COMPUTER LAW & SECURITY REVIEW 41 (2021) 105540

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

The two judgments of the European Court of Justice in the four cases of *Privacy International*, *La Quadrature du Net and Others*, *French Data Network and Others* and *Ordre des Barreaux francophones et germanophone and Others*: The Grand Chamber is trying hard to square the circle of data retention ☆

Xavier Tracol

Senior Legal Officer, Data Protection Office, EUROJUST, P.O. Box 16183, 2500 BD The Hague, the Netherlands

ARTICLE INFO

Keywords:
European Court of Justice
Privacy International
La Quadrature du Net
Metadata
Retention of personal data
Access to personal data
National security
Article 4(2) of the treaty on EU
Articles 1(3), 3, 5, 15(1) of the e-privacy directive
Articles 6, 7, 8, 11 and 52(1) of the Charter of Fundamental Rights
UK
Brexit
Adequacy decision

ABSTRACT

On 6 October 2020, the Grand Chamber of the European Court of Justice rendered two landmark judgments in *Privacy International*, *La Quadrature du Net and Others*, *French Data Network and Others* as well as *Ordre des barreaux francophones et germanophone and Others*. The Grand Chamber confirmed that EU law precludes national legislation which requires a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security.

In situations where a Member State is facing a serious threat to national security which proves to be genuine and present or foreseeable, such State may however derogate from the obligation to ensure the confidentiality of data relating to electronic communications by requiring, by way of legislative measures, the general and indiscriminate retention of this data for a period which is limited in time to what is strictly necessary but which may be extended if the threat persists.[1] In respect of combating serious crime and preventing serious threats to public security, a Member State may also provide for the targeted retention of this data and its expedited retention. Such an interference with fundamental rights must be accompanied by effective safeguards and be reviewed by a court or by an independent administrative authority. It is likewise open to a Member State to carry out a general and

E-mail address: xtracol@eurojust.europa.eu
[1] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 168 and 177.

https://doi.org/10.1016/j.clsr.2021.105540
0267-3649

indiscriminate retention of IP addresses assigned to the source of a communication where the retention period is limited to what is strictly necessary or even to carry out a general and indiscriminate retention of data relating to the civil identity of users of means of electronic communication. In the latter case, the retention is not subject to a specific time limit.

1. Introduction

These two 85-page judgments of the Grand Chamber follow up to its case law on the retention of and access to personal data in the area of electronic communications. Such case law includes the landmark *Tele2 Sverige and Watson* judgment in which the Grand Chamber held that Member States could not impose on providers of electronic communications services an obligation of general and indiscriminate retention of both traffic and location data. This particular judgment has caused concerns in some Member States, which consider that they may have been deprived of an instrument regarded as necessary for the purposes of safeguarding national security and combating crime including terrorism.[2]

The Court sat in the Grand Chamber of fifteen judges, which includes both the President and the Vice-President of the Court as well as three Presidents of Chambers of five Judges, pursuant to Article 16(2) and (3) of the Statute of the Court and Article 27 of the Rules of Procedure of the Court.[3] The fact that the Grand Chamber is composed of senior Judges of the Court shows the importance of these four cases.

Judge Rapporteur Thomas von Danwitz was also Judge Rapporteur in the cases of *Digital Rights*,[4] *Schrems* I[5] and II,[6] *Tele2 and Watson*,[7] *Ministerio Fiscal*[8] as well as in the opinion about the agreement on Passenger Name Record data between the EU and Canada.[9] The Commission, the governments of fifteen Member States and the government of Norway submitted written observations. The Grand Chamber asked questions to the parties ahead of the hearing. The latter took place on both 9 and 10 September 2019. The European Data Protection Supervisor,[10] the Commission and the sixteen governments made verbal submissions before the Grand Chamber.

2. Relevant law

Article 15(1) of e-Privacy Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) gives Member States an option to retain data in the electronic communications sector. This provision sets out that traffic and location data may both be exceptionally retained for a limited period on the basis of a specific legislative measure taken by Member States. The retention is only allowed when it "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."

The relevant data to the four cases are metadata only, *i.e.* "the data necessary for locating the source of a communication and its destination, for determining the date, time, duration and type of communication, for identifying the communications equipment used, and for locating the terminal equipment and communications, data which comprises, inter alia, the name and address of the user, the telephone numbers of the caller and the person called, and the IP address for Internet services. By contrast, that data does not cover the content of the communications concerned."[11]

[2] Opinions of Advocate General Campos Sánchez-Bordona in Case C-623/17, in Joined Cases C-511-18 and C-512/18 and in Case 520/18 [2020] paras 2. For instance, French judges and intelligence services are worried about being deprived of crucial information or seeing their investigations hampered. See https://www.lexpress.fr/actualite/monde/europe/la-justice-europeenne-s-oppose-a-la-collecte-des-donnees-de-connexion-et-de-localisation_2135832.html

[3] See Composition of the Grand Chamber published in *Official Journal* C 296 of 16 August 2016, p. 2.

[4] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014]. See Xavier Tracol, "Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC), thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it", *Computer Law & Security Review*, Volume 30, issue 6, November 2014, pp. 736–746.

[5] Case C-362/14 *Maximillian Schrems* v. *Data Protection Commissioner* [2015]. See Xavier Tracol, "'Invalidator'strikes back: The harbour has never been safe", *Computer Law & Security Review*, Volume 32, issue 2, April 2016, pp. 345–362.

[6] Case C-311/18 *Data Protection Commissioner* v. *Facebook Ireland Ltd and Maximillian Schrems* [2020]. See Xavier Tracol, "'*Schrems* II': the return of the Privacy Shield", *Computer Law & Security Review*, Volume 39, November 2020, pp. 1–11.

[7] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* [2015]. See Xavier Tracol, "The judgment of the Grand Chamber dated 21 December 2016 in the two joint *Tele2 Sverige and Watson* cases: The need for a harmonised legal framework on the retention of data at EU level", *Computer Law & Security Review*, Volume 33, issue 4, July/August 2017, pp. 541–552.

[8] Case C-207/16 *Ministerio Fiscal* [2018]. See Xavier Tracol, "*Ministerio Fiscal*: Access of Public Authorities to Personal Data Retained by Providers of Electronic Communications Services", *European Data Protection Law Review*, 2019, Volume 5, Issue 1, pp. 127–135.

