Case C-793/19

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date lodged:

29 October 2019

Referring court:

Bundesverwaltungsgericht (Germany)

Date of the decision to refer:

25 September 2019

Applicant and respondent in the appeal on a point of law:

SpaceNet AG

Defendant and appellant in the appeal on a point of law:

Federal Republic of Germany

Subject matter of the main proceedings

Action seeking a declaration that SpaceNet is not obliged to store the telecommunications traffic data — listed in Paragraph 113b(3) of the Telekommunikationsgesetz (Law on telecommunications, 'the TKG') — of its customers to whom it provides internet access.

Subject matter and legal basis of the reference

Interpretation of EU law, in particular Article 15(1) of Directive 2002/58, and the *Tele2 Sverige and Watson and Others* judgment; Article 267 TFEU.

Question referred

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?

Provisions of EU law cited

Charter of Fundamental Rights of the European Union ('the Charter'), Articles 6, 7, 8, 11 and 52

Treaty on European Union ('TEU'), Articles 4 and 6

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 ('Directive 2002/58'), Articles 5, 6, 8, 9, in particular Article 15; recital 11

Provisions of national law cited

Telekommunikationsgesetz (Law on telecommunications, 'the TKG'), first sentence of Paragraph 113a(1) ('Obliged parties'), Paragraph 113b ('Obligations to store traffic data'), Paragraph 113c ('Use of data'), Paragraph 113d ('Ensuring the security of data'), Paragraph 113e ('Logging' [by the obliged party of access to stored data]), Paragraph 113f ('Catalogue of requirements' [in relation to technical precautions and other measures]), Paragraph 99(2) ('Individual connection evidence', bodies exempted from recognition in individual connection evidence)

Strafprozessordnung (Code of Criminal Procedure, 'the StPO'), Paragraph 100g(2) ('Collection of traffic data' pursuant to Paragraph 113b of the TKG)

Case-law of the Court of Justice cited

Judgment of the Court of Justice of the European Union of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970 ('*Tele2 Sverige and Watson and Others* judgment')

Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, EU:C:2014:238 ('*Digital Rights Ireland and Others* judgment')

Opinion 1/15 of 26 July 2017, EU:C:2017:592

In addition: Judgments of 29 July 2019, *Funke Medien* (C-469/17, EU:C:2019:623); of 9 March 1978, *Simmenthal* (106/77, EU:C:1978:49); of 3 May 2005, *Berlusconi and Others* (C-387/02, C-391/02 and C-403/02, EU:C:2005:270); of 22 June 2010, *Melki and Abdeli* (C-188/10 and C-189/10, EU:C:2010:363); of 18 September 2014, *Vueling Airlines* (C-487/12, EU:C:2014:2232).

Brief summary of the facts and procedure

1 The applicant, SpaceNet AG ('the applicant' or 'SpaceNet') provides publicly available internet access services. It opposes the obligation imposed on it by Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG, as amended by the Law of 10 December 2015, to retain telecommunications traffic data of its customers as from 1 July 2017.

2 At first instance, the Verwaltungsgericht (Administrative Court) ruled that SpaceNet is not obliged to store the telecommunications traffic data — listed in Paragraph 113b(3) of the TKG — of its customers to whom it provides internet access. The defendant, the Federal Republic of Germany ('the defendant'), lodged

a leap-frog appeal on a point of law against the judgment of the Administrative Court.

3 The appeal on a point of law will be successful only if the obligation, laid down in the aforementioned provisions of the TKG, of providers of publicly available telecommunications services (‘telecommunications providers’) to retain telecommunications traffic data does not infringe EU law.

4 This obligation of telecommunications providers to store certain traffic data for a limited period of time was revised by the Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Law introducing a storage obligation and a maximum storage period for traffic data) of 10 December 2015 (‘Law of 10 December 2015’).

