TO THE PRESIDENT AND MEMBERS OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

In **Cases C-793/19 and C-794/19**

SPACENET AG

Applicant/Respondent

-v-

FEDERAL REPUBLIC OF GERMANY

Defendant/Appellant

-and-

TELEKOM DEUTSCHLAND GMBH

Applicant/Respondent

-v-

FEDERAL REPUBLIC OF GERMANY

Defendant/Appellant

WRITTEN OBSERVATIONS OF IRELAND

Ireland, represented by Maria Browne, Chief State Solicitor, Osmond House, Little Ship Street, Dublin 8, acting as Agent, accepting service by e-Curia with at the Embassy of Ireland, 28 route d'Arlon, Luxembourg, and assisted by David Fennelly BL of the Bar of Ireland, has the honour to submit written observations in these proceedings, the subject of references for preliminary ruling from the *Bundesverwaltungsgericht* (Germany) lodged on 29 October 2019.

Dated 14 February 2020

I. Introduction

1. Ireland submits these Written Observations pursuant to Article 23 of the Protocol on the Statute of the Court of Justice of the European Union.

2. The *Bundesverwaltungsgericht* (Germany) ("**the referring court**") has referred the following question for preliminary ruling pursuant to Article 267 TFEU ("**the References**"):

> *In the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, on the one hand, and of Article 6 of the Charter of Fundamental Rights of the European Union and Article 4 of the Treaty on European Union, on the other hand, is Article 15 of Directive 2002/58/EC to be interpreted as precluding national legislation which obliges providers of publicly available electronic communications services to retain traffic and location data of end users of those services where*
>
> *– that obligation does not require a specific reason in terms of location, time or region,*
>
> *– the following data are the subject of the storage obligation in the provision of publicly available telephone services — including the transmission of short messages, multimedia messages or similar messages and unanswered or unsuccessful calls:*
>
> > *– the telephone number or other identifier of the calling and called parties as well as, in the case of call switching or forwarding, of every other line involved,*
> >
> > *– the date and time of the start and end of the call or — in the case of the transmission of a short message, multimedia message or similar message — the times of dispatch and receipt of the message, and an indication of the relevant time zone,*
> >
> > *– information regarding the service used, if different services can be used in the context of the telephone service,*
> >
> > *– and also, in the case of mobile telephone services*
> > > *– the International Mobile Subscriber Identity of the calling and called parties,*
> > > *– the international identifier of the calling and called terminal equipment,*
> > > *– in the case of pre-paid services, the date and time of the initial activation of the service, and an indication of the relevant time zone,*
> > > *– the designations of the cells that were used by the calling and called parties at the beginning of the call,*
> > > *– in the case of internet telephone services, the Internet Protocol addresses of the calling and the called parties and allocated user IDs,*

– *the following data are the subject of the storage obligation in the provision of publicly available internet access services:*

– *the Internet Protocol address allocated to the subscriber for internet use,*

– *a unique identifier of the connection via which the internet use takes place, as well as an allocated user ID,*

– *the date and time of the start and end of the internet use at the allocated Internet Protocol address, and an indication of the relevant time zone,*

– *in the case of mobile use, the designation of the cell used at the start of the internet connection,*

– *the following data must not be stored:*

– *the content of the communication,*

– *data regarding the internet pages accessed,*

– *data from electronic mail services,*

– *data underlying links to or from specific connections of persons, authorities and organisations in social or ecclesiastical spheres,*

– *the retention period is four weeks for location data, that is to say, the designation of the cell used, and ten weeks for the other data,*

– *effective protection of retained data against risks of misuse and against any unlawful access to that data is ensured, and*

– *the retained data may be used only to prosecute particularly serious criminal offences and to prevent a specific threat to life and limb or a person's freedom or to the continued existence of the Federal Republic or of a Federal Land, with the exception of the Internet Protocol address allocated to a subscriber for internet use, the use of which data is permissible in the context of the provision of inventory data information for the prosecution of any criminal offence, maintaining public order and security and carrying out the tasks of the intelligence services?*

3. Thus, the referring court asks, in essence, if Article 15(1) of Directive 2002/58/EC ("**the ePrivacy Directive**") interpreted in light of the Charter and Article 4 TEU, precludes the German data retention and access legislation, the terms of which are identified in the question and further described in the text of the References.