[9] Opinion 1/15 [2017]. See Xavier Tracol, "Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada", *Computer Law & Security Review*, Volume 34, issue 4, August 2018, pp. 830–842.

[10] See pleading notes available at https://edps.europa.eu/sites/edp/files/publication/19-09-11_data_retention_pleading_en.pdf

[11] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 82.

French law requires providers of electronic communications services to keep metadata so that intelligence services and authorities in the context of a judicial criminal investigation can access it. Belgian law is similar. British law however requires these same providers not to keep but to transmit metadata to security and intelligence services. French and Belgian laws both provide for the mere retention of personal data whilst British law requires the transmittal of data to the authorities. In addition, the British Investigatory Powers Act applies to the personal data of European data subjects upon being processed in the UK.

3. Procedural background of the cases

Proceedings were brought before the British Investigatory Powers Tribunal,[12] the French Council of State[13] and the Belgian Constitutional Court[14] about the lawfulness of legislation adopted by certain Member States in these areas, laying down in particular an obligation for providers of electronic communications services to forward users' traffic and location data to a public authority or to retain such data in a general or indiscriminate way. In a judgment of 17 October 2016, the British Investigatory Powers Tribunal "held that the defendants in the main proceedings had acknowledged that those agencies acquired and used, in their activities, sets of bulk personal data, such as biographical data or travel data, financial or commercial information, communications data liable to include sensitive data covered by professional secrecy, or journalistic material."[15] In other words, British security agencies admitted that they had acquired and used material subject to professional secrecy.

The three domestic Tribunal and Courts referred the cases to the Court of Justice for preliminary rulings. The application of the e-Privacy Directive to activities relating to national security[16] and the fight against terrorism arose in all four cases.

4. Opinion of Advocate General Manuel Campos Sánchez-Bordona dated 15 January 2020

Advocate General Manuel Campos Sánchez–Bordona delivered three different opinions[17] in the four cases. He first clarified the applicability of the e-Privacy Directive to the area at hand. Regarding its scope, the Advocate General submitted that the Directive excludes from its application "*activities* which are intended to safeguard national security and undertaken by the public authorities themselves, without requiring the cooperation of private individuals and, therefore, without imposing on them obligations in the management of businesses."[18] When the cooperation of private parties, on whom certain obligations are imposed, is however required, even on grounds of national security, those activities move into an area governed by EU law, *i.e.* the protection of privacy enforceable against those private actors. The Directive accordingly applies, in principle, where providers of electronic services are required by law to retain their subscribers' data and to allow access by public authorities to such data, as in these four cases, irrespective of whether those obligations are imposed on such providers for reasons of national security.[19]

The Directive further empowers Member States to adopt legislative measures which, in the interests of national security, affect the activities of individuals subject to the authority of those States by restricting their rights. Advocate General Campos Sánchez–Bordona contended that limitations on the obligation to guarantee the confidentiality of communications and related traffic data must be interpreted strictly and with regard to the fundamental rights enshrined in the Charter.

The Advocate General submitted that the Grand Chamber should endorse the *Tele2 Sverige and Watson* judgment including the retention of data within the EU.[20] He expressed his belief that the British legislation does not satisfy the conditions in this judgment since it involves general and indiscriminate retention of personal data, which provides a detailed account of the life of the relevant persons for a lengthy period of time.[21] Advocate General Campos Sánchez–Bordona however recognised the usefulness of an obligation to retain data for the purposes of safeguarding national security and combating crime. He consequently recommended limited and discriminate retention, *i.e.* the retention of specific categories of data which are absolutely essential for the effective prevention and control of crime and the safeguarding of national security for a set period adapted to each particular category and limited access to this data. The latter is subject to a prior review carried out either by a court or by an independent administrative authority,[22] to the data subjects being notified – provided that the notification does not jeopardize ongoing investigations[23] – and to the adoption of rules to avoid misuse of, and unlawful access to, this data. The Advocate General nonetheless added that in genuinely *exceptional* situations characterised by an imminent threat or extraordinary risk such as to warrant the of-

[12] C-623/17 *Privacy International* [2020].
[13] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020].
[14] C-520/18 *Ordre des barreaux francophones et germanophone and Others* [2020].
[15] Case C-623/17 *Privacy International* [2020] para 20.
[16] Regarding the emphasis placed by the British Investigatory Powers Tribunal on the activities of the security and intelligence agencies connected to national security in the *Privacy International* case, see Opinion of Advocate General Campos Sánchez-Bordona in Case C-623/17 [2020], para 34.
[17] Opinions of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18, Case C-520/18 and Case C-623/17 [2020].
[18] Opinion of Advocate General Campos Sánchez-Bordona in Case C-623/17 [2020] para 79.
[19] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 [2020] para 42; Case C-623/17 [2020] para 24. See also *ibidem*, paras 30 to 32.
[20] Opinion of Advocate General Campos Sánchez-Bordona in Case C-623/17 [2020] para 43.
[21] Opinion of Advocate General Campos Sánchez-Bordona in Case C-623/17 [2020] para 37.
[22] Opinions of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 and Case C-520/18 [2020] paras 139.
[23] Opinion of Advocate General Campos Sánchez-Bordona in Case C-623/17 [2020] para 43; Joined Cases 511/18 and C-512/18 [2020] para 153.

ficial declaration of a state of emergency, national legislation may provide for the option, for a limited period of time, of imposing an obligation to retain data which is as extensive and general as necessary.[24]

In response to the first question asked by the Council of State, Advocate General Campos Sánchez–Bordona submitted that the Directive precludes the French legislation which, against a background of serious and persistent threats to national security, in particular the terrorist threat, imposes on operators and providers of electronic communications services the obligation to retain, in a general and indiscriminate fashion, the traffic and location data of all subscribers as well as data which can be used to identify the creators of the content offered by the providers of those services. He asserted that, as recognised by the Council of State itself, the obligation to retain data imposed by the French legislation is general and indiscriminate,[25] and therefore a particularly serious interference in the fundamental rights enshrined in the Charter. The Advocate General reiterated that, in the *Tele2 Sverige and Watson* judgment, the Court had rejected the possibility of general and indiscriminate retention of personal data in the context of the fight against terrorism that he defined as an example of a threat to national security.[26] Advocate General Campos Sánchez-Bordona maintained that the fight against terrorism must not be considered solely in terms of practical effectiveness but in terms of legal effectiveness so that its means and methods should be compatible with the requirements of the rule of law under which power and strength are subject to the limits of the law and, in particular, to a legal order which finds in the defence of fundamental rights the reason and purpose of its existence. Further, the French legislation is again incompatible with the Directive since it imposes no obligation to notify the data subjects of the processing of their personal data by the competent authorities in order to ensure that those persons can exercise their right to effective judicial protection other than when such notification jeopardises the actions of those authorities.

