EUROPEAN COMMISSION

Brussels, 09 February 2018
sj.f(2018)865066

Court procedural document

TO THE PRESIDENT AND MEMBERS OF THE COURT OF JUSTICE

WRITTEN OBSERVATIONS

Submitted pursuant to Article 23 of the Statute of the Court

by the European Commission, represented by Martin WASMEIER, Piedade COSTA DE OLIVEIRA, Herke KRANENBORG and Daniele NARDI, acting as agents, with a postal address for service in Brussels at the Legal Service, *Greffe Contentieux*, BERL 1/169, 200, rue de la Loi, 1049 Brussels, who consent to service by e-Curia,

in Case C-623/17

concerning a reference to the Court under Article 267 TFEU by the Investigatory Powers Tribunal of the United Kingdom for a preliminary ruling in the proceedings pending before that court between

Privacy International

(applicant in the main proceedings)

and

(1) Secretary of State for Foreign and Commonwealth Affairs
(2) Secretary of State for the Home Department
(3) Government Communications Headquarters
(4) Security Service
(5) Secret Intelligence Service

(respondents in the main proceedings)

on the interpretation of Article 4(2) TEU and Articles 1(3) and 15(1) of Directive 2002/58/EC.

Contents

1. LEGAL CONTEXT 3

1.1. Union law 3

1.2. National legislation 5

2. THE FACTS IN THE MAIN PROCEEDINGS AND THE QUESTIONS REFERRED FOR A PRELIMINARY RULING 6

3. IN LAW 9

3.1. The first question 9

3.1.1. The Tele2/Watson ruling 10

3.1.2. Applicability of the Tele2/Watson reasoning to this case 12

3.1.3. Subsidiary considerations 15

3.2. The second question 18

3.2.1. The requirements set out in the Tele2/Watson ruling 18

3.2.2. Applicability of the Tele2/Watson conditions in this case 20

4. CONCLUSIONS 22

The Commission has the honour to submit the following observations:

1. LEGAL CONTEXT

1.1. Union law

1. The request for a preliminary ruling concerns the interpretation of Article 4(2) TEU and Articles 1(3) and 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L201, 31.7.2002, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L337, 18.12.2009, p. 11) (hereinafter: 'Directive 2002/58').

2. Article 4(2) TEU reads as follows:

> '[…]
>
> 2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.
>
> […]'

3. Article 1 of Directive 2002/58, headed 'Scope and aim', provides as follows:

> '1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.
>
> 2. The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.
>
> 3. This 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.'

4. Article 5 of Directive 2002/58, headed 'Confidentiality of the communications', provides as follows:

> '1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
>
> […]
>
> 3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'

5. Article 6 of Directive 2002/58, headed 'Traffic data', provides as follows:

> '1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).
>
> 2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.
>
> 3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.
>
> […]
>
> 5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public

communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.'

6. Article 15 of that Directive, headed 'Application of certain provisions of Directive [95/46]', states:

'1. 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]. 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.

[…]

1b. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

[…]'

1.2. National legislation

7. Section 94 of the UK Telecommunications Act 1984 ('the 1984 Act') provides as follows:

'Directions in the interests of national security etc.

(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be [necessary] in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

(2) If it appears to the Secretary of State to be [necessary] to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.

[(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.]

(3) A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under [Part 1 or Chapter 1 of Part 2 of the Communications Act 2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network].

(4) The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.

(5) A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

(6) The Secretary of State may, with the approval of the Treasury, make grants to [providers of public electronic communications networks] for the purpose of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given under this section.

(7) There shall be paid out of money provided by Parliament any sums required by the Secretary of State for making grants under this section.

(8) This section applies to [OFCOM and to providers of public electronic communications networks.]'

The full text of Section 94, including footnotes to the parts between square brackets, can be found in **Annex A.3**.