II. Preliminary Observations

4. These References follow in a long line of references from Member States' courts concerning the compatibility of national data retention legislation with EU law in the wake of this Court's judgment in *Digital Rights Ireland & Others*.[1] To date, there have been eleven references from eight Member States, asking whether different aspects of national data retention and access regimes are precluded by EU law.[2]

5. In *Digital Rights Ireland & Others*, this Court struck down the Data Retention Directive, Directive 2006/24/EU, on the basis that it constituted a disproportionate interference with the rights to privacy and protection of personal data guaranteed under Articles 7 and 8 of the Charter of Fundamental Rights. The Data Retention Directive had sought to harmonize the obligations on telecommunications service providers to retain telecommunications metadata in order to ensure that such data were available for law enforcement purposes. Significantly, it did so without prejudice to the power of Member States to regulate access to retained data.[3] However, since the striking down of the Directive, there is no EU legislation governing data retention for law enforcement purposes.

6. In the judgments which have followed *Digital Rights Ireland & Others*, this Court has based its jurisdiction to examine national data retention and access measures on Article 15(1) of the Directive 2002/58/EC. For the reasons which will be set out in detail below, Ireland considers that this provision is now being called upon to play a role which it was never intended to play, which is inconsistent with the legal basis on which the ePrivacy Directive was adopted, and which it is inappropriate as a matter of constitutional principle.

7. In its written and oral observations in a number of pending references,[4] Ireland has expressed its concern that the Court is in effect being drawn into legislating in this field. In *Tele2*

---

[1] Judgment of 8 April 2014, *Digital Rights Ireland & Others*, C‑293/12 and C‑594/12, EU:C:2014:238.
[2] C-203/15, *Tele2 Sverige*; C-698/15, *Watson*; C-475/16, *K* (withdrawn); C-207/16, *Ministerio Fiscal*; C-623/17, *Privacy International*; C-511/18, *Quadrature du Net & Others*; C-512/18, *French Data Network & Others*; C-520/18, *Ordre des barreaux francophones et germanophone*; C-746/18, *Prokuratuur*; C-793/19, *SpaceNet AG*; C-794/19, *Telekom Deutschland GmbH*.
[3] Directive 2006/24/EC, recital 25 and Article 4.
[4] C-623/17, *Privacy International*; C-511/18, *Quadrature du Net & Others*; C-512/18, *French Data Network & Others*; C-520/18, *Ordre des barreaux francophones et germanophone*; C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*.

Sverige/Watson, the Court purported to prescribe the particular model of data retention, targeted retention, which it was permissible for Member States to adopt in their national legislation.[5] It also laid down detailed rules in relation to the safeguards which must be laid down in national legislation in respect of access to retained telecommunications data. In the further references which have followed *Tele2 Sverige/Watson*, the Court has been asked to define more and more detailed rules in the context of diverse national regimes. These rules touch upon sensitive areas of Member State competence – including, for example, the organisation of national systems of criminal justice, the rules governing the admissibility of evidence and the safeguarding of national security – in respect of which there are few common rules across Member States, still less at EU level.

8. The extremely detailed question which is the subject of the present References exemplifies the difficulties to which the Court's case-law gives rise. In these References, the Court is, in effect, being asked to decide whether the detailed rules and requirements laid down in German data retention and access legislation – which represent the carefully considered choices of the democratically elected legislature in that Member State – are precluded by EU law in circumstances where the only EU legislation which makes any reference to data retention is now Article 15(1) of Directive 2002/58/EC.

9. Moreover, as in *Tele2 Sverige/Watson*, the Court is being asked to rule on these issues in the context of what are essentially abstract challenges to the national legislation. The References are devoid of any meaningful factual or evidential foundation, particularly on the central issues of the scope, necessity and utility of data retention. Yet the challenges to which the judgment in *Tele2 Sverige/Watson* has given rise underline the perils of the Court pronouncing on these issues without a robust and reliable evidential basis.