The Directive does however not preclude national legislation which permits the real-time collection of both traffic and location data of individuals provided that those activities are carried out in accordance with established procedures for accessing legitimately retained personal data and are subject to the same safeguards.[27]

In the *Ordre des Barreaux francophones and germanophone and Others* case,[28] the Advocate General proposed that the Court of Justice should reply to the Constitutional Court that the Directive precludes legislation which, like the Belgian legislation, has as its objectives not only the fight against terrorism and serious crime but also defence of the territory, public security, the investigation, detection and prosecution of less serious offences and, in general, any other objective provided for in Article 23(1) of the GDPR on restrictions.[29] The reason is that, even though access to the data retained is subject to precisely prescribed safeguards, a general and indiscriminate obligation is imposed on operators and providers of electronic communication services.[30] Such obligation, which applies permanently and continuously to retain both traffic and location data processed in the course of the provision of those services, is incompatible with the Charter.[31]

Regarding the question whether, in the event that national legislation is incompatible with EU law, its effects could be temporarily maintained, Advocate General Campos Sánchez–Bordona considered that a national court may, if its domestic law so permits, maintain the effects of legislation such as the Belgian legislation, on an exceptional and temporary basis, even where this legislation is incompatible with EU law, if maintaining those effects is justified by overriding considerations relating to threats to public security or national security which cannot be addressed by other means or other alternatives but only for as long as is strictly necessary to correct the incompatibility with EU law.

Last, in the *Privacy International* case,[32] the issue was whether national legislation is compatible with the Directive when it imposes on a provider of electronic communications networks the obligation to supply to the British Security and Intelligence Agencies bulk communications data after general and indiscriminate collection.[33] The Advocate General considered that, notwithstanding Article 4(2) of the treaty on EU, which provides that national security is the exclusive responsibility of each Member State, the Directive precludes the British legislation.

Advocate General Campos Sánchez-Bordona thus submitted that a high level of protection should continue applying to both traffic and location data even when accessed for purposes of national security.

5. Judgments of the Grand Chamber dated 6 October 2020

The Grand Chamber rendered two judgments on the basis of the three opinions of Advocate General Campos Sánchez–Bordona. These complex and technical judgments both require a careful analysis.

5.1. *Applicable law*

Regarding the scope of the e-Privacy Directive, the Grand Chamber first ruled on the basis of detailed reasons that the Directive is applicable to national legislation requiring

[24] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 [2020] para 104.
[25] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 [2020] para 111.
[26] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 [2020] para 60.
[27] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 [2020] paras 145 and 146.
[28] Case C-520/18.
[29] Opinion of Advocate General Campos Sánchez-Bordona in Case C-520/18 [2020] para 155(1).
[30] Opinion of Advocate General Campos Sánchez-Bordona in Case C-520/18 [2020] para 125.
[31] Opinion of Advocate General Campos Sánchez-Bordona in Case C-520/18 [2020] para 126.
[32] Case C-623/17.
[33] Opinion of Advocate General Campos Sánchez-Bordona in Case C-623/17 [2020] para 45.

providers of electronic communications services to carry out personal data processing operations such as its transmission to public authorities or its retention for the purposes of safeguarding national security and combating crime.[34] In addition, the Grand Chamber reiterated its judgment in the *Tele2 Sverige and Watson* case about the disproportionate nature of general and indiscriminate retention of both traffic and location data. The Grand Chamber however clarified inter alia the *scope of powers* conferred on Member States by this Directive in the area of retention of such data for the above-mentioned purposes.

The Grand Chamber clarified the applicability of the e-Privacy Directive in these four cases. Nine Member States, which submitted written observations to the Grand Chamber, expressed inconsistent opinions on the matter.[35] They contended inter alia that the Directive does not apply to the national legislation at issue since the purpose of this legislation is to safeguard national security which is the sole responsibility of Member States as shown by in particular Article 4(2) of the Treaty on EU. The Grand Chamber however considered that *national legislation which requires providers of electronic communications services to retain both traffic and location data or to forward this data to the national security and intelligence authorities for this purpose falls within the scope of this Directive*.[36]

Before any consideration of the substance, the Grand Chamber interpreted the context and objectives pursued by the e-Privacy Directive[37] the purpose of which is the effective implementation of the right to respect for private life and the protection of personal data set out in Articles 7 and 8 of the Charter.[38] This effective implementation of fundamental rights requires the regulation of both the process and storage of traffic data by providers of electronic communications services.[39] In adopting the e-Privacy Directive, the EU legislature thus gave concrete expression to these two rights "so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise."[40]

5.2. *The control of proportionality by the Grand Chamber*

The Grand Chamber then reiterated that Article 15(1) and (3) of the e-Privacy Directive does not permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and the related data and to the prohibition on storage of such data to become the rule.[41] This means that the e-Privacy Directive *does not authorize Member States to adopt*, inter alia *for the purposes of national security, legislative measures intended to restrict the scope of rights and obligations provided for in this directive, in particular the obligation to ensure the confidentiality of communications and traffic data set out in Article 5(1) of the e-Privacy Directive, unless such measures comply with general principles of EU law including the principle of proportionality and the fundamental rights guaranteed by Article 7 on respect for private life, Article 8 on protection of personal data, Article 11 on freedom of expression and Article 52(1) on the principle of proportionality of the Charter*.[42] Given the intrusive nature of both traffic and location data, their mere detention interferes, in itself, with Articles 7 and 8 of the Charter, irrespective of their subsequent use.[43]

