COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

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

Xavier Tracol *

Data Protection Service, EUROJUST, The Hague, The Netherlands

Keywords:
European Court of Justice
Tele2 Sverige and Watson
Digital Rights Ireland and Seitlinger
Article 15(1) of e-privacy Directive 2002/58/EC of 12 July 2002
Telecommunications metadata
Retention of personal data
Legal validity
Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights
Access to data
Prior review by a court or independent administrative authority

A B S T R A C T

As a follow up to the *Digital Rights* judgment of 8 April 2014 in which the Grand Chamber invalidated the data retention directive, the Administrative Court of Appeal in Stockholm and the Court of Appeal in London both referred questions to the Court of Justice for a preliminary ruling. On 21 December 2016, the Grand Chamber rendered a landmark judgment in which it interpreted Article 15(1) of e-privacy directive 2002/58/EC dated 12 July 2002 in light of Article 7 on the right to privacy, Article 8 on the protection of personal data, Article 11 on freedom of expression and Article 52(1) on the principle of proportionality of the Charter of Fundamental Rights. The Grand Chamber ruled that EU law does not allow a general and indiscriminate retention of all traffic and location data. It also ruled that access of competent national authorities to retained data must be restricted solely to fighting serious crime and subject to prior review by a court or an independent administrative authority.

"*Justice raises her voice, but she has difficulty making herself heard amid the tumult of the passions.*"

Charles-Louis de Sécondat, Baron of Brède and of Montesquiou a/k/a Montesquieu, *Persian Letters*, Letter 81, Usbek to Rhedi, in Venice, 1721.

1. Introduction

In its judgment of 8 April 2014 in *Digital Rights*, the Grand Chamber held data retention directive 2006/24/EC to be invalid *ex tunc* since it seriously interfered with the fundamental rights

* P.O. Box 16183, 2500 BD, The Hague, The Netherlands.
E-mail address: xtracol@eurojust.europa.eu.

http://dx.doi.org/10.1016/j.clsr.2017.05.003

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

to respect for private life and protection of personal data and exceeded the limits of the principle of proportionality which are provided for in the Charter of Fundamental Rights. A harmonised legal framework regulating the retention of data has consequently been unavailable at EU level since the date of this judgment. The latter has however not impacted on the legal validity of national laws adopted by Member States to enact the invalidated directive.

The two cases at hand of *Tele2 Sverige* and *Watson* precisely dealt with national laws which enacted the invalidated directive. The landmark judgment of the Grand Chamber accordingly focused on the results and implications of its earlier judgment invalidating the data retention directive for the legislative reality in Member States as well as on the compatibility of national data retention measures with fundamental rights set out in the Charter.

2. Relevant law

Article 15(1) of e-privacy directive 2002/58/EC 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."

3. Procedural background of the cases

The day after the judgment was handed down, Tele2 Sverige which is a provider of electronic communications services notified the Swedish Post and Telecommunications Authority ("PTS") of its decision to cease retaining the data referred to in Chapter 6 of Law 2003:389 on electronic communications ("the LEK") from 14 April 2014. Tele2 Sverige also proposed to delete the data which had been retained until then in accordance with this chapter.[1] Tele2 Sverige had concluded that the Swedish legislation enacting then invalidated data retention directive 2006/24 was not in conformity with the Charter.[2]

By decision of 29 April 2015, the Administrative Court of Appeal in Stockholm stayed the proceedings and referred the following question to the Court of Justice for a preliminary ruling:[3]

"Is a general obligation to retain data in relation to all persons and all means of electronic communication and extending to all traffic data, without any distinction, limitation or exception being made by reference to the objective of fighting crime [. . .] compatible with Article 15(1) of Directive 2002/58, taking into account Articles 7, 8 and 52(1) of the Charter?"[4]

In the UK, the deputy leader of the Labour party, Tom Watson, Peter Brice and Geoffrey Lewis brought actions against the rules provided for in the Data Retention and Investigatory Powers Act 2014 ("DRIPA") which authorised the Home Secretary to require public telecommunications operators to retain all communications data except their content for a maximum period of 12 months. By judgment of 17 July 2015, the High Court of Justice in London ruled that the regime of the DRIPA was inconsistent with EU law in that it did not meet the requirements laid down in the *Digital Rights* judgment that it regarded as applying to the rules in the Member States on the retention of data relating to electronic communications and on access to such data.[5] The Home Secretary appealed against this judgment.

By judgment of 20 November 2015, the Court of Appeal considered that the Court of Justice had simply identified and described protections which were missing in the harmonised EU regime in the *Digital Rights* judgment.[6] The Court of Appeal requested the Court of Justice to clarify the impact of its judgment which limited both the collection of and access to data. The Court of Appeal specifically asked the Court of Justice whether the *Digital Rights* judgment and especially paragraphs 60 to 62 thereof "lay down mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of the [Charter]".[7]

The approach of the two referring courts is thus quite different since the relevant national systems of data retention substantially differ: the Swedish legislation provides for a general obligation of retention whilst the British legislation is based on the discretion of the Secretary of State for the Home Department.