5 Such revision was necessary after a judgment of the Bundesverfassungsgericht (Federal Constitutional Court) from 2010 declared the previous provisions governing data retention to be null and void due to a violation of fundamental rights and, moreover, after Directive 2006/24, for the implementation of which those previous provisions had been enacted, was declared to be invalid by the *Digital Rights Ireland and Others* judgment in 2014. The Law of 10 December 2015 is intended to close gaps in law enforcement and at the same time take account of the constitutional requirements and requirements of EU law arising from the aforementioned decisions.

6 In order to answer the question whether the storage obligation laid down in Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG infringes EU law, it is necessary for the Court of Justice to give an interpretation of Directive 2002/58 and, in particular, to clarify how the *Tele2 Sverige and Watson and Others* judgment is to be understood.

Brief summary of the basis for the reference

7 The obligation to retain telecommunications traffic data laid down in the first sentence of Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG restricts the scope of the rights provided for in Article 5(1), Article 6(1) and Article 9(1) of Directive 2002/58.

8 It constitutes an interference with the confidentiality of electronic communications protected by the first sentence of Article 5(1) of the directive and is contrary to the principle, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the user concerned, the traffic data related to electronic communications.

9 In addition, it does not comply with the requirement under Article 6 of the directive that the processing and storage of traffic data are permitted only to the extent necessary and for the duration necessary for the billing and marketing of services and the provision of value added services.

10 In the event that location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, the first sentence of Article 9(1) of Directive 2002/58 provides that such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The legislation also deviates from this requirement in so far as, pursuant to point 2 of Paragraph 113b(1) in conjunction with Paragraph 113b(4) of the TKG, the location data referred to in those provisions must also be stored.

11 The restriction of the rights provided for in Article 5(1), Article 6(1) and Article 9(1) of Directive 2002/58/EC is justified only if Article 15(1) of Directive 2002/58 can be relied on as a basis for the provisions of the first sentence of Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG.

12 Pursuant to that article, 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 the 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. 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 that paragraph must 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 (TEU).

13 According to the statements of the Court of Justice in the *Tele2 Sverige and Watson and Others* judgment, particularly in paragraph 82 et seq. and paragraph 108 et seq. of that judgment, in order for national legislation on data retention pursuant to Article 15(1) of Directive 2002/58 to be permissible, there must be sufficient grounds for that legislation. This means that only those persons for whom there is evidence of a connection to serious criminal offences are covered, that there will be a limitation to the region, period of time and means of communication that are relevant to the reason for the data retention, and that only those data that are indispensable for the investigation of the crimes referred to are covered.

14 The defendant's view that the mere circumstance of using internet access or telephone services is to be regarded as a sufficient ground for the storage is clearly inconsistent with this. Nor is the assumption expressed in the *Tele2 Sverige and Watson and Others* judgment that any retention of data without a reason is generally contrary to EU law called into question by the defendant's reference to the Opinion of the Court of Justice of 26 July 2017 on the Agreement between Canada and the European Union on the transfer of Passenger Name Record data.

It is true that, in the context of the necessity of the interferences entailed by the agreement with the fundamental rights to respect for private life and the protection of personal data, the Court of Justice stressed that the transfer of PNR data to Canada is to take place regardless of whether there is any objective evidence that the passengers are liable to present a risk to public security in Canada. However, this does not constitute retention of data without a reason, because the storage and transfer are connected with the border control checks to which all air passengers who wish to enter or depart from Canada are subject under the requirements laid down by the Canadian law in force. This ground for storage ceases to be applicable when the air passengers depart from the territory. The continued storage after that point in time therefore requires — as a new ground — that objective evidence is identified from which it may be inferred that the air passengers concerned may present a risk in terms of the fight against terrorism and serious transnational crime.

15 If the case-law of the Court of Justice is to be understood as meaning that the retention of data without a reason is not compatible with EU law under any circumstances, the defendant's appeal on a point of law against the contested judgment of the Administrative Court cannot succeed. This is because, as is the case for the Swedish and United Kingdom legislation on data retention, which was the subject of the *Tele2 Sverige and Watson and Others* judgment, the first sentence of Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG requires neither a ground — beyond the mere use of internet access or telephone services — for the storage nor a connection between the data stored and a criminal offence or a risk to public security. Rather, it is legislation which prescribes the storage of a large part of all relevant telecommunications traffic data without a particular reason, in a comprehensive manner and with no differentiation in terms of individuals, time and geography.