2. THE FACTS IN THE MAIN PROCEEDINGS AND THE QUESTIONS REFERRED FOR A PRELIMINARY RULING

8. The facts in the main proceedings can be summarised as set out below. For a more elaborate description of the facts, reference is made to the order for reference (in particular paragraphs 6 to 22) and the two judgments of the Investigatory Powers Tribunal (the 'referring court') of, respectively, 17 October 2016 and 8 September 2017 (see **Annex A.1** and **A.2**).

9. Pursuant to section 94 of the 1984 Act the UK Secretary of State may, after consultation with an operator of a Public Electronic Communications Network (PECN), give that operator such general or specific directions as appear to the Secretary of State to be necessary in the interests of national security or relations with a foreign government.

10. On the basis of the directions made by the Secretary of State (see **Annex A.4** for examples) the UK Security and Intelligence Agencies acquire Bulk Communications Data (BCD) from PECN operators. These Security and Intelligence Agencies (hereafter: 'SIAs') are the Government Communications Headquarters (GCHQ), the Security Service (MI5) and the Secret Intelligence Service (MI6). GCHQ has acquired BCD since 2001 and the Security Service (MI5) since 2005. MI6 does not collect or hold BCD (see the ruling of the referring court of 17 October 2016, **Annex A.1**, pt. 19 on p. 10).

11. BCD is non-targeted personal data held by PECN operators which includes traffic data and service use information (the 'who, where, when and how' of a communication), but not the content of communications.[1] The PECN operators are not required to retain the BCD after its transmission to the SIAs.

12. After acquisition of the BCD by the SIAs, the data is retained by the SIAs and interrogated with techniques that are mostly non-targeted, i.e. not directed at specific, known targets (see paragraph 20 of the order for reference). This non-targeted nature is a fundamental feature of the SIAs' techniques for interrogating BCD. According to the referring Court, basing itself on a report published by David Anderson QC in 2016 (the 'Anderson Report'), only a 'miniscule quantity' of the collected data is ever examined (see paragraph 20 of the order for reference).

13. The applicant in the national proceedings before the referring court submits that the acquisition of (and access to and use of) BCD is unlawful under Union law, in particular in the light of the *Tele2/Watson* ruling of the Court of Justice of 21 December 2016 (C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen*

---

[1] The notions of 'traffic data' and 'service use information' are defined in paragraph 3.5.1, section 21(4) of the Regulation of Investigatory Powers Act 2000 (RIPA), see p. 44 of the judgment of the referring Court of 17 October 2016, **Annex A.1**.

and *Secretary of State for the Home Department v Watson and others*, ECLI:EU:C:2016:970).

14. In the *Tele2/Watson* ruling the Court of Justice concluded that national legislation requiring telecom operators to retain traffic and location data and setting out the conditions for access to such data by competent authorities for the purpose of combating crime fell within the scope of Directive 2002/58. The Court set out substantive and procedural conditions which should govern the access of the competent national authorities to the retained data (see paragraph 118 and further of the *Tele2/Watson* ruling).

15. The respondents in the national proceedings basically argue that the *Tele2/Watson* ruling concerned national legislation which served the purpose of fighting crime, being different from the national measure at issue in this case which serves purposes of national security. According to the respondents the present matter requires separate consideration and, also with a view to Article 4(2) TEU, should be considered as falling outside the scope of Directive 2002/58.

16. As the matter concerns a question of interpretation of Union law, the referring court decided to refer two questions to the Court of Justice. However, before formulating those questions, the referring court lists the circumstances in the light of which it considers the questions should be assessed by the Court of Justice:

> '*a. the SIAs' capabilities to use BCD supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;*
>
> *b. a fundamental feature of the SIA's use of the BCD is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of the BCD in one place. Its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;*
>
> *c. the provider of an electronic communications network is not thereafter required to retain the BCD (beyond the period of their ordinary business requirements), which is retained by the State (the SIAs) alone;*

d. the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of BCD by the SIAs are consistent with the requirements of the ECHR; and

e. the referring court has found that the imposition of the requirements specified in [paras] *119-125 of the* [*Tele2/Watson* judgment of the Court of Justice]*, if applicable, would frustrate the measures taken to safeguard national security by the SIAs, and thereby put the national security of the United Kingdom at risk*'.