In granting the expedited procedure pursuant to Article 105(1) of the Rules of Procedure of the Court, the president of the Court of Justice, Judge Koen Lenaerts, considered that the dispute in the UK was over the Secretary of State's powers "to require public telecommunications operators to retain communications data for a maximum period of 12 months, retention of the content of the communications concerned being excluded."[8] Regarding Sweden, the judge also noted that "it is clear that national legislation that permits the retention of all electronic communications data and subsequent access to that data is liable to cause serious interference with the fundamental rights laid down in Articles 7 and 8 of the Charter".[9]

The Commission and governments of 15 Member States including Sweden and the UK submitted observations. Privacy International, the Law Society and Open Rights Group intervened in the case.[10] The Council did however not intervene.

[1] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 44.
[2] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 50; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] paras 15 and 63.
[3] Regarding this decision, see Pam Storr, "Blanket Storage of Communications Data – Proportional or Not? Sweden Asks CJEU for Clarification on Data Retention", *European Data Protection Law Review*, 2015, Volume 1, Issue 3, pp. 230–235.
[4] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 55(1).
[5] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 58.
[6] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 59.
[7] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 60(1).
[8] Order of the President of the Court, Case C-698/15, 1 February 2006, para 3.
[9] Order of the President of the Court, Case C-698/15, 1 February 2006, para 10.
[10] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 57.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

A high profile hearing took place on 12 April 2016.[11] Judge Rapporteur Thomas von Danwitz was also Judge Rapporteur in the cases of *Digital Rights*[12] and *Schrems*.[13]

4. Analysis of the opinion of Advocate General Henrik Saugmandsgaard Øe dated 19 July 2016

Advocate General Saugmandsgaard Øe first identified that the questions referred to the Court concerned the compatibility of domestic "regimes establishing a general data retention obligation [. . .] with Directive 2002/58/EC and Articles 7 and 8 of the Charter".[14] He added that the Court would in particular need to clarify how its *Digital Rights* judgment was to be interpreted in the domestic context to answer those questions.[15] The Danish Advocate General started by strangely expressing his "feeling that a general data retention obligation imposed by a Member State may be compatible with the fundamental rights enshrined in EU law, provided that it is strictly circumscribed by a series of safeguards".[16] The latter turned out to form the backbone of the whole reasoning of the Advocate General.[17]

4.1. *Applicability of the Charter to general data retention obligations*

Advocate General Saugmandsgaard Øe considered that recourse by Member States to the option provided for in Article 15(1) of the directive of imposing a general data retention obligation is "subject to compliance with strict requirements"[18] which flow from this provision and the relevant provisions of the Charter read in light of the *Digital Rights* judgment.[19] He considered that "the provisions of the Charter are applicable to national measures introducing such an obligation, in accordance with Article 51(1) of the Charter".[20] Being subject to Article 15(1) of the directive, national rules are implementing EU law which entails the applicability of the Charter.

The Advocate General has surprisingly not relied on the *Pfleger* judgment of 30 April 2014[21] in which the Court of Justice found that where Member States adopt national measures as exceptions provided for by EU law to the exercise of fundamental freedoms and rights, these measures have to comply with the Charter. He argued that general data retention obligations are "a serious interference with the right to privacy, enshrined in Article 7 of the Charter, and the right to the protection of personal data guaranteed by Article 8 of the Charter."[22]

4.2. *Test of strict necessity*

Advocate General Saugmandsgaard Øe went on to detail the necessary elements of the test of "strict requirements".[23] First, he recommended that the general obligation to retain data and the accompanying guarantees must be "laid down by legislative or regulatory measures possessing the characteristics of accessibility, foreseeability and adequate protection against arbitrary interference."[24] Second, the obligation must respect the essence of the right to respect for private life and the right to the protection of personal data provided for in the Charter.[25] Third, the Advocate General noted that any interference with fundamental rights should be in the pursuit of an objective in the general interest.[26] He deemed that "the requirement of proportionality within a democratic society prevents the combating of ordinary offences and the smooth conduct of proceedings other than criminal proceedings from constituting justifications for a general data retention obligation. The considerable risks that such obligations entail outweigh the benefits they offer in combating ordinary offences and in the conduct of proceedings other than criminal proceedings."[27]

In what is arguably the main consideration of his opinion, Advocate General Saugmandsgaard Øe further deemed that solely the fight against *serious* crime is an objective in the general interest which is capable of justifying a general obligation to retain data whereas combating ordinary offences and the smooth conduct of proceedings other than criminal proceedings are not.[28] Fourth, the general obligation to retain data "must be *strictly necessary* in the fight against serious crime, which means that no other measure or combination of measures could be as effective [. . .] while at the same time interfering to a lesser extent"[29] with fundamental rights and must comply with all the safeguards set out by the Grand Chamber in the *Digital Rights* judgment regarding "access to the data, the period of retention and the protection and security of the data".[30] Last, the general obligation to retain data must be proportionate which means that the serious risks engendered by this obligation within a democratic society must not be disproportionate "to the advantages it offers in the fight against serious crime."[31]

[11] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 259.
[12] 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, December 2014, pp. 736–746.
[13] See Xavier Tracol, "'Invalidator' strikes back: The harbour has never been safe", *Computer Law & Security Review*, April 2016, Volume 32, Issue 2, p. 346.
[14] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 6.
[15] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 6.
[16] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 7.
[17] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 150, 152, 159, 195, 200–202, 204, 205, 216–221, 224, 226–228, 245, 262 and 263.
[18] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 116.
[19] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 116.
[20] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 122.
[21] Case C-390/12, para 36.
[22] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 128.
[23] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 131–248.
[24] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 153.
[25] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 159 and 160.
[26] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 184.
[27] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 172.
[28] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 173.
[29] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 263, emphasis added.
[30] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 263.
[31] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 262.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

