Digital Rights Ireland*, above), the Court ruled:

- on the one hand, that "*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, 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*" and,

- on the other hand, that "*Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 as well as Article 52(1) of the Charter of Fundamental Rights, 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 European Union."

59. This case law was further confirmed by Opinion 1/15 of 26 July 2017, in which the Court notably held, in relation to the Passenger Name Records (PNR) Agreement negotiated between the European Union and Canada, on the one hand that the retention of passenger name record data after their departure from Canada must be strictly limited to those passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime and, on the other hand, that air passengers must be afforded a right to individual notification in the event of use of passenger name record data concerning them during their stay in Canada and after their departure from that country, as well as in the event of disclosure of that data by the Canadian competent authority to other domestic authorities or to individuals, and that compliance with said rules must be guaranteed by an independent supervisory authority.

60. **In this case**, the French rules in question in the main proceedings provide for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users, relating to all means of electronic communication, and they impose on providers of electronic communications services an obligation to retain those data systematically and continuously, with no exceptions (see, *mutatis mutandis*, *Tele2*, para. 97).

61. Those rules thus exceed the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 as well as Article 52(1) of the Charter (see, *mutatis mutandis*, *Tele2*, para. 107).

62. Furthermore, those rules provide for a form of mass surveillance and non-targeted intelligence system, without any prior authorization by a judge or by an administrative authority, nor any notification of surveillance measures that were carried out and without any effective judicial review, in breach, in particular, of the Directive of 12 July 2002 and of Article 5(1)(c) of the GDPR and Article 4(1)(c) of Directive 2016/680, read in the light of the Charter.

63. This is especially true since many States, such as the United States, reject any general and indiscriminate obligation to retain connection data upon operators of electronic communications, as well as mass surveillance on their own territory (III).

III.- <u>United States law prohibits any mass surveillance on the territory of the United States, and excludes any general retention of connection data</u>

64. The present questions referred for a preliminary ruling were formulated in such a way as to attempt to give rise to the impression that rules that are particularly infringing upon fundamental rights of EU citizens are "necessary" in view of the actual risks faced by the EU Member States.

65. That is not the case.

66. The experience of the United States shows that a general and indiscriminate obligation to retain data is not necessary to ensure public safety, therein including for an effective fight against terrorism, and neither is legislation authorizing mass and indiscriminate surveillance.

67. Indeed, under US law there is no obligation upon electronic communications operators to retain connection data.

68. The United States Supreme Court has recently held that access to location data of a portable cell phone is subject to obtainment of a warrant in due form, supported by probable cause (which is the standard that governs searches and seizures by law enforcement), rather than a simple court order issued under the Stored Communications Act, which requires a showing of "reasonable grounds" (see SCOTUS, 22 June 2018, *Carpenter v. US*, No 16-402).[3]

69. Instead of a mass and general retention, the United States Congress granted law enforcement authorities a procedure that allows them to compel electronic communications providers to retain data of a specifically targeted person for up until 90 days, with the possibility to renew that retention period.[4] A court order or other court procedure, depending on the nature of the data, is necessary for law enforcement authorities to be allowed to compel the transfer of the requested data.

70. It should be noted that the United States Congress has had the opportunity to lay down rules mandating the general and indiscriminate retention of connection data in 2011, but the proposed law was not able to gather sufficient support to result in a vote in the House of Representatives (one of the two chambers of Congress). This proposal was met with the decisive opposition of the former president of the full Committee, representative James Sensenbrenner, who explained that the proposal to create a general obligation to retain connection data should have been relegated to the "dustbin of history" and that "this bill goes against the privacy rights of people that use the Internet for thousands of lawful purposes."[5]

71. Similarly, within the United States domestic surveillance and intelligence must be targeted and not indiscriminate, on the basis of the Foreign Intelligence Surveillance Act (FISA). Within the context of foreign intelligence, that law applies regardless of the objective pursued, including in relation to national security, public safety or the fight against terrorism carried out by foreign organizations. Surveillance of the content of a communication is not allowed, under FISA, except when there is "probable cause" that the surveillance measure targets a

---

[3] https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf: "As with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." *Id.*, at 415 (opinion of SOTOMAYOR, J.). These location records "hold for many Americans the 'privacies of life.'" *Riley*, 573 U. S., at ___(slip op., at 28) (quoting *Boyd*, 116 U. S., at 630). And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in Jones. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone – almost a "feature of human anatomy," *Riley*, 573 U. S., at ___ (slip op., at 9)—tracks nearly exactly the movements of its owner.
(…)
Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may – in the Government's view – call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance."