10. Against this backdrop, in Ireland's submission, these References present the Court with an opportunity to recognize the limitations of Article 15(1) of Directive 2002/58/EC and to accord due respect to the carefully considered choices of the democratically elected legislatures of Member States in adopting national data retention and access measures.

[5] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 108 *et seq*.

III. The Assessment of the Compatibility of National Data Retention and Access Measures with Article 15(1) of Directive 2002/58/EC

11. Before addressing the detailed question which is the subject of these References, it is necessary to place that question within its broader context, by examining, first, the EU legislative provision by reference to which the national measures are to be assessed and, secondly, the standard of review which this Court ought to apply in carrying out that assessment.

A. The Limits of Article 15(1) of Directive 2002/58/EC

12. First, it is important to emphasize that, while these References are framed as asking if Article 15(1) of the ePrivacy Directive, interpreted in light of the Charter, precludes the relevant German legislation, Article 15(1), on its terms, provides no answer to the questions to which the References give rise.

13. Article 15(1) provides:-

> *Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.*

14. This provision recognizes that Member States may adopt measures to restrict the scope of certain rights and obligations under Directive 2002/58/EC for certain enumerated purposes, which fall outside the scope of the Directive and remain within Member State competence. Among these purposes is *"the prevention, investigation, detection and prosecution of criminal offences"*. Article 15(1) makes it clear, in its second sentence, that such measures may include *"legislative measures providing for the retention of data for a limited period*

justified on the grounds laid down in this paragraph". In its third sentence, Article 15(1) provides that such measures shall be in accordance with the general principles of Community (now Union) law, including fundamental rights.

15. Article 15(1) says nothing further about data retention measures and makes no reference whatsoever to national measures on access to retained data.[6] More particularly, in respect of the matters identified in the question the subject of these References, Article 15(1) provides no guidance on the scope, whether general or limited, of data retention measures, the specific categories of data to be retained, the retention period (save only that this must be limited), the safeguards against abuse or unlawful access of retained data, or the purposes for which retained data may be accessed.

16. This is not surprising because, in accordance with Article 1(3), the ePrivacy Directive shall not apply to activities *"which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law".* Put simply, Article 15(1) does not purport to define the scope of, or the specific safeguards in, any data retention legislation applicable in these fields.

17. The limited scope of the Directive is consistent with the legal basis relied upon by the EU legislature for the adoption of Directive 2002/58/EC: Article 95 EC. The purpose of the Directive was to harmonize Member States' laws and regulations on data protection in the electronic communications sector *"in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty"*, such harmonization to be limited *"to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered"*.[7]

[6] Indeed, even when the EU legislature adopted the Data Retention Directive in 2006, it did so without prejudice to Member States' competence to regulate access to retained data: see Directive 2006/24/EC, recital 25 and Article 4.

[7] Directive 2002/58/EC, recital 8.

18. It follows that Directive 2002/58/EC was never intended to, and had no legal authority to, regulate measures adopted by the Member States in fields lying outside the scope of EU law, including criminal law and national security.[8] Insofar as Article 15(1) has been interpreted as bringing within the scope of the Directive matters which are explicitly excluded from the scope of its application,[9] such an interpretation cannot be reconciled with the text of the Directive (specifically Article 1(3)), the legal basis on which it was adopted (Article 95 EC), and, most fundamentally of all, the constitutional division of powers between the Union and Member States under the Treaties, as reflected in the principle of conferral in Article 5(2) TEU.[10] As Ireland has previously submitted in its observations in Case C-623/17, Joined Cases C-511/18 and C-512/18, Case C-520/18 and Case C-746/18, Article 15(1) is properly interpreted as a provision which seeks to address the co-existence of Union and Member State competence in a particular field and, to the extent possible, to ensure consistency between the two; by contrast, it cannot be interpreted as bringing within the scope of Union law the very matters which are excluded from the scope of the Directive and reserved to the Member States.