4.3. *Respect for the essence of the fundamental right to privacy and access to communications metadata*

Advocate General Saugmandsgaard Øe reiterated that the Grand Chamber held in the *Digital Rights* judgment that "Directive 2006/24 did not adversely affect the essence of the right to privacy or of the other rights enshrined in Article 7 of the Charter, since it did not permit the acquisition of knowledge of the content of the electronic communications as such."[32] He expressed the view that this "finding could equally apply to the national regimes at issue in the main proceedings, since they also do not permit the acquisition of knowledge of the content of the electronic communications as such."[33] The Advocate General however emphasised that the risks associated with access to communications metadata "may be as great or even greater than those arising from access to the content of communications".[34] On the basis of specific examples,[35] he added that metadata "facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not."[36]

The Advocate General found that the general obligation to retain data must be strictly necessary to the fight against serious crime.[37] He did state that certain sensitive data such as data which is subject to professional privilege or makes it possible to identify the source of a journalist should be excluded from the scope of the retention obligation.[38]

4.4. *Adequate controls on geographical safeguards: retention and storage of personal data within the EU*

Advocate General Saugmandsgaard Øe's interpretation of paragraph 68 of the *Digital Rights* judgment contributes to the development of EU personal data law. In this paragraph, the Grand Chamber noted that the data retention directive did not require the data to be retained within the EU "with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security [. . .] is fully ensured."[39] The Grand Chamber thus noted this missing requirement as one of the reasons why the data retention directive did not "provide for sufficient safeguards [. . .] to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data."[40]

In his opinion, Advocate General Saugmandsgaard Øe however stated that in paragraph 68 of the *Digital Rights* judgment, the Grand Chamber "established that service providers are under an obligation to retain data"[41] within the EU. He thus turned the finding of the Grand Chamber about a missing requirement into a positive obligation and "requirement"[42] to retain data within the EU.[43]

The Advocate General considered that all the guarantees described by the Grand Chamber in paragraphs 60 to 68 of the *Digital Rights* judgment "are mandatory and consequently must accompany any general data retention obligation in order to limit the interference [with the fundamental rights] to what is strictly necessary."[44] In addition, this obligation must be proportionate, within a democratic society, to the objective of fighting serious crime.[45]

Last but not least, domestic courts bear the onus to determine, in light of all the relevant characteristics of the national regimes, whether the requirements are met and sufficient safeguards are in place for data retention.[46] Advocate General Saugmandsgaard Øe thus questionably left it to domestic courts to make their own assessment of proportionality in individual cases.

5. Analysis of the judgment of the Grand Chamber dated 21 December 2016

On 21 December 2016, the Court of Justice sitting in the Grand Chamber composed of 15 judges[47] rendered its judgment in the two joint *Tele2 Sverige* and *Watson* cases. It ruled that EU law does not allow a "general and indiscriminate retention of all traffic and location data".[48] The Grand Chamber also ruled that access of competent national authorities to retained data must be "restricted solely to fighting serious crime"[49] and "subject to prior review by a court or an independent administrative authority".[50]

5.1. *National legislation on the retention of data falls within the scope of EU law*

The Grand Chamber first considered that "the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active".[51]

[32] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 156.
[33] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 157.
[34] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 259.
[35] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 257 and 258.
[36] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 259.
[37] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 205.
[38] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 212.
[39] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 68.
[40] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 66.
[41] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 238.
[42] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 240 and 241.
[43] 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, December 2014, pp. 744 and 745.
[44] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 244.
[45] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 247.
[46] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 160, 209, 211, 215, 245 and 261.
[47] See Composition of the Grand Chamber, *Official Journal of the European Union*, C 296, 16 August 2016, p. 2.
[48] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 134(1).
[49] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 134(2).
[50] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 134(2).
[51] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 72.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

Whilst Articles 1(3) and 15(1) of the directive seem to overlap, it does not mean that matters permitted on the basis of Article 15(1) of the directive fall outside its scope since "otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein [. . .] fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met."[52] By adopting measures which are expressly excluded from the scope of EU law, States continue being paradoxically regarded as implementing EU law. The scope of the latter thus depends on the purpose of Article 15(1) of the directive.

The Grand Chamber held that retention and access both lay within the field of the directive.[53] It ruled that "a legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services, for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that directive."[54]

The Charter as interpreted by the Grand Chamber in its *Digital Rights* judgment accordingly applies to national regimes about both retention of data and access thereto by public authorities on security grounds.