[4] 18 USC §2703(f).

[5] https://judiciary.house.gov/_files/hearings/printers/112th/112-60_67309.PDF%20at%202.

foreign power (such as a foreign government or terrorist organization) or an agent of a foreign power.[6]

72. Under FISA, such a surveillance request must be submitted to a specific court (the Foreign Intelligence Surveillance Court, FISC) and must include: 1) an illustration of the reasons leading to believe that the target of the surveillance is a foreign power or an agent of a foreign power, 2) a statement that the sought information is considered to be of a foreign nature and that such information cannot be reasonably obtained through conventional intelligence measures, 3) a detailed description of the previous requests concerning the target, 4) a detailed description of the nature of the information requested and of the type of communications or activities subject to surveillance, 5) the duration of the envisaged surveillance, 6) whether introduction in private property is necessary, and 7) suggestions to minimize the acquisition, use and retention of necessary information concerning non-consenting US citizens or residents.

73. The Fourth Amendment of the US Constitution requires that surveillance measures carried out by law enforcement authorities be targeted. In relation to criminal investigations, law enforcement authorities are also subject to the Electronic Communications Privacy Act (ECPA), when they seek to surveil communications or obtain communications data (dates, headers, in particular the sender and recipient of a message).

74. Under the Wiretap Act, law enforcement authorities must have prior authorization by a court before wiretapping the content of a communication.[7] The request can only be authorized after a complete examination of the facts that are capable of justifying that such a court authorization must be granted, including in particular the details relating to the offense in question (which must be a serious crime such as corruption or terrorism), a description and localization of the devices to be placed under surveillance and the identity of the person that committed the crime, if known, and a complete and detailed statement that other investigation procedures have been tried and failed or why they would clearly fail. The requested surveillance measure is granted only if a court determines that there is solid and serious evidence ("probable cause") to grant said request. As a result, these surveillance measures can only be authorized when they concern a particular individual and a particular investigation.

75. Similarly, a warrant issued by a court in accordance with the protection standards of the Fourth Amendment of the US Constitution is necessary in order to access the content of a targeted communication.[8] Searches for traffic data or information pertaining to a subscription also require prior authorization by a warrant, a court order[9] or a by a subpoena. In this case as well, the request must be targeted.

76. In 2013, Edward Snowden, a National Security Agency (NSA) contractor, revealed, *inter alia*, that the NSA received data relating to all telephone calls placed within the United States. CDT[10], among several other organizations, the US Privacy and Civil Liberties Oversight

[6] 50 USC Section 1805(a)
[7] 18 U.S.C. § 2518
[8] *United States v. Warshak*, 631 F.3d 266 (2010).
[9] 18 U.S.C. § 2703 (c)
[10] August 1, 2013 Statement for the Record at Privacy and Civil Liberties Oversight Board Hearings on Surveillance Programs, https://www.cdt.org/files/pdfs/CDT-PCLOB-Statement-for-the-Record.pdf

Board,[11] and at least one court, all considered such mass surveillance of all data relating to telephone calls to be illegal and unconstitutional.

77. In 2015, the United States Congress adopted the USA Freedom Act,[12] for the specific purpose of prohibiting, without question, any general surveillance measure within the United States. Sections 102, 201 and 501 expressly prohibit all mass surveillance measures.[13] In any case, said law requires that sufficiently precise selectors be used before any intelligence collection measure is carried out.