16 Irrespective of the statements in the *Tele2 Sverige and Watson and Others* judgment, however, the referring court takes the view that it cannot be ruled out that Article 15(1) of Directive 2002/58 can be relied on as a basis for the obligation to retain telecommunications traffic data without a reason that is laid down in the first sentence of Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG, for the following reasons:

17 First, the relevant provisions of the TKG do not require the storage of all the telecommunications traffic data of all subscribers and registered users in relation to all means of electronic communication. Not only is the content of the communication excluded from the storage obligation, but, in addition, data regarding internet pages accessed, data from email services or data underlying links to or from specific connections in social or ecclesiastical spheres are not to be stored (see Paragraph 113b(5) and (6) of the TKG). Although the exclusion of certain means of communication or categories of data from the storage obligation may not eliminate the risk of a comprehensive profile of the individuals concerned being established, it may at least significantly reduce that risk.

18 Second, the referring court takes the view that the fact that the data retention period of six months to two years (see Article 6 of Directive 2006/24) is significantly reduced to four weeks and ten weeks pursuant to Paragraph 113b(1) of the TKG constitutes an even more important difference between the provisions of the TKG at issue here and the earlier provisions of Directive 2006/24 or the Swedish and United Kingdom legislation which are based on these provisions and which were the subject of the *Tele2 Sverige and Watson and Others* judgment.

19 The shorter the periods during which the traffic data are stored, the lower the risk of a comprehensive profile of the individuals concerned being established. The shorter the storage period, the more incomplete the personal profile, as an inevitable consequence, and the lower the intensity of the interference with fundamental rights.

20 Third, the provisions of the TKG at issue here are subject to strict restrictions with regard to the protection of the data stored and access to them. On the one hand, the provisions in Paragraph 113d et seq. of the TKG ensure effective protection of retained data against risks of misuse and against any unlawful access to those data. On the other hand, the retained data may, pursuant to Paragraph 113c(1) of the TKG, be used only to combat 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*.

21 Under Paragraph 100g(2) of the StPO, the collection of traffic data for law enforcement purposes requires that there is a suspicion of one of the particularly serious criminal offences definitively specified in the law, that the offence is particularly serious in the individual case, that the investigation of the facts of the case or the determination of the whereabouts of the accused would otherwise be significantly impeded or futile, and that the collection of the data is proportionate to the importance of the matter. The collection or use of traffic data of the persons subject to an obligation of professional secrecy referred to in points 1 to 5 of the first sentence of Paragraph 53(1) of the StPO, which include lawyers, doctors or journalists, for example, is impermissible pursuant to Paragraph 100g(4) of the StPO. Paragraph 101a(1) of the StPO also contains a provision stipulating judicial authority for the collection of traffic data pursuant to Paragraph 100g of the StPO.

22 It is true that these rules for restricting access are not applicable to the Internet Protocol address allocated to the subscriber for internet use. This is because, pursuant to point 3 of Paragraph 113c(1) of the TKG, those addresses may also be used in the context of the provision of inventory data information for the prosecution of any criminal offence, maintaining public order and security and generally carrying out the tasks of the intelligence services. However, it must be assumed that information specifying which subscriber was registered on the internet at an Internet Protocol address that was already known does not allow the creation of personal profiles and profiles of the movements of a data subject.

23 Even if SpaceNet's argument were to be accepted and it were to be assumed that increasingly technical procedures are being used, where an Internet Protocol address can no longer be clearly attributed to a specific telecommunications connection and can only be attributed to a relatively large group of connections, and the inventory data information has therefore developed into a measure involving a considerable 'spread', the degree of interference that such inventory data information entails is still significantly lower than that which exists in the consultation and use of the actual telecommunications traffic data.