5.2. *Interpretation of Article 15(1) of the directive*

The Grand Chamber noted that "as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data".[55] It noted that:

> *Under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services. As regards, in particular, the billing of services, that processing is permitted only up to 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 processed and stored must be erased or made anonymous.*[56]

In addition, recital 30 of the directive sets out the principle of data minimisation.[57] Whilst Article 15(1) of the directive permits exceptions, they must be *interpreted strictly* so that the exception does not become the rule. The latter would otherwise "be rendered largely meaningless."[58] The Grand Chamber emphasised that the list of objectives provided for in Article 15(1) of the directive is exhaustive.[59] *In fine*, this provision requires that all the measures referred to in Article 15(1) of the directive including the retention of data be in accordance with general principles of EU law. The latter encompass the Charter in light of which this provision must be interpreted.[60]

The Grand Chamber emphasised that the obligation to retain traffic data raises questions on the compatibility with Articles 7, 8 and 11 of the Charter on freedom of expression and information.[61] Contrary to the *Digital Rights* judgment,[62] the Grand Chamber emphasised that Article 15 of the directive provided further detail in the context of communications whilst recital 11 requires measures to be "'strictly' proportionate to the intended purpose".[63]

5.3. *A very far-reaching and particularly serious interference*

The scope of the judgment dealt with the Swedish legislation which "provides 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 [. . .] imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions."[64]

The Grand Chamber considered that communications metadata described in detail[65] allows "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[66] They make the profiling of data subjects possible, as observed by Advocate General Saugmandsgaard Øe in his opinion that the Grand Chamber expressly approved, which is as sensitive information as the actual content of communications. The interference by national legislation which provides for the retention of traffic and location data "in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance"[67] which are the same terms as the *Digital Rights* judgment.[68] The Grand Chamber however considered that the relevant legislation did not affect the *essence* of fundamental rights since the retention did not include the content of communications.[69] The Grand Chamber justified the different findings on freedom of expression made in this case and in the *Digital Rights* judgment by holding that the retention of traffic and location data could "have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter".[70] Accordingly, "only the objective of fighting

[52] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 73.
[53] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 76.
[54] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 78.
[55] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 85.
[56] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 86.
[57] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 87.
[58] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 89 *in fine*.
[59] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 90.
[60] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 91.
[61] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 92.
[62] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] paras 28 and 70.
[63] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 95.
[64] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 97.
[65] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 98.
[66] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 99.
[67] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 100.
[68] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 37.
[69] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 101.
[70] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 101.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

serious crime is capable of justifying such a measure".[71] Although the Grand Chamber did not cross-refer to the opinion of Advocate General Saugmandsgaard Øe, it agreed with him that the seriousness of the interference implied that the retention of communications data should be restricted to "serious crime".[72]

Even in this case, the Grand Chamber found that "while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight".[73] In line with its *Digital Rights* judgment,[74] the Grand Chamber acknowledged that the use of modern investigation techniques may contribute to this fight.

The Grand Chamber emphasised that the directive requires the retention of traffic and location data to be the exception and not the rule as in the Swedish legislation.[75] It applied the same logic as in its *Digital Rights* judgment and reiterated its essential finding that:

> *National legislation such as that at issue in the main proceedings, which covers, in a* generalised manner, *all subscribers and registered users and* all means of electronic communication *as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that* it affects all persons using electronic communication *services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore* applies 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 criminal offences. *Further,* it does not provide for any exception, *and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.*[76]

The Swedish legislation thus provides for generalised mass processing and surveillance of metadata which infringes upon the fundamental right to respect for private life[77] and is outlawed in the EU. As in the *Digital Rights* judgment,[78] the Grand Chamber noted that the Swedish legislation does not require "any relationship between the data which must be retained and a threat to public security."[79] It also noted that this legislation is not limited to retention of "(i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime".[80]

5.4. *"Targeted retention" of both traffic and location data is permitted*

The Swedish legislation "therefore exceeds 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 and Article 52(1) of the Charter."[81]

The Grand Chamber however found that:

> *Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a* preventive measure, *the* targeted *retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*[82]

Importantly, the Grand Chamber did therefore not question or challenge the appropriateness and effectiveness of targeted retention of traffic and location data which remains a lawful purpose for both preventing and fighting serious crime subject to compliance with requirements to be met by domestic law. In addition, the findings of the Grand Chamber went against the opinion of Advocate General Saugmandsgaard Øe who felt that "a general data retention obligation imposed by a Member State may be compatible with the fundamental rights enshrined in EU law, provided that it is strictly circumscribed by a series of safeguards".[83]

The Grand Chamber set out two cumulative requirements, *i.e.*, first, "clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse."[84] National data retention laws "must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary".[85] Second, the Grand Chamber observed that while "conditions may vary according to the nature of the measures

[71] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 102.
[72] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 262.
[73] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 103.
[74] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 51.
[75] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 104.
[76] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 105, emphasis added.
[77] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] paras 57 and 58; Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2014] paras 93 and 94. See Xavier Tracol, "'Invalidator' strikes back: The harbour has never been safe", *Computer Law & Security Review*, Volume 32, Issue 2, April 2016, p. 355.
[78] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 59.
[79] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 106.
[80] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 106.
[81] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 107.
[82] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 108, emphasis added.
[83] Opinion in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 7.
[84] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 109.
[85] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 109.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish *a connection between the data to be retained and the objective pursued*. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected."[86]

5.5. *Scope of data retention*

The Grand Chamber specified that "the national legislation must be *based on objective evidence* which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to fighting serious crime or to prevent a serious risk to public security."[87] The Grand Chamber accepted that a geographical criterion could be used to set limits on the basis of objective evidence that "there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."[88] The Grand Chamber thus repeatedly required that national legislation be based on objective evidence to meet the standards of proportionality and the test of strict necessity although its analysis about their meaning is far from being as detailed and structured as that of Advocate General Saugmandsgaard Øe.[89] In addition, the Grand Chamber required objective evidence for competent national authorities to consider the level of risk and prevent it if assessed as serious or high.