19. These References illustrate the difficulties which arise when Article 15(1) is called upon to take up a role which it was never intended to serve. How can Article 15(1) be understood as the source of the detailed rules governing Member States' national data retention and access measures – such as those identified in the References – when it does not in any way address these issues?

20. As is apparent from the References,[11] the regulation of data retention and access for law enforcement and security purposes presents complex and challenging policy choices for the Member States. By their very nature, these choices are matters first and foremost for the democratically elected legislature, subject to review by the courts as appropriate. These choices include whether to make provision for data retention and access at all and, if so, the appropriate scope and limits of such measures. In the context of law enforcement and national security, this inevitably involves the weighing of competing public interests, such as the protection of the fundamental right to privacy and data protection, on the one hand, and the

[8] See also Directive 2002/58/EC, recital 11.
[9] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 73; Judgment of 2 October 2018 in *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 39.
[10] See by analogy judgment of 30 May 2006, *Parliament v. Council & Commission*, Joined Cases C-317/04 and C-318/04, ECLI:EU:C:2005:190, paragraphs 56-8.
[11] See especially Reference in C-793/19, paragraphs 25-28.

protection of other rights, such as the right to life and the right to security, and the public interest in fighting crime and safeguarding national security, on the other hand. Moreover, by their nature, data retention and access measures reach deep into Member States' criminal justice systems, requiring a high level of legal certainty because of their significant implications for criminal investigations and prosecutions. Finally, because the systems of criminal justice vary widely from one Member State to another, the detailed rules and regulations governing data retention and access must be tailored to the specificities of the national constitutional and criminal law framework. This being so, Article 15(1) of Directive 2002/58/EC, even when interpreted in light of the Charter with the benefit of the guidance of this Court, is simply not an appropriate or effective substitute for detailed legislation in this field.

21. For these reasons, it is submitted that, in the absence of any EU-level legislation in this field, and in accordance with the fundamental principle of conferral, it must be for Member States' legislatures to weigh these competing interests, to make the complex and challenging policy choices that this exercise entails, and – following such consultation, assessment of evidence and public debate as may be appropriate – to decide on the detailed rules regulating data retention and access. This is precisely what the German legislature has done in adopting and amending its national data retention and access regime at issue in these cases. In Ireland's submission, it is incumbent on the Court to accord due respect to the carefully considered choices of the national legislature, particularly in a field which lies, to a significant degree, outside the scope of Union competence.

B. The Appropriate Standard of Review

22. This leads to the second general consideration which is relevant to the Court's examination of these References. In Ireland's submission, the respect which must be accorded to Member States' legislatures – in making complex and challenging policy choices, in a field where there are no meaningful EU legislative rules and which remains, to a significant degree, within the competence of Member States – must be reflected in the standard of review applied by the Court in its review of national data retention and access measures.

23. In its assessment of the validity of the Data Retention Directive in *Digital Rights Ireland & Others*, this Court stated as follows:

> *47 With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R.,* S. and Marper v. the United Kingdom *[GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).*
>
> *48 In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.*

In short, because of the seriousness of the interference to fundamental rights entailed by the Data Retention Directive, the Court took the view that the EU legislature's discretion was reduced and the standard of strict review.

24. In arriving at this conclusion, this Court expressly referred to and relied upon paragraph 102 of the Grand Chamber judgment of the European Court of Human Rights in *S. and Marper v. United Kingdom*,[12] in which the Strasbourg Court set out its approach to the assessment of the proportionality of an interference with Article 8 ECHR. It is instructive to set out this paragraph in full:

> *A margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights (see* Connors v. the United Kingdom*, no. 66746/01, § 82, 27 May 2004, with further references). Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted (see* Evans v. the United Kingdom *[GC], no. 6339/05, § 77, ECHR 2007-I). Where, however, there is no consensus within the member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider (see* Dickson v. the United Kingdom *[GC], no. 44362/04, § 78, ECHR 2007-V).*

[12] *S. and Marper v. United Kingdom,* Applications nos. 30562/04 and 30566/04, § 102, ECHR 2008-V.