78. By contrast, mass and general surveillance, as well as non-targeted surveillance, are carried out outside the United States, and, in relation to the transatlantic telecommunication cables, until the connection point between the latter and national territories, to the detriment of the rest of the world and, in particular, of EU citizens and of their fundamental rights.

79. Despite the fact that only criminal investigations and targeted intelligence are allowed within the United States and that there is no law requiring electronic communication operators to retain connection data, the United States have a robust criminal system and a solid national security. This shows that legislation mandating the general and indiscriminate retention of connection data, as well as a mass surveillance system, are not necessary to ensure security or to fight against serious crime.

80. Finally, CDT expressly shares the observations submitted in this case before the Court by the French associations "La Quadrature du Net", the "Fédération des fournisseurs d'accès à Internet associatifs" and "igwan.net".

FOR THESE REASONS, and sharing those submitted by the Fédération des fournisseurs d'accès à Internet associatifs, igwan.net and La Quadrature du Net, as well as their conclusions, CDT asks the Court of Justice of the European Union to hold that:

1) A general and indiscriminate retention obligation imposed upon telecommunication operators on the basis of the provision of Article 15 of the Directive of 15 July 2002 must necessarily be considered, regardless of the context, as an interference with the rights protected by the Charter which cannot be justified by any reason whatsoever (first question referred in case C-511/18 and first question referred in case C-512/18).

2) The provisions of the Directive of 8 June 2000, read in the light of Articles 6, 7, 8 and 11 as well as Article 52(1) of the EU Charter of Fundamental Rights and of the Directive of 12 July 2002, absolutely prohibit EU Member States from introducing 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 the recipients of those services, to retain the data capable

[11] https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
[12] https://www.govinfo.gov/content/pkg/PLAW-114publ23/html/PLAW-114publ23.htm
[13] Section 102 of the law, entitled "Prohibition of bulk collection of tangible things", prohibits bulk collection under Section 215 of the USA PATRIOT Act, which governs collection of stored metadata for intelligence purposes. Section 201 of the law, entitled "Prohibition of bulk collection", outlaws bulk collection of metadata domestically in real time. Section 501 of the law, entitled "Prohibition of bulk collection", outlaws the use of National Security Letters to obtain stored metadata domestically in intelligence investigations. In each case, the USA FREEDOM Act precludes bulk collection by requiring that a "specific selection term" or selector be used as the basis for the collection.

of enabling the identification of anyone who has contributed to the creation of content or some of the content of the services that they provide, regardless of the objective pursued (second question referred in case C-512/18).

3) The Directive of 12 July 2002, read in light of the EU Charter of Fundamental Rights, of Regulation 2016/679 and of Directive 2016/680, prohibits national legislation that allows for the implementation of intelligence measures for purposes that are not limited by objective criteria, or that are aimed at combating offenses that do not constitute serious crime, that allows for the collection of data that are not necessary for the pursuit of the objectives set out under the legislation, that does not limit on the basis of objective criteria the agents that can carry out said measures to what is strictly necessary, that does not limit the further use of the collected data or that does not subject the collection, use and transfer of the data to any effective independent supervision (second question referred in case C-511/18).

4) The Directive of 12 July 2002, read in light of the EU Charter of Fundamental rights, of Regulation 2016/679 and Directive 2016/680, makes the legality of the procedures for the collection of connection data subject in all cases, on the one hand, to a requirement that the persons concerned are duly informed once such information is no longer liable to jeopardize the investigations being undertaken by the competent authorities and, on the other hand, to the possibility, for any person and without exception, to have an effective remedy before a court against any measure involving the collection, use and transfer of information (third question referred in case C-511/18).

LIST OF ATTACHMENTS PRODUCED

Document No. 1: Request by CDT to intervene before the French Conseil d'Etat;

Document No. 2: Conclusions by Mr. Edouard Crépey, *rapporteur public* of the Conseil d'Etat, delivered during the public hearing of 11 July 2018 of the 10th and 9th joint chambers, on the case of *La Quadrature du Net and others*, No. 393099, 394924, 394922, 394844 and 397851.

Alexis FITZJEAN Ó COBHTHAIGH
Lawyer of the Paris Bar