In contradiction to the opinion of the Advocate General,[90] the Grand Chamber found concerning the first question in *Tele2* Case C-203/15 that:

> *Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.*[91]

5.6. *Criteria for national legislation about access of national authorities to retained data*

Regarding the second question in *Tele2* Case C-203/15 and the first question in *Watson* Case C-698/15, the Grand Chamber found that the *scope of access* to retained data must be restricted to the *purpose* of "fighting serious crime".[92] As in the *Digital Rights* judgment,[93] it framed the obligation to retain data[94] and to make it accessible to national law enforcement authorities[95] as two distinct interferences with fundamental rights.

A data retention measure must "lay down *clear and precise rules* indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law."[96] Although the Grand Chamber did not expressly cross-refer to the opinion of Advocate General Saugmandsgaard Øe on the latter issue, the Advocate General made this specific point and relied on codes of practice or internal guidelines.[97] The national legislation must "lay down the *substantive and procedural conditions* governing the access of the competent national authorities to the retained data".[98]

The Grand Chamber emphasised that "the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users."[99] As Advocate General Saugmandsgaard Øe,[100] the Grand Chamber referred to the judgment of the Grand Chamber of the European Court of Human Rights ("ECHR") dated 4 December 2015 in the case of *Roman Zakharov v. Russia*.[101] Regarding the *scope of access* in relation to the *persons* whose data can be accessed, the Grand Chamber specified that:

> *Access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the* data of individuals suspected *of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.*[102]

The Grand Chamber however lowered the bar for terrorist activities: Access to the personal data of other data subjects might be granted where there is "objective evidence"[103] that the data might effectively contribute to combat them.

---

[86] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 110, emphasis added.
[87] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 111 as rectified by Order of the Grand Chamber dated 16 March 2017 in Joined Cases C-203/15 REC and C-698/15 REC, emphasis added.
[88] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 111 *in fine*.
[89] Opinion in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] paras 186–263. See also Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/34/60, 24 February 2017, p. 8, para 17.
[90] Opinion in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 116.
[91] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] paras 112 and 134(1).
[92] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 115.
[93] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] paras 34 and 35.
[94] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] paras 100 and 102.
[95] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 115.
[96] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 117, emphasis added.
[97] Opinion in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 150.
[98] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 118, emphasis added.
[99] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 119.
[100] Opinion in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 243.
[101] CE:ECHR:2015:1204JUD004714306, para 260.
[102] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 119, emphasis added.
[103] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 119.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

The Grand Chamber also followed the opinion of Advocate General Saugmandsgaard Øe[104] in requiring that "access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a *prior review* carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime".[105] The Grand Chamber did not only refer to its own *Digital Rights* judgment but also to the judgment of the ECHR in *Szabó and Vissy v. Hungary*.[106] The Grand Chamber considered that data subjects should be notified by competent national authorities that access has been granted to their own retained personal data "as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities".[107] The United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism welcomed these specific findings of the judgment.[108]

5.7. *Data location and destruction*

The Grand Chamber listed the mandatory requirements for the lawfulness of relevant data retention that it had already enumerated in its *Digital Rights* judgment, *i.e.*, the notification of data subjects so that they may exercise their right to a legal remedy, rules relating to the security and effective protection of retained data by providers of electronic communications services who must ensure "a particularly high level of protection and security by means of appropriate technical and organisational measures",[109] the retention of the latter within the territory of the EU – which raises the issue of cloud computing[110] – and "the irreversible destruction of the data at the end of the retention period".[111]

5.8. *Prior review by either a court or an independent body*

Member States must also ensure that an independent authority controls compliance with applicable rules on the protection of personal data as required by Article 8(3) of the Charter and previously noted in both the *Digital Rights* and *Schrems* judgments (strict legality scrutiny).[112] Unlike Advocate General Saugmandsgaard Øe,[113] the Grand Chamber did not specifically examine whether the safeguards that it had laid down in the *Digital Rights* judgment[114] were mandatory requirements of EU law applicable to a Member State's domestic regime for access to data retained in accordance with national legislation to comply with Articles 7 and 8 of the Charter.[115]

The Grand Chamber however considered that referring courts bear the onus "to determine whether and to what extent the national legislation at issue in the main proceedings satisfies the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as set out in paragraphs 115 to 123 of this judgment, with respect to both the access of the competent national authorities to the retained data and the protection and level of security of that data."[116]

The Grand Chamber then summed up its findings and held that Article 15(1) of the directive read in light of Articles 7, 8, 11 and Article 52(1) of the Charter

> *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.*[117]

The retention of personal data must accordingly not only be targeted but access by the authorities to retained data must be limited to the purpose of fighting against serious crime, be subject to a prior review carried out either by a court or by an independent administrative body and personal data must remain on the territory of the EU.