Article 15(1) of the e-Privacy Directive "reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society".[44]

To satisfy the requirement of proportionality, the legislation of a Member State must lay down in any case and regardless of the seriousness of the interference the following guarantees: "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. This legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.[45] The need for such safeguards is all the greater where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake".[46]

5.3. *Preventive retention of both traffic and location data for the purpose of safeguarding national security*

The Grand Chamber followed the opinion of Advocate General Campos Sánchez–Bordona[47] and found that terrorist activities directly threaten society, the population or the State

[34] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 87 to 104; C-623/17 *Privacy International* [2020] paras 30 to 49.
[35] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 89.
[36] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 104; C-623/17 *Privacy International* [2020] para 49.
[37] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 105.
[38] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 106.
[39] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 106 to 108.
[40] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 109.
[41] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 111.
[42] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 113.
[43] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 115 and 116.
[44] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 120.
[45] C-623/17 *Privacy International* [2020] para 68. See also Case C-746/18 *Prokuratuur* [2021] para 48.
[46] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 132. See also Case C-746/18 *Prokuratuur* [2021] para 48.
[47] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 [2020] para 60.

itself and therefore constitute a serious threat to national security.[48] The Grand Chamber examined "the objective of safeguarding national security"[49] in light of the e-Privacy Directive for the first time. National security remains the sole responsibility of each Member State, pursuant to Article 4(2) of the Treaty on EU.[50] The Grand Chamber found that this objective is more important than those listed in Article 15(1) of the e-Privacy Directive and may justify "measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives."[51] That is the reason why Article 15(1) of the e-Privacy Directive does not, in principle, preclude a legislative measure taken on the basis of this objective which permits the competent authorities to order providers of electronic communications services to retain both traffic and location data of all users of electronic communications systems. The Grand Chamber established a connection between the indiscriminate retention of personal data and the prevention of a threat to national security.[52]

This measure must however be taken "for a limited period of time" and "as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat […] to national security which is shown to be genuine and present or foreseeable."[53] In other words, the preventive retention of personal data must "be limited in time to what is strictly necessary"[54] and "limited to situations in which there is a serious threat to national security".[55] The measure must also "be subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed."[56]

Data retention is thus authorised if it is proportionate to the objective of safeguarding national security and if it provides sufficient guarantees.

In this context, the Grand Chamber held in the *Privacy International* judgment that the e-Privacy Directive read in light of the Charter *precludes national legislation which requires providers of electronic communications services to carry out the general and indiscriminate transmission of both data and location data to the security and intelligence agencies*, i.e. *Government Communications Headquarters (GCHQ), Security Service (MI5) and Secret Intelligence Service (MI6), for the purpose of safeguarding national security*.[57]

5.4. *Preventive retention of both traffic and location data for the purposes of combating crime and safeguarding public security*

In the *La Quadrature du Net and Others* and *Ordre des barreaux francophones et germanophone and Others* judgment, the Grand Chamber reiterated that if a State bases itself on the objective of preventing, investigating, detecting and prosecuting criminal offences "only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights […] such as the interference entailed by the retention of traffic and location data."[58] A general and indiscriminate retention however "exceeds the limits of what is strictly necessary".[59] By reading the e-Privacy Directive in light of Article 4(2) of the Treaty on EU,[60] the Grand Chamber showed that it duly took into account the exclusive responsibility of Member States to safeguard national security but that the obligation to comply with fundamental rights including the protection of personal data applies to the exercise of such responsibility. In addition, a general and indiscriminate retention is not justified since it affects all persons for the sole objective albeit important of combating serious crime and the preventing threats to public security.[61]

The Grand Chamber found that the Directive *precludes legislative measures which require providers of electronic communications services to carry out the general and indiscriminate retention of both traffic and location data as a preventive measure* to safeguard national security and combat crime. These obligations to forward and to retain such data in a general and indiscriminate way constitute *particularly serious interferences with the fundamental rights guaranteed by the Charter* where there is no link between the conduct of the persons whose data is affected and the objective pursued by the legislation at issue.[62]

Legislation may however permit, as a preventive measure, the targeted retention of both traffic and location data provided that such retention is limited to what is strictly necessary regarding "the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted".[63] The Grand Chamber provided the example of "persons who have been identified beforehand, in the course of the applicable national procedures

[48] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 135, 181 and 182; Case C-623/17 *Privacy International* [2020] para 74.
[49] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 137.
[50] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 135.
[51] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 136. See also C-623/17 *Privacy International* [2020] para 75.
[52] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 137 *in fine*.
[53] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 137.
[54] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 138.
[55] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 139.
[56] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 139 *in fine*.
[57] C-623/17 *Privacy International* [2020] paras 82 and 83(2).
[58] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 140. See also Case C-746/18 *Prokuratuur* [2021] para 33.
[59] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 141; Case C-623/17 *Privacy International* [2020] para 81.
[60] C-623/17 *Privacy International* [2020] paras 81 and 82.
[61] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 142 and 143; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* [2015] paras 105 and 107.
[62] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 143 and 145.
[63] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 147.

and on the basis of objective evidence, as posing a threat to public or national security in the Member State concerned" or limits based on "a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences".[64]

5.5. *Preventive retention of IP addresses and data relating to civil identity for the purposes of combating crime and safeguarding public security*

Unlike both traffic and location data, the Grand Chamber considered proportionate a legislative measure which requires providers of electronic communications services, without imposing a specific time limit, to retain data relating to the civil identity of all users of electronic communications systems for the purposes of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security. The seriousness of the offense or threat is an irrelevant consideration. Merely knowing the identity of users does not seriously interfere with their rights.