17. The 'reserved issues' referred to in point d concern the proportionality of the measure and the arrangements as to transfer of data to third parties (see paragraph 3 of the judgment of the referring court of 8 September 2017, **Annex A.2**).

18. The two questions referred to the Court of Justice are the following:

"1. *Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications* […]*, does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies* […] *of a Member State fall within the scope of Union law and of* [Directive 2002/58]*?*

2. *If the answer to Question (1) is 'yes', do any of the Watson Requirements, or any other requirements in addition to those imposed by the* [European Court of Human Rights (ECHR)]*, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the SIAs to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?*"

3. IN LAW

3.1. The first question

19. With its first question the referring court wants to know whether a requirement in a direction by the UK Secretary of State to a telecom operator to provide BCD to the SIAs falls within the scope of Directive 2002/58, having regard to Article 4(2) TEU and Article 1(3) of Directive 2002/58.

20. In the Commission's view, it follows from the reasoning of the Court of Justice in the *Tele2/Watson* ruling that the first question should be answered in the affirmative.

3.1.1. The Tele2/Watson ruling

21. In the *Tele2/Watson* ruling the Court of Justice clarified the meaning of Article 1(3) of Directive 2002/58 which excludes from the scope of the Directive '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'.

22. The national legislation at issue in the *Tele2/Watson* ruling entailed requirements on telecom operators to retain traffic and location data as well as conditions for access to such data by competent authorities for the purpose of combating crime. Under Article 1(3), such activities could be seen as falling outside the scope of the Directive: first, at the time Directive 2002/58 was adopted, cooperation in criminal matters was not covered by the Treaty establishing the European Community and, second, activities of the State in areas of criminal law were explicitly excluded from the scope of the Directive.[2]

23. However, despite the wording of Article 1(3), the Court of Justice concluded, in *Tele2/Watson,* that the national legislation at issue fell within the scope of Directive 2002/58. The Court came to that conclusion by looking at the general structure of the Directive. The reasoning of the Court of Justice can be found in paragraphs 67 to 81 of the judgment.

24. In particular, the Court of Justice referred to Article 15(1) of Directive 2002/58 which enables Member States to adopt legislative measures to restrict the scope of certain rights and obligations provided for in the Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard, amongst others, national security (i.e. State security), defence,

---

[2] Cooperation in criminal matters was not covered by the Treaty establishing the European Community, but was not excluded from *Union* law as such, as the EU competence in that area was laid down in the former Treaty on the European Union.

public security, and the prevention, investigation, detection and prosecution of criminal offences.

25. On the basis of Article 15(1), the obligations to ensure the confidentiality of communications (see Article 5(1)), and to erase or anonymise data when it is no longer needed for the commercial objectives of the telecom operator (see Article 6), for example, can be restricted.

26. The Court acknowledged that the legislative measures 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 (paragraph 72) and that there is a substantial overlap between the objectives which the measures referred to in Article 15(1) must pursue and the objectives pursued by the activities referred to in Article 1(3) of Directive 2002/58 (see point 21 above).

27. However, the Court considered that the legislative measures referred to in Article 15(1) govern, for the purposes mentioned in that provision, the activity of electronic communications service providers (paragraph 74). As follows from Article 3 of Directive 2002/58, the activities of these providers are precisely what Directive 2002/58 is regulating (paragraph 74).

28. According to the Court, the national measures at issue in the *Tele2/Watson* ruling should not be excluded from the scope of Directive 2002/58, for otherwise Article 15(1) would be deprived of any purpose (see paragraph 73).