6. Comments

For the first time, the judgment of the Grand Chamber set EU standards about the retention of personal data for surveillance purposes that Member States need to comply with. The Grand Chamber applied Article 7 of the Charter on the respect for private life and Article 8 of the Charter on the protection

[104] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 205, 234 and 236.
[105] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 120, emphasis added.
[106] CE:ECHR:2016:0112JUD003713814.
[107] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 121.
[108] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, A/HRC/34/61, 27 January 2017, p. 12, para 34.
[109] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 122.
[110] Regarding cloud computing, 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, December 2014, p. 745; "'Invalidator' strikes back: The harbour has never been safe", *Computer Law & Security Review*, April 2016, Volume 32, Issue 2, p. 360. On 27 January 2017, an industry body of Cloud Infrastructure Services Providers operating in Europe has established and signed up to a new data protection code of conduct available at https://cispe.cloud/wp-content/uploads/2017/02/CISPE-CodeOfConduct-27012017.pdf. The code requires providers to offer customers the option to process and store personal data entirely within the European Economic Area (pp. 7 and 14).
[111] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 122.
[112] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 123.
[113] Opinion in Joined Cases C-203/15 and C-698/15 [2015] paras 221, 226, 244 and 262.
[114] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] paras 60–68.
[115] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 59(1).
[116] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 124.
[117] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 125.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

of personal data together in its analysis of the consequences of domestic measures which provide for retention of personal data[118] as it had already done in the *Google Spain* case.[119] The Grand Chamber has however clearly distinguished the application of these two different provisions in the *Digital Rights*[120] and *Schrems*[121] judgments. In the judgment rendered in the two joint Dutch immigration cases,[122] the Court of Justice also applied Article 8 of the Charter but not Article 7 of the Charter. In this case, the Grand Chamber thus regrettably blurred the different scopes of the two provisions which had however been clearly distinguished in the three *Digital Rights*, *Schrems* and joint Dutch immigration judgments.

6.1. *Legal effects of the judgment*

6.1.1. *Effect* ex tunc

The interpretation of Article 15(1) of the directive by the Grand Chamber in its judgment delivered on a reference for a preliminary ruling clarifies the meaning and scope of this provision as it must be or ought to have been understood and applied from the date when it entered into force.[123] Pursuant to Article 20 of this directive, it entered into force on the day of its publication in the *Official Journal*, i.e. 31 July 2002. The judgment of the Grand Chamber is purely declaratory with the consequence that it takes effect from this date.[124]

6.1.2. *Effect* erga omnes

The judgment of the Grand Chamber has an effect *erga omnes*. The consequences of the interpretation of Article 15(1) of the directive as well as Articles 7, 8, 11 and 52(1) of the Charter apply to the parties to the proceedings before the two referring courts, all other national courts, third parties, institutions and Member States as well as to all situations covered by these five provisions.[125]

6.2. *Plea raised* ex officio

Although the two referring courts had not asked any question about the compliance of national measures on the retention of data with Article 11 of the Charter for a preliminary ruling, the Grand Chamber examined the compatibility of the data retention obligation imposed on providers with this provision in light of "the particular importance accorded to that freedom in any democratic society."[126] It characterised this fundamental right as "one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded".[127]

The Court of Justice thus raised this plea *ex officio* for the first time concerning the substance of the case where fundamental rights set out in the Charter are involved. This precedent stands in stark contrast to the traditional reluctance of the Court of Justice to raise pleas *ex officio*.[128]

6.3. *Distinction between content and metadata*

The reasoning of the Grand Chamber that communications metadata "is no less sensitive, having regard to the right to privacy, than the actual content of communications"[129] but that the Swedish legislation does not "affect adversely the essence" of both Articles 7 and 8 of the Charter since it "does not permit retention of the content of a communication"[130] is rather difficult to follow. It is even more challenging to reconcile the views of Advocate General Saugmandsgaard Øe that the risks associated with access to communications metadata may be greater than those arising from access to the content of communications[131] with those that national regimes which provide for general data retention obligations do not adversely affect the essence of the right to privacy since they do not permit the acquisition of knowledge of the content of electronic communications as such.[132]

Beyond the merged and confused application of the two different fundamental rights to respect for private life and protection of personal data which has already been pointed out, metadata about communications contain "very sensitive, valuable and extensive information."[133] They "can provide a very detailed profile of an individual and processing it can be just as intrusive as processing 'content' of communications."[134] The UNESCO report on human rights and encryption of 2016 noted "the pervasive availability of metadata and the possibility to use metadata to make inferences about people and user

[118] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] paras 53, 92 and 100.
[119] Case C-131/12 *Google Spain and Google* [2013] paras 69, 74, 81, 97, 99 and 100(4).
[120] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] paras 29, 30, 34 to 36, 39, 40, 53, 66 and 68.
[121] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2014] paras 39, 47, 53, 54, 58, 65, 72, 94 and 99.
[122] Joined Cases C-141/12 and C-372/12 *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M, S* [2013], paras 58–60. See Xavier Tracol, "Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it", *Computer Law & Security Review*, Volume 31, Issue 1, February 2015, pp. 112–119.
[123] Case C-453/00 *Kühne & Heitz* [2003] paras 21 and 22.
[124] Case C-2/06 *Kempter* [2007] para 35; Cases C-89/10 and C-96/10 *Q-Beef and Bosschaert* [2010] para 48; Case C-429/12 *Pohl* [2013] para 30.
[125] Case 69/85 *Wünsche v. Germany* [1985] para 13: "a judgment in which the Court gives a preliminary ruling on the interpretation [. . .] of an act of a Community institution conclusively determines [. . .] questions of Community law"; C-231/06 to C-233/06 *Jonkman* [2006] para 38.
[126] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 93.
[127] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 93.
[128] René Barents, *Remedies and Procedures before the EU Courts*, Wolters Kluwer, Alphen aan den Rijn, 2016, p. 880, § 24.12.
[129] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 99.
[130] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 101.
[131] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 259.
[132] Opinion in Joined Cases C-203/15 and C-698/15 [2015] para 157.
[133] United Nations, Summary of the Human Rights Council panel discussion on the right to privacy in the digital age, A/HRC/28/39, 19 December 2014, p. 9, para 28. See also *ibidem*, p. 4, para 9.
[134] Preliminary European Data Protection Supervisor Opinion 2/2016 on the review of the ePrivacy Directive (2002/58/EC), 22 July 2016, p. 17.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