IP addresses may however disclose information inferred from the browsing history of a user. Their retention thus seriously interferes with the fundamental rights of the user.[65] Given this seriousness, only their retention to combat serious crime, to prevent serious threats to public security and to safeguard national security may justify such interference provided the period of retention complies with the principle of strict necessity in light of the objective pursued.[66]

5.6. *Expedited retention of traffic and location data for the purpose of combating serious crime*

Situations may arise in which it becomes necessary to retain both traffic and location data after statutory time periods have ended to shed light on serious criminal offences or acts adversely affecting national security. This is the case both in situations where such offences or acts have already been established and where they may reasonably be suspected after an objective examination of all relevant circumstances.[67] Member States may then adopt a legislation pursuant to Article 15(1) of the e-Privacy Directive which instructs providers of electronic communications services to retain both traffic and location data for a specified period of time.[68] In light of the serious interference with fundamental rights to the respect for private life and the protection of personal data, only action to combat serious crime and – *a fortiori* – the safeguarding of national security are such as to justify such interference.[69] The duration of the expedited retention must be limited to what is strictly necessary although it may be extended where the circumstances and the objective pursued by the measure justify doing so.[70] Regarding persons whose data is subject to expedited retention, the measure may be extended from data relating to suspects to both traffic and location data about the victim, his or her social or professional circle, or even specified geographical areas, such as the place where the offense or act was committed or prepared.[71]

5.7. *Automated analysis of both traffic and location data*

As a preliminary point, the Grand Chamber specified that the relevant data were personal data since all persons whose data has been the subject of automatic analysis were likely to be identified.[72] As a matter of fact, data subjects must be notified so that they can duly exercise their fundamental rights to the respect for private life, the protection of personal data and an effective remedy before a tribunal if this notification is not "liable to jeopardize the tasks for which those authorities are responsible".[73]

In this case, the automated analysis corresponds, in essence, to a screening of all the retained traffic and location data carried out by those providers, independently of "the subsequent collection of data relating to the persons identified following that automated analysis".[74] Such analysis of all relevant data by itself is therefore a serious interference with fundamental rights which must comply with requirements of proportionality. It must thus be provided for by law[75] which sets out identical guarantees to those applying to the data retention generally[76] and both substantive and procedural conditions specifically.[77]

The Grand Chamber specified that such an analysis may only be implemented when "facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary."[78]

The decision authorizing automated analysis must also "be subject to effective review, either by a court or by an indepen-

[64] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 150.
[65] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 153.
[66] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 154 to 156.
[67] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 161.
[68] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 163.
[69] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 164.
[70] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 164.
[71] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 165.
[72] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 171.
[73] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 190 and 191.
[74] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 172.
[75] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 175.
[76] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 132.
[77] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 176. See also Case C-746/18 *Prokuratuur* [2021] para 49.
[78] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 177. See also *ibidem* para 178.

dent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed."[79]

The algorithm must be based on specific and reliable pre-established models and criteria[80] and not on sensitive data in isolation.[81] A regular re-examination of such models and criteria should be undertaken to ensure their reliability.[82]

Last, automated analyses must be subject to re-examination by a person before an individual measure adversely affecting the relevant persons is adopted[83] *inter alia* to avoid false positives.

5.8. *Real-time collection of traffic and location data*

As for "regular" traffic and location data,[84] real-time traffic and location data are personal data. Data subjects must be notified about the processing in case where the notification does not jeopardize its purpose.[85] Real-time collection of both traffic and location data allows to individually monitor a data subject and people around him or her if need be for the sole purpose of preventing terrorism. As data retention, it seriously interferes with fundamental rights to the respect for private life and protection of personal data and possibly with the exercise of freedom of expression.[86] The Grand Chamber emphasised the risk of profiling.[87] It held that national legislation authorizing real-time collection derogates from the obligation of principle to ensure the confidentiality of electronic communications and related data established in Article 5 of the e-Privacy Directive.[88] Given the objective of preventing terrorism, the Grand Chamber found that implementing this measure was justified "only in respect of persons with respect to whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities."[89]

The Grand Chamber specified that the decision authorizing the real-time collection must be based on both objective and non-discriminatory criteria provided for in the national legislation which must define the circumstances and conditions under which such collection may be authorised and the persons who may be subject to such collection.[90] The practical implementation of the decision must "be subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding".[91]

5.9. *General and indiscriminate retention of data by providers of access to online public communication services and hosting service providers*

Directive 2000/31/EC of 8 June 2000 on electronic commerce does not apply to the protection of the confidentiality of communications and personal data[92] which must be assessed on the basis of the e-Privacy Directive or GDPR, as appropriate.[93] The e-Privacy Directive applies to Internet access services and to electronic communications services provided they consist wholly or mainly in the conveyance of signals on electronic communications networks. The Grand Chamber similarly interpreted Article 23(1) of the GDPR read in light of Articles 7, 8, 11 and 52(1) of the Charter as precluding national legislation which requires providers of access to on-line public communication services and hosts service providers to generally and indiscriminately retain inter alia personal data relating to these services.[94]

The Grand Chamber however set out three requirements to this preclusion where Member States may derogate from the general confidentiality requirements set out by the Directive for the purposes of safeguarding national security, combatting serious criminality and preventing serious threats against public security, *i.e.*:

(1) rules outlining these derogations must be clear and precise,
(2) applicable substantive and procedural conditions must be complied with and
(3) the persons concerned must have effective safeguards against the risks of abuse.

First, the Grand Chamber added that the e-Privacy Directive read in light of the Charter does not preclude legislative measures which allow recourse to the **targeted retention, limited in time to what is strictly necessary, of both traffic and location data. The latter must be limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion**.

Second, this Directive likewise does not preclude legislative measures which provide for the general and indiscriminate retention of IP addresses assigned to the source of

[79] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 179.
[80] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 180.
[81] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 181.
[82] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 182.
[83] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 182.
[84] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 171.
[85] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 190 and 191.
[86] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 184 to 187.
[87] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 184. Regarding IP addresses, see *ibidem*, para 153.
[88] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 186. Regarding national legislation authorising the automated analysis of both traffic and location data, see *ibidem*, para 173.
[89] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 188.
[90] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 189.
[91] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 189.
[92] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 197 to 199.
[93] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 200 and 201.
[94] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 207 to 212.

a communication provided that the retention period is **limited to what is strictly necessary** or measures which provide for such retention of data relating to the civil identity of users of means of electronic communication. In the latter case, Member States are not required to limit the retention period.

Third, this Directive does not preclude a legislative measure which allows recourse to the expedited retention of data available to service providers where **situations arise in which it becomes necessary to retain this data beyond statutory data retention periods to shed light on serious criminal offences or attacks on national security**, where such offences or attacks have already been established or where their existence may reasonably be suspected.