24 Fourth, the fact that the national legislature has thus complied with the obligations to act arising for the Member States from the right to security guaranteed by Article 6 of the Charter also militates in favour of the assumption that Article 15(1) of Directive 2002/58 can be relied on as a basis for the obligation to retain telecommunications traffic data without a reason, as laid down in the first sentence of Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG. In the *Digital Rights Ireland and Others* judgment, the Court of Justice expressly mentioned Article 6 of the Charter and pointed out in that regard that the fight against international terrorism in order to maintain international peace and security constitutes an EU objective of general interest and that the same is true of the fight against serious crime in order to ensure public security.

25 Against that background, the referring court is uncertain as to whether the case-law of the Court of Justice to date must be understood as meaning that Article 15(1) of Directive 2002/58 cannot be relied on as a basis for the retention of data without a reason not only in the specific form which it takes in Directive 2006/24 and the Swedish and United Kingdom legislation based thereon, but also generally. The reason for this is that the basic concept of data retention cannot be reconciled with the Court of Justice's unqualified requirement that the data to be stored must be differentiated according to individuals, periods of time and geographical areas.

26 The referring court also takes the view that the requirement to strike a balance between the obligation of the Member States to ensure the security of individuals within their territory and observance of the fundamental rights enshrined in Articles 7 and 8 of the Charter also militates against the assumption that the storage of traffic data without a reason is, per se, incompatible with the Charter.

27 The referring court cannot therefore clearly infer from the case-law of the Court of Justice that national legislatures should no longer have the possibility, on the basis of an overall assessment, of introducing the retention of data without a reason, supplemented, where appropriate, by strict access rules, in order to take account of the specific risk potential associated with the new means of telecommunication.

28 Fifth, the referring court points out that, in the event that it is generally not possible to rely on Article 15(1) of Directive 2002/58 as a basis for the retention of data without a reason and, as a result, the specific rules governing the means of communication covered, the categories of data to be stored, the storage period, the

conditions for access to the stored data and protection against the risks of misuse are irrelevant, the national legislature's leeway in an area of law enforcement and national security, which in any event remains, in principle, the sole responsibility of each Member State pursuant to the third sentence of Article 4(2) TEU, would be significantly restricted.

29 Sixth, finally, the referring court takes the view that, in the light also of the more recent case-law of the European Court of Human Rights ('ECtHR'), the question whether the statements of the Court of Justice in the *Tele2 Sverige and Watson and Others* judgment are to be understood as prohibiting the Member States from relying on Article 15(1) of Directive 2002/58 as a basis for introducing an obligation to store telecommunications traffic data without a reason has not been clarified.

30 Most recently, the ECtHR ruled in a judgment of 19 June 2018 that the Swedish legislation on the bulk interception of transborder data flows is in line with Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). The ECtHR stated that, in view of the current threats facing many 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 data are transmitted, 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 (ECtHR, judgment of 19 June 2018 — No 35252/08 [ECLI: CE:ECHR:2018:0619JUD003525208], *Centrum för Rättvisa v. Sweden* — paragraph 112). In so far as the ECtHR refers to the unpredictability of the routes via which electronic data are transmitted and to advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, it emphasises, even more strongly than the Court of Justice of the European Union, the specific risk potential associated with the new means of telecommunication.

31 The referring court makes reference to recital 11 of Directive 2002/58 and Article 52(3) of the Charter, from which it follows that the necessary consistency between the rights enshrined in the Charter and the corresponding rights guaranteed by the ECHR must be established without thereby adversely affecting the autonomy of EU law and that of the Court of Justice of the European Union.

32 Finally, the referring court cites other pending preliminary ruling proceedings concerning an interpretation of the *Tele2 Sverige and Watson and Others* judgment, that is to say, the question whether a general prohibition on the retention of data without a reason — which cannot be overcome either in the light of the seriousness of the threats to national security to be combated or in the context of 'being compensated for' by rules restricting access and stringent security requirements — can be derived from that judgment.

33 The referring court cites the request for a preliminary ruling from the Investigatory Powers Tribunal — London (United Kingdom) (C-623/17), the request for a preliminary ruling from the Conseil d'État (Council of State) (France) (C-511/18 and C-512/18) and the request for a preliminary ruling from the Cour constitutionnelle (Constitutional Court) (Belgium) (C-520/18).