behavior".[135] A study by Stanford University of 12 March 2014 showed that medical, financial and legal information could be obtained from metadata.[136] It has been shown that "intimate details about a person's lifestyle and beliefs, such as political leanings and associations, medical issues, sexual orientation, habits of religious worship, and even marital infidelities can be discovered through mobile phone traffic data".[137] A "trend towards increased protection of metadata"[138] has already been noted. For instance, the International Association of Lawyers stated that metadata "deserves strong privacy protections and at least same protection than the content" (*sic*).[139]

The Grand Chamber has already held in the *Digital Rights* judgment that the essence of the fundamental right to private life was not adversely affected since the data retention directive did not permit the acquisition of content data.[140] The Grand Chamber thus examined whether the interference with this right was justified[141] and applied the tests of proportionality[142] and strict necessity.[143] In the subsequent *Schrems* judgment, the Grand Chamber consistently found that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter".[144] The Grand Chamber did accordingly not examine whether the interference with this right was justified and did not apply the tests of proportionality and strict necessity either.

The distinction drawn by the Grand Chamber between retention and access to content data, which does not respect the essence of the fundamental right to private life provided for in Article 7 of the Charter and to telecommunications metadata which does, is far from being persuasive. The Court of Justice should accordingly depart from the two *Digital Rights* and *Tele2 Sverige* judgments and consider that both retention of and access to telecommunications metadata do not respect the essence of the fundamental right to respect for private life within the meaning of Article 52(1) of the Charter and consequently infringe upon Article 7 of the Charter.

6.4. *Notion of serious crime*

The Grand Chamber repeatedly referred to the notion of serious crime[145] and ruled that "only the objective of fighting serious crime is capable of justifying"[146] the retention of both traffic and location data and that access of competent national authorities to retained data must be "restricted solely to fighting serious crime".[147] The latter notion should accordingly become an autonomous concept of EU law.

The exhaustive list of ten "areas of crimes" set out in Article 83(1) of the Treaty on the Functioning of the EU ("TFEU")[148] may provide guidance in this respect. 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."[149]

6.5. *Consequences and impact on national data retention laws*

The two cases were remitted back to the Administrative Court of Appeal of Stockholm and the UK Court of Appeal which had referred the questions to the Court of Justice for a preliminary ruling and must now rule on the legal challenges to the relevant Swedish and British legislation. The situation of the UK is especially complex.

The judgment of the Grand Chamber relates to the DRIPA which expired on 31 December 2016. The decision to be rendered by the UK Court of Appeal will consequently be academic. New legislation, the Investigatory Powers Act 2016 ("IPA"), has however been in force since 1 January 2017. This very controversial law substantially extended the powers of government and its demands on firms. It requires telecommunications operators, providers of Internet access, social media companies and data storage firms to collect and retain communications data such as the Web browsing history of users for a year and give free access to public authorities including the police and security services. The IPA also allows State hacking of telephones and computers. The judgment of the Grand Chamber may trigger legal challenges to the IPA. Even though the British government is not legally bound to amend the IPA, it may elect

[135] Wolfgang Schulz and Joris van Hoboken, Human rights and encryption, UNESCO Series on Internet Freedom, 2016, available at http://unesdoc.unesco.org/images/0024/002465/246527E.pdf, p. 23.
[136] Jonathan Mayer and Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata", available at http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.
[137] Preliminary European Data Protection Supervisor Opinion 2/2016 on the review of the ePrivacy Directive (2002/58/EC), 22 July 2016, p. 13.
[138] United Nations, Summary of the Human Rights Council panel discussion on the right to privacy in the digital age, A/HRC/28/39, 19 December 2014, p. 9, para 28 *in fine*.
[139] Resolution on "Privacy in the Digital Communications", Valencia Congress 2015, available at http://www.uianet.org/en/content/resolution-privacy-digital-communications-valencia.
[140] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 39.
[141] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 60.
[142] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] para 61.
[143] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] paras 61, 62, 64 and 65.
[144] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2014] para 94.
[145] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] paras 102, 103, 106, 108, 110, 111, 114, 115, 118, 119, 125 and 134(2).
[146] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 102.
[147] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] para 134(2).
[148] "[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."
[149] Perrine Simon, "The Criminalisation Power of the European Union after Lisbon and the Principle of Democratic Legitimacy", *New Journal of European Criminal Law*, 2012, Volume 3, Issue 3–4, pp. 247 and 248.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

to do so in light of the judgment of the Grand Chamber since some of its findings may be difficult to reconcile with it.