Fourth, the Grand Chamber ruled that the e-Privacy Directive read in light of the Charter **does not preclude national legislation which requires providers of electronic communications services to have recourse to real-time collection**, inter alia, **of both traffic and location data**, where:

(1) a Member State is facing a serious, genuine and present or foreseeable threat to national security,
(2) this collection is **limited to persons in respect of whom there is a valid reason to suspect that they are involved** in one way or another **in terrorist activities** and
(3) this collection is subject to a **prior review carried out either by a court or by an independent administrative body whose decision is legally binding**, to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In urgent cases, the review must take place promptly.[95]

The legally binding nature of the decision to be rendered by either a court or an independent administrative body represents a major development.

5.10. *Powers of domestic courts*

An ultimate question was posed to the Grand Chamber to ascertain whether a national court may apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality that it is bound to make under this law in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, pursuing the objectives of safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data, owing to the fact that this legislation is incompatible with Article 15(1) of the e-Privacy Directive read in light of Articles 7, 8, 11 and 52(1) of the Charter.[96]

In light of the primacy principle,[97] the Grand Chamber reiterated that national courts must give full effect to EU law "if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means".[98] The Grand Chamber found that domestic courts **may not apply a provision of national law empowering them to limit** the temporal effects of a declaration of illegality that they are bound to make under this law in respect of a national legislation **which imposes** on providers of electronic communications services a general and indiscriminate retention **of traffic and location data which is incompatible with the e-Privacy Directive** read in light of the Charter.[99]

As EU law currently stands, the Grand Chamber reiterated that **it is for national law alone to determine the rules relating to the admissibility and assessment of information and evidence obtained by the retention of data in breach of EU law in criminal proceedings against persons suspected of having committed serious criminal offences**. The Grand Chamber however specified that the e-Privacy Directive interpreted in light of the principle of effectiveness requires national criminal courts to "disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact."[100]

6. Comments

Regarding the applicable procedure, the British Investigatory Powers Tribunal, the French Council of State and the Belgian Constitutional Court are now tasked with disposing of the four cases in accordance with the two judgments of the Grand Chamber which legally bind them.

6.1. *Distinction between national security and information collected by private operators for commercial purposes*

In the two judgments, the Grand Chamber confirmed the distinction drawn in the e-Privacy Directive between national security and information collected by private operators for commercial purposes. Article 4(2) *in fine* of the Treaty on EU provides that "national security remains the sole responsibility of each Member State."

[95] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 192.
[96] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 213.
[97] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 214
[98] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 215.
[99] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 216 to 220.
[100] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 227. See also *ibidem* paras 221 to 226; Case C-746/18 *Prokuratuur* [2021] paras 41 to 44.

This provision is reflected in the *exception to scope* under Article 1(3) of the e-Privacy Directive which does reserve national security, *i.e.* State security, to Member States. Article 4(2) of the Treaty on EU however excludes from EU law only the activities that intelligence agencies carry out *themselves*, exercising *sovereign authority*. In contrast, EU law applies to information collected by *private operators for commercial purposes*: requirements laid down in Article 15(1) of the e-Privacy Directive apply when it is *then* accessed for intelligence purposes.

6.2. Legal, operational and technical implications of the judgments

The Grand Chamber reiterated its *Tele2 Sverige and Watson* judgment in which it ruled that Article 15(1) of the e-Privacy Directive read in light of Articles 7, 8, 11 and 52(1) of the Charter 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.[101]

The Grand Chamber however set out an exhaustive number of exceptions in specific situations which deal with national security, public defence and security or crime prevention, investigation, detection and prosecution. The Grand Chamber emphasised that these exceptions can never become the rule.

Regarding the objective of safeguarding national security, the primary interest in protecting the essential functions of the State and the fundamental interests of society is a legitimate purpose to retain data. The general and indiscriminate retention of both traffic and location data for national security reasons is however permissible only if there is evidence of a serious, genuine and present or foreseeable threat to national security. In addition, the retention period of the data can be extended if the threat persists. Decisions instructing providers of electronic services to retain data must be subject to effective review by a court or by an independent administrative body whose decision is legally binding. Regarding the objectives of safeguarding national security, combating serious crime and safeguarding public security, the Grand Chamber also reiterated the notion of targeted retention. It however found that targeted retention does not apply to the retention of two types of data, *i.e.* the IP address of the source of a communication and civil identity data. The Grand Chamber generally displayed flexibility to retain these two categories of data, depending on the purposes pursued. First, the Grand Chamber specifically allowed the general and indiscriminate retention of source IP addresses for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security provided that the period of retention is limited in time. Access to data must always be subject to appropriate procedural and substantive safeguards. Second, the Grand Chamber allowed the general and indiscriminate retention of civil identity data for the purposes of safeguarding national security, combating crime and safeguarding public security without specifying any period of retention.

In the *La Quadrature du Net and Others* judgment, the Grand Chamber referred to the concept of expedited retention[102] that it has however not clearly defined and explained. This concept needs to be distinguished from that of expedited preservation[103] that the Grand Chamber also mentioned in its judgment.

6.3. Definition of serious crime

The Grand Chamber considered that "particularly serious child pornography offences, such as the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1)"[104] should be legally characterised as serious crime.[105] The Grand Chamber thus contributed to solve the issues raised in its *Tele2 Sverige and Watson* judgment about the seriousness of a crime[106] as a requirement to retain both traffic and location data[107] and to access by competent national authorities thereto.[108]

Although Member States exercise discretion in defining serious crimes which justify access to retained data in their domestic law, the notion of serious crime should become an autonomous concept of EU law. The exhaustive list of ten "areas of crimes" set out in Article 83(1) of the TFEU[109] which include the sexual exploitation of children may provide guidance in this respect.[110] These ten areas of crime should meet the two cumulative and undefined requirements of "particularly serious crimes" and "cross-border dimension" resulting from three alternative criteria, *i.e.* "nature or impact of such offences or from a special need to combat them on a common basis."[111]

---

[101] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* [2015], disposition, para 1.

[102] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] paras 163 to 165 and 168.

[103] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 162.

[104] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 154.