29. The Court considered that the scope of Directive 2002/58 extends, in particular, to a legislative measure requiring retention of traffic and location data by the electronic communications service providers, but also to a legislative measure, such as the one at issue in the *Tele2/Watson* ruling, relating to the access of the national authorities to the retained data (paragraphs 75 and 76).

30. In that respect, the Court pointed out that the protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies (paragraph 77). Furthermore, the Court held that since the data in the *Tele2/Watson* case was retained for the sole purpose of making that data accessible to the competent national authorities, the

national legislation imposing the retention of data necessarily entailed, in principle, the existence of provisions relating to access by the authorities to such data (paragraph 79).

3.1.2. Applicability of the Tele2/Watson reasoning to this case

31. In this case, the objective pursued by the national measure at issue (the direction of the UK Secretary of State based on section 94 of the 1984 Act) is in principle different from the objective pursued by the measure at issue in the *Tele2/Watson* case as it concerns the safeguarding of national security.

32. However, like the objective of combating crime, national security is referred to in both Article 1(3) and Article 15(1) of Directive 2002/58.[3] Therefore, the Commission takes the view that the reasoning of the Court of Justice in the *Tele2/Watson* ruling based on the general structure of Directive 2002/58 should, in principle, be applied in this case. The fact that Article 4(2) TEU states that national security remains the sole responsibility of each Member State in principle does not, in the Commission's view, have a bearing on the reasoning of the Court of Justice in the *Tele2/Watson* case as regards the applicability of the Directive.

33. As the Court pointed out in the *Tele2/Watson* ruling, Directive 2002/58 regulates the activities of the providers of electronic communications services. It follows that the activity of the PECN operators consisting in the transmission of BCD to the SIAs is governed by the Directive. Since such transmission departs at least from the obligation in Article 5 of the Directive to ensure the confidentiality of communications, and possibly also from the obligation in Article 6 of the Directive, to erase data, the PECN operators can only provide the information on the basis of a national legislative measure within the meaning of Article 15(1) of Directive 2002/58.

34. The Commission would submit, however, that if it is confirmed that the retention and subsequent use of the data by the SIAs after their receipt are considered to be activities of the State for the purpose of national security and no further involvement of the PECN operators is required, those activities of the SIAs would normally fall outside the scope of Directive 2002/58. In that respect, in contrast to the situation in

Tele2/Watson (see paragraph 79), the provisions on access and further use in this case are not a necessary part of the obligation imposed on telecom operators to retain the data. In this case the obligation on the PECN operators is to transfer BCD to the SIAs, after which the operators have no further involvement in the processing of the data by the SIAs.

35. The consequences of considering the mandatory transmission of BCD by the PECN operators to the SIAs as falling within the scope of Directive 2002/58 will be further discussed when answering the second question of the referring court.

36. The referring court considers that the transmission of BCD by the PECN operators should be seen as advancing an essential State function, in this case the protection of national security, through a framework established by the public authorities that relates to public security (see paragraph 36 of the order for reference). According to the referring court, following the reasoning of the Court of Justice in its rulings from 2006 on the transfer of Passenger Name Records (PNR) by airline companies to the US (C-317/04 and C-318/04, *European Parliament v Council* and *v European Commission*, ECLI:EU:C:2006:346, hereinafter: the 'US PNR rulings'), the activity should be considered as falling outside the scope of Directive 2002/58, on the basis of Article 1(3) thereof.[4]

37. The Commission takes the view that the reasoning of the Court of Justice in the US PNR rulings cannot be applied in the context of this case, in particular in the light of the Court's ruling in *Tele2/Watson*.

38. In this respect, the Commission refers to the opinion of AG Mengozzi on the draft agreement between the EU and Canada on the transfer of PNR data (A-1/15, ECLI:EU:C:2016:656). In his opinion, the AG emphasised the specific context of the US PNR rulings. The US PNR rulings, which were delivered well before the adoption of the Treaty of Lisbon, concerned an adequacy decision relating to the processing of data in the context of an agreement with the United States for the

---

[3] Article 1(3) of Directive 2002/58 refers to 'state security', which in these observations is treated as a synonym of 'national security'.