The judgment of the Grand Chamber may compel other Member States to reconsider, adjust and revise rules provided for in their national legislation to make sure that they comply with its requirements. For instance, Articles L. 34-1 III and R. 10–13 of the French Code of Posts and Electronic Communications both set out a general and indiscriminate retention by electronic communications operators including Internet access providers of all communications metadata of users for a year. In addition, Law No. 2015-912 of 24 July 2015[150] established a commission which may however carry out judicial or administrative review only *after* national authorities have already been granted access to intelligence.

Coming back to the UK, the latter may continue applying the General Data Protection Regulation ("GDPR")[151] after Brexit. If the UK however elects not to do so, transferring personal data to non EU countries will be subject to certification by the EU about the adequate level of protection of personal data in the UK. In this case, the judgment of the Grand Chamber could negatively impact on the ability of the UK to meet the requirement of essential equivalence and to obtain adequacy status for the purposes of foreign data transfers under the post-Brexit data protection regime. Transfers of personal data from the EU to the UK could then be challenged on the basis that British law is insufficiently adequate in comparison to EU standards. The judgment of the Grand Chamber may also provide an authority to support this challenge.

6.6. *Need for a harmonised legal framework on data retention at EU level*

The judgment of the Grand Chamber shows that the legislation in force in two Member States, *i.e.* Sweden and the UK, substantially differ. This situation is not surprising since the Grand Chamber did not invalidate national laws enacting the data retention directive in the *Digital Rights* judgment since it was not seized of the matter and does not have the jurisdiction to rule on their legal validity, pursuant to Article 267 of the TFEU. National laws consequently remain valid and applicable.

In the last three years, some Member States such as Sweden did accordingly not amend their national law enacting the judicially invalidated data retention directive. Other Member States such as the UK adopted a new law. National legislation of yet other Member States has been legally challenged before domestic courts. For instance, the Constitutional Court of Belgium has repealed the domestic law by judgment of 11 July 2015.

As a result, a mosaic if not a patchwork of inconsistent national legislation on the retention of data is currently in force. A harmonised legal framework on data retention at EU level is necessary to create a level-playing field on the issue.

On 11 January 2017, the Commission proposed a new e-privacy regulation which would replace the directive.[152] The draft regulation aims to align the applicable regime to that of the GDPR. The draft regulation does no longer contain a provision similar to Article 15(1) of the directive on the retention of data. It however includes Article 11 which is similar to Article 23 of the GDPR and leaves the option of targeted retention measures for the EU and Member States subject to compliance with the Charter as interpreted in the case law of the Court of Justice.[153] As the directive, Articles 6(2)(b) and 7(3) of the draft regulation also allow providers of electronic communications to process and retain metadata if necessary for billing and calculating interconnection payments.

After the *Digital Rights* judgment, the Commission had to determine whether it intended to propose the adoption of a new data retention directive which would have needed to take account and address the findings contained in the judgment.[154] The Commission has elected not to do so more than three years later. In the meantime, the situation has evolved. If the Commission were to propose a new data retention directive, national legislation adopted by Member States to enact the directive would need to comply with all the requirements set out by the Grand Chamber in the *Tele2* judgment.

The current trend is however for the Commission to propose the adoption of regulations instead of directives in the area of personal data protection. For instance, the GDPR replaces directive 95/46/EC whilst the e-privacy regulation would replace the e-privacy directive. Regulations are directly applicable in the legal order of Member States without any need to adopt national legislation enacting them. If the Commission were to propose the adoption of a regulation on data retention, the latter would need to comply with the findings of the *Digital Rights* judgment. The adoption of a regulation on data retention would however avoid the need for Member States to adopt national legislation which would have to comply with the requirements set out by the Grand Chamber in the *Tele2* judgment.

7. Conclusion

The Grand Chamber showed by this new judgment its firm willingness to scrupulously monitor compliance with Article 7 on respect for private life, Article 8 on protection of personal data,

[150] Published in the *Official Journal* of 26 July 2015, p. 12735.

[151] Regarding an analysis of the GDPR, see Xavier Tracol, "The regulation and the directive on the protection of personal data", *Europe*, October 2016, No. 10, pp. 5–10.

[152] 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), COM(2017) 10 final.

[153] 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), COM(2017) 10 final, p. 3, Section 1.3.

[154] 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, December 2014, p. 746.

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003

Article 11 on freedom of expression and Article 52(1) on the principle of proportionality of the Charter. This judgment thus represents a new step in the process of reconciling legislation of Member States against serious crime and terrorism with fundamental rights. The Grand Chamber is increasingly building up a real and effective privacy shield[155] to protect European values which are increasingly eroded by domestic legislation of Member States aiming to organise the fight against serious crime and terrorism.

Last, the Court of Justice may refer back to the list of requirements for access by competent national authorities to retained personal data[156] when it renders its opinion on the draft EU-Canada passenger name record ("PNR") agreement about data directly transferred by companies to law enforcement authorities in third countries with no limit.[157]

Acknowledgement

The views expressed herein are those of the author in his personal capacity and do not necessarily reflect those of EUROJUST or the EU in general.

[155] See Xavier Tracol, "EU-U.S. Privacy Shield: The saga continues", *Computer Law & Security Review*, Volume 32, Issue 5, October 2016, pp. 775–777.

[156] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2015] paras 119–121 and 125.

[157] Request for an opinion submitted by the European Parliament, draft EU-Canada PNR agreement (opinion 1/15).

Please cite this article in press as: 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: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.003