[105] Joined Cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 156.

[106] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* [2016] paras 102, 103, 106, 108, 110, 111, 114, 115, 118, 119, 125 and 134(2).

[107] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* [2016] para 102.

[108] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* [2016] para 134(2).

[109] "[T]errorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime."

[110] See Xavier Tracol, "*Ministerio Fiscal*: Access of Public Authorities to Personal Data Retained by Providers of Electronic Communications Services", *European Data Protection Law Review*, 2019, Volume 5, Issue 1, p. 134.

[111] Perrine Simon, "The Criminalisation Power of the European Union after Lisbon and the Principle of Democratic Legitimacy",

6.4. *Fundamental right to security*

The Grand Chamber found that "Article 6 of the Charter cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences."[112] The French Council of State had relied on the right to security protected by Article 6 of the Charter as a factor capable of justifying the imposition of the obligation to retain traffic data that national authorities impose on providers of electronic communications services.[113] The Commission submitted that this reliance on Article 6 of the Charter may be misplaced and that this "provision is to be interpreted as meaning that it is capable of 'imposing on the Union a positive obligation to adopt measures aimed at protecting persons against criminal acts'."[114] Advocate General Campos Sánchez-Bordona expressed his agreement with the Commission on this specific matter and contended that the "security guaranteed by that article of the Charter is not synonymous with public security."[115]

This finding of the Grand Chamber, the opinion of the Advocate General and written observations of the Commission about the scope of Article 6 of the Charter are all legally correct. The explanations on this provision specify that "[t]he rights in Article 6 are the rights guaranteed by Article 5 of the ECHR, and in accordance with Article 52(3) of the Charter, they have the same meaning and scope."[116] In the judgment of 15 February 2016 in the *J.N.* case, the Grand Chamber confirmed that "the explanations relating to Article 6 of the Charter […] make clear that the rights laid down in Article 6 of the Charter correspond to those guaranteed by Article 5 of the ECHR"[117] on the right to liberty and security. This interpretation clearly shows that the scope of Article of the Charter is restricted to both criminal procedural law and administrative detention including deprivation of liberty, prohibition of arbitrary detention, immigration law and asylum law as well as detention pursuant to a European Arrest Warrant.[118] As Advocate General Campos Sánchez-Bordona pointed out, "[i]t is apparent from reading Article 5 of the ECHR that the 'security' it protects is strictly personal security, in the sense of a guarantee of the right to physical freedom from arbitrary arrest or detention. In short, it is an assurance that nobody can be deprived of his or her liberty save in the cases and in accordance with the requirements and procedures prescribed by law."[119]

Article 6 of the Charter is however not relevant to the fight against serious crime.[120] As noted in a document of the LIBE committee,[121] the Grand Chamber itself however created some confusion by unclearly referring to this provision in both the *Digital Rights* judgment[122] and opinion 1/15.[123] In *La Quadrature du Net and Others* judgment, the Grand Chamber finally corrected its own legally erroneous reliance on Article 6 of the Charter in the *Digital Rights* judgment and opinion 1/15.

It is however regrettable that the Grand Chamber elected to implicitly depart from its two earlier decisions that it has not mentioned. Explicitly departing from them would have provided a welcome clarity and legal certainty about the applicable law. An implicit departure from earlier decisions is conversely a recipe for confusion. This situation reflects the unwillingness of the Grand Chamber to clearly recognize its departure from its own earlier decisions.

6.5. *Recommendations of the European Data Protection Board on European Essential Guarantees*

On 10 November 2020, the European Data Protection Board (EDPB) adopted Recommendations 02/2020[124] on the European Essential Guarantees (EEG) for surveillance measures. This document is an update of the previous WP 29 Working document on the EEG[125] to take into account the *Schrems* II,[126]

New Journal of European Criminal Law, 2012, Volume 3, Issue 3-4, p. 247 and 248.

[112] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* [2020] para 125 *in fine*.

[113] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases C-511/18 and C-512/18 [2020] paras 94 and 95.

[114] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases C-511/18 and C-512/18 [2020] para 96.

[115] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases C-511/18 and C-512/18 [2020] para 97.

[116] Published in *Official Journal* C 303 of 14 December 2007, p. 19.

[117] Case C-601/15 *J.N.* v. *Staatssecretaris van Veiligheid en Justitie* [2016] para 45.

[118] See Daniel Wilsher, "Article 6", *The EU Charter of Fundamental Rights*, Steve Peers *et al.* (eds), Hart Publishing, Oxford and Portland, 2014, pp. 121–151.

[119] Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases 511/18 and C-512/18 [2020] para 98.

[120] See Xavier Tracol, Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada, *Computer Law & Security Review*, Volume 34, issue 4, August 2018, p. 840, section 6.3.

[121] 6th Working Document (C) on the Proposal for a Regulation on European Production and PreservationOrders for electronic evidence in criminal matters (2018/0108 (COD)) – Safeguards and remedies, PE637.469v01-00, 1 April 2019, available at https://www.europarl.europa.eu/doceo/document/LIBE-DT-637469_EN.pdf?redirect, p. 8, footnote 20.

[122] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] para 42 *in fine*. See Xavier Tracol, "Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC), thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it", *Computer Law & Security Review*, Volume 30, issue 6, November 2014, pp. 736–746.

[123] Opinion 1/15 [2017] para 149. See Xavier Tracol, "Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada", *Computer Law & Security Review*, Volume 34, issue 4, August 2018, pp. 830–842.

[124] Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

[125] Article 29 Working Party working document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

[126] Case C-311/18 *Data Protection Commissioner* v. *Facebook Ireland Ltd and Maximillian Schrems* [2020]. See Xavier Tracol, "'*Schrems* II': the

Privacy International and La Quadrature du Net and Others judgments. EEG concern guarantees to be taken into account when assessing the interference stemming from surveillance measures by national security or law enforcement authorities of third States with the two fundamental rights to privacy and to the protection of personal data when transferring personal data. They are part of the overall assessment made by the Commission about the adequacy of the legal system of third States but should be distinguished from this assessment as such.

The four EEG are the following:

A processing should be based on clear, precise and accessible rules;
B necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
C an independent oversight mechanism should exist;
D effective remedies need to be available to the individual.