[4] The US PNR rulings concerned, inter alia, an interpretation of Article 3(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of persona data and on the free movement of such data (OJ 1995, L281, p. 31) (hereinafter: 'Directive 95/46'). Article 3(2) of Directive 95/46 corresponds with Article 1(3) of Directive 2002/58.

transfer of PNR which could not be associated with the supply of services, but fell within a framework established by the public authorities that related to public security (see point 85 of the AG's opinion). According to the AG, the Court logically concluded that the subject matter *of the adequacy decision* fell outside the scope of Directive 95/46/EC. However, the AG warned against drawing any definitive conclusions outside the specific context of the case.

39. The Commission concurs with that conclusion, in particular in the light of the *Tele2/Watson* ruling.

40. In *Tele2/Watson*, the Court did not rely on the reasoning used in the US PNR rulings when determining whether the national measures at issue fell within the scope of Directive 2002/58. On the contrary, in paragraphs 69 and 70 of the ruling the Court made a clear distinction between activities of the State and activities of telecommunications service providers. Article 1(3) of Directive 2002/58 excludes 'activities of the State' from the scope of the Directive (paragraph 69), whilst the activities of telecommunications service providers are regulated by, and thus fall within the scope of the Directive (paragraph 70). The Court concluded that the national legislative measures at issue in *Tele2/Watson* fell within the scope of Directive 2002/58 because they concerned the activity of the telecommunications providers. The fact that the purpose of the retention (and the subsequent access by competent authorities) was to combat crime did not have a bearing on that finding.[5]

41. Finally, point 29 of the order for preliminary reference refers to point 5 of Section C of the Decision of the Heads of State of Government, meeting within the European Council, concerning a new settlement for the United Kingdom in the European Union, of 19 February 2016. The Commission wishes to point out that that Decision has never taken effect (see point 2 of Section E of the Decision)[6] and should therefore not be taken into consideration by the Court.

---

[5] On Article 3(2) of Directive 95/46, which corresponds with Article 1(3) of Directive 2002/58, the Court of Justice has, in more general terms, considered that the clause should be interpreted strictly. See C-73/16, *Puškar*, ECLI:EU:C:2017:725, para 38.

[6] See also point 4 of the European Council conclusions of 18-19 February 2016, according to which the whole set of arrangements referred to in point 2 of these conclusions, of which the Decision was part, ceased to exist after a referendum in the UK the result of which was for the United Kingdom to leave the EU.

42. On the basis of all the considerations set out above, the Commission would suggests that the Court answer the first question as follows:

'A requirement in a direction by a Secretary of State to a provider of an electronic communications service that it must provide bulk communications data to the Security and Intelligence Agencies of that Member State for reasons of national security, such as in the present case, falls within the scope of Directive 2002/58 in so far as the transmission by the provider is concerned.'

3.1.3. Subsidiary considerations

43. In the event that the Court of Justice does not agree with the above conclusion, but rather considers that, in principle, a national measure requiring a telecom operator to provide data to the national security agencies, on grounds of national security, falls outside the scope of Directive 2002/58, the Commission submits that the following considerations should be taken into account in order to enable the national court to determine whether the situation before it is covered by such an exclusion.