Thus, while recognizing that the breadth of the margin of appreciation afforded to States – and thus the intensity of judicial review – may vary and depend on a number of factors, including the nature of the right and the interference therewith, the Strasbourg Court emphasized the importance of leaving a margin of appreciation to competent national authorities in this field, particularly where there is no consensus across member states.

25. This is consistent with the approach of the Strasbourg Court in more recent cases in this field. Thus, in *Centrum för Rättvista v Sweden,* the Court (Third Section) concluded that Swedish legislation providing for bulk interception of signals communications did not violate Article 8 ECHR. In assessing the proportionality of the legislation, the Court emphasized, in line with its settled case-law, that this depended on *"all the circumstances of the case"*.[13] In the particular context of interception legislation, the Court noted the wide margin of appreciation enjoyed by national authorities and, in an important passage, the nature of the current threats facing States:

> *The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see* Weber and Saravia*, cited above, § 106). In* Weber and Saravia *and* Liberty and Others *the Court accepted that bulk interception regimes did not per se fall outside this margin. Given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.*[14]

At the same time, the Court recognized the potential for abuse in any system of this kind and distinguished between the margin of appreciation to be applied *"in deciding what type of interception regime is necessary to protect national security"* – which was wide – and *"the*

[13] Judgment of 19 June 2018, European Court of Human Rights (Third Section), *Centrum för Rattvista v Sweden*, Application no. 35252/08, paragraph 104.
[14] *Centrum för Rattvista v Sweden*, paragraph 112.

discretion afforded to them in operating an interception regime must necessarily be narrower". [15] Ultimately, the Court concluded, on the basis of *"an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security"*, that, while there were some areas for improvement, the Swedish legislation provided adequate and sufficient guarantees against arbitrariness and the risk of abuse.[16] So too, in *Big Brother Watch & Others v. United Kingdom*, the Strasbourg Court (First Section) – in its examination of the compatibility of certain provisions of UK law providing for interception of communications, intelligence sharing and acquisition of communications data respectively with the Convention – reaffirmed its position on the margin of appreciation applicable to national security measures.[17] While these cases have since been referred for hearing before the Court's Grand Chamber, the judgments of which are awaited, the statements of principle on the margin of appreciation reflect the Court's longstanding jurisprudence.

26. In Ireland's submission, the logic of this approach – which was applied by analogy at paragraph 47 of the judgment in *Digital Rights Ireland & Others* – requires this Court to afford greater leeway to Member States when the Court is requested to review the compatibility of *national* measures on data retention and, in particular, on access to retained data with EU law, in circumstances where there is no EU level instrument regulating these matters.

27. While, in its judgment in *Tele2 Sverige/Watson*, the Court did not articulate the standard of review it applied in as explicit a way as in its earlier judgment in *Digital Rights Ireland*, the Court appears to have adopted a similarly strict standard of review to *national* data retention and access measures as it had to EU measures, notwithstanding the absence of any EU-wide legislation governing data retention and the fact that these measures, particularly insofar as access is concerned, are adopted in fields which remain, to a significant degree, within Member State competence.[18]

---

[15] *Centrum för Rattvista v Sweden*, paragraph 113.
[16] *Centrum för Rattvista v Sweden*, paragraph 181.
[17] Judgment of 13 September 2018, European Court of Human Rights (First Section), *Big Brother Watch & Others v. United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, paragraph 314.
[18] Judgment of 21 December 2016, *Tele2 Sverige/Watson*, C‑203/15 and C‑698/15, EU:C:2016:970, paragraphs 95-96, 107-110, 115-119; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788.

28. Yet, as the references which have followed *Tele2 Sverige/Watson* demonstrate, this approach gives rise to very significant challenges for Member States. In his Opinion of 15 January 2020 in Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*, Advocate General Campos Sánchez-Bordona has explicitly recognized that "*the determination of investigative techniques and the assessment of their effectiveness are within the margin of appreciation of the Member States*".[19] In Ireland's submission, this logic applies more broadly to the specific choice of data retention regime in each Member State, its precise scope of application, and the choice of detailed safeguards which accompany access to retained data in fields which remain, in large part, within Member State competence, including law enforcement and, most significantly of all in light of Article 4(2) TEU, national security.