6.6. *Draft e-Privacy Regulation*

On 14 February 2019, the Belgian, Estonian, Dutch, Austrian, Latvian, Danish, French and British delegations to Council issued a non-paper, considering that the e-Privacy Regulation should allow for "the possibility for existing and future data retention regimes".[127] They submitted that a new Article 7(2a) should be added to the draft e-Privacy Regulation which would provide that "Union or national law may impose an obligation on the providers of the electronic communication services to retain metadata for a longer period of time, where such an obligation respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences".[128]

Concerns have also been raised over the version of the draft e-Privacy Regulation of the Portuguese presidency of Council. On 25 January 2021, a cross-section of digital rights groups led by EDRi sent a letter to the telecoms working party of Council, challenging the exception for national security and public order in then Article 2.2(a) of the draft e-Privacy Regulation. It contended that this provision aimed at bypassing the case law of the Court of Justice on data retention. It accordingly requested the telecoms working party of Council to reject this provision.[129]

On 10 February 2021, the Portuguese presidency of Council made amendments to the text on data retention and data processing for national security processes.[130] Recital 26 of the draft e-Privacy Regulation now provides *inter alia* that "this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications, including by requiring providers to enable and assist competent authorities in carrying out lawful interceptions, or take other measures, such as legislative measures providing for the retention of data for a limited period of time, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights."[131]

Article 7(4) of the draft e-Privacy Regulation provides that "Union or Member State law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists." This provision reflects new Article 7(2a) proposed by the eight delegations to Council in their non-paper of 14 February 2019 and the wishes of the French delegation expressed in a working document of 12 January 2021.[132] On 9 March 2021, the EDPB adopted strongly worded statement 03/2021 on the ePrivacy Regulation. The Board expressed concerns about processing and retention of electronic communication data for the purposes of law enforcement and safeguarding national security. It stated that "providing a legal basis for anything else than targeted retention for the purposes of law enforcement and safeguarding national security is not allowed under the Charter, and would anyhow need to be subject to strict temporal and material limitations as well as review by a Court or by an independent authority."[133]

6.7. *Draft adequacy decision based on the law enforcement directive about the UK*

On 19 February 2021, the Commission launched the process towards the adoption of an adequacy decision for transfers of personal data to the UK on the basis for the first time on the Law Enforcement Directive. The Commission found that the UK ensures an essentially equivalent level of protection

return of the Privacy Shield", *Computer Law & Security Review*, Volume 39, November 2020, pp. 1–11.

[127] Interinstitutional File: 2017/0003(COD), document 6358/19, available at https://www.accessnow.org/cms/assets/uploads/2019/05/ePrivacy-Access-to-Document.pdf, p. 2.

[128] Interinstitutional File: 2017/0003(COD), document 6358/19, available at https://www.accessnow.org/cms/assets/uploads/2019/05/ePrivacy-Access-to-Document.pdf, p. 5.

[129] Available at https://www.euractiv.com/wp-content/uploads/sites/2/2021/01/20210125-ePrivacy-letter-EDRi.pdf

[130] Available at https://twitter.com/SamuelStolton/status/1359482943224369158

[131] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Interinstitutional File: 2017/0003(COD), document 6087/21, 10 February 2021, available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

[132] ePrivacy Regulation: FR comments (doc. 5008/21), WK 390/2021 INIT.

[133] Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_032021_eprivacy_regulation_en.pdf

to the one guaranteed under the Directive.[134] On 5 February 2021, the LIBE committee issued an opinion strongly encouraging the Commission to take into account the case law of the Court of Justice such as the *Privacy International* judgment in its assessment.[135] The LIBE Committee therefore called "on the Commission to ensure that the UK has resolved the problems identified in this opinion prior to considering UK data protection law adequate in line with Union law"[136] as interpreted by the Court of Justice. The LIBE Committee specifically referred to the *Privacy International* judgment again.[137]

The judgment of the Grand Chamber in the *Privacy International* case is however surprisingly not mentioned in the draft adequacy decision. Now that the UK has left the EU, the ECHR provides the only European oversight mechanism over surveillance in the UK pursuant to the British Investigatory Powers Act.

On 3 October 2019, the US and the UK signed a data transfer agreement on "Access to Electronic Data for the Purpose of Countering Serious Crime" about data sharing between their national security agencies.[138] By letter of 15 June 2020 to members of Parliament, the Chair of the EDPB considered that "the agreement concluded between the UK and the US will have to be taken into account by the European Commission in its overall assessment of the level of protection of personal data in the UK, in particular as regards the requirement to ensure continuity of protection in case of 'onward transfers' from the UK to another third country."[139] The draft adequacy decision of the Commission based on the Law Enforcement Directive does however not mention this agreement either.

The EDPB has been requested to provide comments to the Commission on the draft adequacy decision by 19 April 2021. It can be expected to request amendments on the above-mentioned issues.

7. Conclusion

In these two landmark judgments, the Grand Chamber endeavoured to reach the proper balance[140] between the requirements to fight against serious crime including terrorism and to safeguard national security and the requirements to respect private life and protect personal metadata. The Grand Chamber has already relied on them in its *Prokuratuur* judgment on the interpretation of the Estonian data retention legislation about requirements for access by investigating authorities to data in electronic communications.[141] These two judgments will also have implications on other pending cases about the retention of personal data such as the request for a preliminary ruling by the Federal Administrative Court of Germany to assess the lawfulness of the 2015 German law on data retention.[142]

Declaration of Competing Interest

None.

Data availability

No data was used for the research described in the article.

[134] Available at https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf

[135] Available at https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_EN.pdf, para 12.

[136] *Ibidem*, para 13.

[137] *Ibidem*, footnote 6.

[138] US Department of Justice, "U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online", 3 October 2019, available at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists and https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

[139] Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf

[140] Case C-623/17 *Privacy International* para 67; Joined cases 511/18, C-512/18 and 520/18 *La Quadrature du Net and Others* [2020] para 130. See also Case C-746/18 *Prokuratuur* [2021] para 38.

[141] Case C-746/18 *Prokuratuur* [2021] paras 29 to 38, 41 to 44 and 48 to 51.

[142] See eucrim 3/2019, p. 176.