29. While the Court of Justice has refrained from developing a margin of appreciation doctrine as part of EU law, as the passage from the judgment in *Digital Rights Ireland & Others* cited above demonstrates, this Court has nonetheless drawn on the logic of the Strasbourg Court's doctrine in defining the standard of review which it applies to measures involving an interference with fundamental rights. In accordance with the approach adopted by the Strasbourg Court, this margin of appreciation – and, by extension, the intensity of review carried out by the Court – varies and depends on a number of factors, including not only the right at issue and the nature of the interference with that right but also the degree of consensus among States as to how best to protect that right. Moreover, in assessing the compatibility of a national regime with fundamental rights, it is necessary to undertake an overall assessment of that regime.

30. While it is of course true that national data retention legislation, like the Data Retention Directive at issue in *Digital Rights Ireland*, involves a serious interference with fundamental rights, national data retention regimes are accompanied by detailed regimes governing access to retained data, something which has never been regulated at EU level, even under the now invalidated Data Retention Directive. Having regard to the factors set out above – in particular, the complex and challenging policy choices and balancing exercise which the adoption of national data retention and access regimes entails, the absence of any EU-level legislative

[19] Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*, EU:C:2020:7, paragraph 81, footnote 69.

rules governing these matters, and the degree to which those regimes relate to fields which remain within the competence of Member States and which, moreover, vary significantly from Member State to Member State – Ireland submits that the Court must afford Member States' legislatures appropriate discretion in the choice and design of national data retention and access regimes and in the definition of the detailed rules governing the scope and application of such regimes, the proportionality of which must be based on an overall assessment. Moreover, this assessment must be carried out first and foremost by Member States' courts which are best placed to understand the specific factual and legal context within which such regimes are adopted.

31. It is on this basis, in Ireland's submission, that the Court must approach its examination of the German legislation which is the subject of these References.

IV. The Question Referred

32. Turning to the question the subject of these References, and applying these principles, in Ireland's submission, Article 15(1) of Directive 2002/58/EC, interpreted in light of the Charter of Fundamental Rights and Article 4 TEU, must not be interpreted as precluding national data retention legislation of the kind adopted by the German legislature.

33. While the References identify various elements of the national legislation, it is clear that the primary basis on which the Applicants in the national proceedings seek to impugn the national legislation is the general scope of the retention obligation under that legislation. In support of their case, the Applicants rely on this Court's judgment in *Tele2 Sverige/Watson*.

34. However, in Ireland's submission, a general data retention obligation – of the kind identified in the legislation at issue in these References – is *not* precluded by EU law.

35. In *Digital Rights Ireland*, this Court accepted that retained telecommunications data were a *"valuable tool for criminal investigations"*[20] and that general data retention – of the kind provided for in the Data Retention Directive – was *appropriate* for attaining the objective of fighting serious crime.[21] However, the Court ultimately concluded that the particular regime established by the Data Retention Directive - which failed to lay down clear and precise rules governing its scope and application, failed to impose minimum safeguards, and left the question of access to retained data entirely to Member States - constituted a disproportionate interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter.[22] However, in reaching this conclusion, the Court did not call into question its earlier conclusion that data retention, general in scope, was an appropriate means of achieving the objective of fighting serious crime.[23]

---

[20] Judgment of 8 April 2014 in *Digital Rights Ireland & Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 49; see also paragraph 51.
[21] *Digital Rights Ireland & Others*, paragraph 49.
[22] *Digital Rights Ireland & Others*, paragraphs 54-69.
[23] See in this regard the Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*, EU:C:2020:7, paragraph 84.

36. In its subsequent judgment in *Tele2 Sverige/Watson*, this Court held that Article 15(1) of the e-Privacy Directive 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 communications"*.[24] At the same time, the Court observed that Article 15(1) *"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"*.[25] While the Court stipulated that any data retention measures must be based on objective evidence,[26] it does not appear that there was any evidence before the Court in the present case to support the conclusion that *"targeted retention"* was either an appropriate means of achieving the objective of fighting serious crime or an effective alternative to general retention.[27]

37. In observations made in a number of pending proceedings before the Court,[28] Ireland – alongside other Member States and intervening parties – has submitted that, insofar as *Tele2 Sverige/Watson* might be interpreted as precluding general data retention, it must be reconsidered. The reason for this submission may be simply stated: data retention can only be an effective tool for the purposes of fighting serious crime and safeguarding national security if it is general in scope at the stage of retention. As the referring court has expressed the position, "*the basic concept of data retention cannot be reconciled with the Court of*

[24] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.
[25] *Tele2 Sverige/Watson*, paragraphs 108-111.
[26] *Tele2 Sverige/Watson*, paragraph 111.
[27] While the Opinion of Advocate General Saugmandsgaard Øe in *Tele2 Sverige/Watson* made reference to a number of studies which questioned the necessity of general retention, none of the studies referred to by the Advocate General in fact provides any support for the concept of targeted retention: instead, they either suggest data preservation as an alternative to data retention or simply highlight the issues identified by this Court with the particular data retention regime established under the Data Retention Directive: see Opinion of 19 July 2016 of Advocate General Saugmandsgaard Øe in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:572, paragraph 209, footnote 65.
[28] C-623/17, *Privacy International*; C-511/18, *Quadrature du Net & Others*; C-512/18, *French Data Network & Others*; C-520/18, *Ordre des barreaux francophones et germanophone*; C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*.

Justice's unqualified requirement that the data to be retained must be differentiated according to individuals, periods of time and geographical areas".[29]

38. The real and distinctive value added of data retention – as opposed to other possible tools such as data preservation[30] – is that it can assist in identifying persons who are hitherto unknown to the authorities in the context of investigations into serious crime and national security. In providing the authorities with access, subject to appropriate safeguards, to historical telecommunications data, data retention can also allow evidence trails to be established, including on the movements of suspects, victims or witnesses to serious crime and those involved in threats to national security, such as terrorism. In many cases, without access to this data, investigations would be fundamentally undermined. In particular, the investigation and prosecution of many serious forms of cybercrime, such as online child sexual exploitation and child pornography, would be severely compromised without access to retained telecommunications data.[31] That real and distinctive value would be lost if Member States could only make provision for some form of *"targeted retention"* of the kind envisaged in *Tele2 Sverige/Watson*, which appears to share the limitations of data preservation. For the reasons which Ireland has set out in detail in its written observations in the pending cases, such a data retention regime would not only be unworkable in practice but would also be very difficult to justify in principle, having regard to the very real risk of discriminatory targeting.

39. In his Opinion of 15 January 2020 in Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*, Advocate General Campos Sánchez-Bordona appears to recognize the difficulties with the concept of targeted retention laid down by the Court in *Tele2 Sverige/Watson*.[32] While the Advocate General has advised the Court to maintain "*the*

[29] Reference in C-793/19, paragraph 25.

[30] Data preservation was rejected by the EU legislature as an effective alternative to data retention both prior to the adoption of the now invalidated Data Retention Directive and in 2011 in the context of its evaluation: see Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, SEC(2005) 1131, 1, 5-6, 13; European Commission, *Evaluation report on the Data Retention Directive*, COM(2011) 225, pp. 1 and 5.

[31] See e.g. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, paragraphs 7.47, 14.19-22.

[32] Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*, EU:C:2020:7, paragraphs 87-91. See also Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Joined Cases C-

position of principle" in its earlier judgments that general and indiscriminate retention is precluded by EU law,[33] he suggests that "*national legislation providing for appropriate restrictions on the retention of some of these data, generated in connection with the provision of electronic communications services, could be compatible with Union law*". Thus, in place of the problematic concept of targeted retention, the Advocate General refers to the concept of "*limited retention*".[34] The Advocate General acknowledges that the criteria for targeted retention of the kind envisaged in *Tele2 Sverige/Watson* "*might be impractical or inoperative for the purposes sought, or even become a source of discrimination*".[35] According to the Advocate General, a system of "*limited retention*" might involve elements such as the limitation of the categories of data retained, the introduction of limited retention periods, the pseudonymization of data, the exclusion of certain categories of providers of electronic communications services, the obligation to retain data within the Union or the systematic and regular monitoring, by an independent administrative authority, of the guarantees offered by providers of electronic communications services against the misuse of data.[36] Significantly, the Advocate General recognizes that it is a matter for the legislative branch of government to define the limits of a data retention regime. Thus, Advocate General Campos Sánchez-Bordona expressed the following view:

> *Pending a common regulation for the whole of the Union in this specific area, I do not believe that the Court can be asked to take on regulatory functions and specify in detail what categories of data may be retained and for how long. It is up to the institutions of the Union and the Member States, once the limits which, according to the Court, derive from the Charter have been set, to place the cursor in the right place in order to strike a balance between safeguarding security and the fundamental rights protected by the Charter.*[37]

40. While it remains to be seen whether the Court will follow the approach of the Advocate General in this case, the Opinion in *Ordre des barreaux* is a welcome recognition of the

511/18 and C-512/18, *Quadrature du Net/French Data Network and Others*, EU:C:2020:6, paragraphs 112-123; and Opinion of Advocate General Pitruzzella in C-746/18, *Prokuratuur,* EU:C:2020:18, paragraphs 54-56.

[33] Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*, EU:C:2020:7, paragraph 72. However, note the important caveat to this conclusion at paragraph 105 of the Opinion.

[34] *Ordre des barreaux francophones et germanophone and Others*, paragraph 73.

[35] *Ordre des barreaux francophones et germanophone and Others*, paragraph 74.

[36] *Ordre des barreaux francophones et germanophone and Others*, paragraph 92.

[37] *Ordre des barreaux francophones et germanophone and Others*, paragraph 101.

problems to which the concept of "*targeted retention*" defined by the Court in *Tele2 Sverige/Watson* gives rise.

41. It is clear from the References that the German legislation impugned in these proceedings, while general in scope, nonetheless constitutes a form of "*limited retention*" which is not precluded by EU law:
    (i) First, as the referring court observes, the legislation does not require "*the storage of all the telecommunications traffic data of all subscribers and registered users in relation to all means of electronic communication*" but instead the retention of limited categories of data which are carefully defined under that legislation.[38]
    (ii) Secondly, the retention period is strictly limited to four weeks for location data and to ten weeks for other data.[39]
    (iii) Thirdly, the legislation provides "*effective protection against risks of misuse and against any unlawful access*" to retained data.[40]
    (iv) Fourthly, access to retained data – with the exception of certain categories of subscriber data – is limited to the purposes of fighting particularly serious crime and of preventing a specific threat to the life, limb or freedom of a person, or to the continued existence of Federal Republic or a Federal Land.[41]

42. Having regard to the discretion which must be afforded to Member States' legislatures in the detailed choice and design of national data retention and access regimes, particularly in the absence of any EU legislative rules, and the need for an overall assessment of such regimes, in Ireland's submission, there is no basis on which it can be suggested that the German legislation at issue in the main proceedings is precluded by Article 15(1) of Directive 2002/58/EC, interpreted in light of the Charter and Article 4 TEU.

[38] Reference in C-793/19, paragraph 17.
[39] Reference in C-793/19, paragraph 18.
[40] Reference in C-793/19, paragraph 20.
[41] Reference in C-793/19, paragraphs 21-22.

V. Conclusion

43. FOR THESE REASONS, it is submitted that the Court should respond as follows to the References:

> Article 15 of Directive 2002/58/EC, interpreted in light of Articles 6, 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union and Article 4 of the Treaty on the European Union, must not be interpreted as precluding national legislation which imposes an obligation on the providers of publicly available electronic communications services to retain traffic and location data on the terms defined in the References herein.

Dated 14 February 2020

Signed: Tony Joyce

Agent for Ireland

On behalf of Maria Browne, Chief State Solicitor

Signed: Juliana Quaney

Agent for Ireland

On behalf of Maria Browne, Chief State Solicitor