44. At the outset, the Commission wishes to stress that the statement that national security remains the sole responsibility of Member States, in the third sentence of Article 4(2) TEU, must be read in the light of the principle of respect for the national identity of Member States of which national security is an element (see Article 4(2) TEU, first and second sentence).[7]

45. Article 4(2) TEU should, in any event, not be read in such a way as to confer on Member States a power to depart from their duties under EU law based on the mere fact that a decision concerns State security (see Case C-300/11, *ZZ*, EU:C:2013:363, paragraph 38, with reference to C-387/05, *Commission v Italy*, ECLI:EU:C:2009:781, paragraph 45; Case C-273/97, *Sirdar*, EU:C:1999:523, paragraph 16; opinion of AG Kokott in Case C-187/16, *Commission v Austria*, EU:C:2017:578, point 46) In its judgment in Case 461/05, *Commission v Denmark* (EU:C:2009:783, paragraph 51), the Court explained:

> 'It cannot be inferred that the Treaty contains an inherent general exception excluding all measures taken for reasons of public security from the scope of

---

[7] This principle was already enshrined in ex-Article 6(3) TEU, i.e. before the adoption of the Lisbon Treaty (respectively Article F(1) of the Maastricht Treaty).

> Community law. The recognition of the existence of such an exception, regardless of the specific requirements laid down by the Treaty, would be liable to impair the binding nature of Community law and its uniform application (see Case C-186/01 *Dory* [2003] ECR I-2479, paragraph 31 and case-law there cited).'[8]

46. In order to determine whether a Member State can claim sole responsibility for a certain matter, it is necessary to assess whether the measure in question *genuinely* meets the objective of safeguarding national security. According to the Commission, this first requires a clarification of the notion of 'national security' as contained in Article 4(2) TEU, and as reflected in Article 1(3) of Directive 2002/58. Secondly, it requires an assessment of whether the measure is in fact *capable* of achieving the intended objective.

47. The Commission takes the view that the notion of 'national security' constitutes a concept of Union law which requires an autonomous interpretation. The binding nature of Union law could be seriously undermined if a Member State could avoid the application of Union law simply by stating that a measure serves the objective of national security. That being said, the Commission acknowledges that Member States should enjoy a wide margin of discretion when it comes to defining what they consider to be measures safeguarding national security (see, similarly, the opinion of AG Kokott in Case C-187/16, *Commission v Austria*, EU:C:2017:578, pt. 47).

48. The TEU and the TFEU do not define the notion of 'national security'. Article 4(2) TEU, in the context of the general principle of respect for the national identities of Member States, states that national security is an example of the 'essential State functions'.

49. The Commission considers there to be similarities between the notion of 'national security' and the Member State's 'essential interests of its security' in Article 346(1) TFEU. As regards Article 346(1) TFEU, it is settled case law that the notion of 'security' in that provision constitutes an autonomous concept of Union law (see Case C-273/97, *Sirdar*, EU:C:1999:523, para 16; opinion by AG Kokott on Case C-187/16, *Commission v Austria*, EU:C:2017:578, para 46 et seq.).

---

[8] See also the almost identical reasoning in the judgment in Case C-387/05, *Commission v Italy*, EU:C:2009:781, paragraph 45.

50. From this, it can be derived that the notion of 'national security' relates to the need to preserve and defend a core set of essential interests of the State, which are necessary to ensure its existence and its constitutional order (see e.g. Case C-601/15 PPU, *J.N.*, EU:C:2016:84, paras 64-67). National security could be seen as referring to genuine, present and sufficiently serious threats affecting one of the fundamental interests of the State (see to that effect, *ibid*., para 65).[9]

51. It is for the Member States in each case to offer substantiated evidence to show which national security interests are affected and to what extent compliance with certain obligations under Union law would, in practice, be contrary to those security interests (cf. Case C-474/12, *Schiebel Aircraft*, EU:C:2014:2139, paragraph 34, and opinion of AG Kokott in Case C-187/16, *Commission v Austria*, point 48, and case law cited therein).

52. In the Commission's view, there could be a certain overlap between objectives pursued in the interest of national security and 'ordinary' law enforcement objectives. In particular, the prevention of acts of terrorism might relate to both prevention of criminal offences and prevention of threats to national security.

53. In order to establish whether a national measure constitutes a national security activity or, rather, a law enforcement activity, consideration should be given to the purpose for which data is collected and to whether that purpose is of such a nature that it corresponds to protection of the essential interests of the State. In that respect, certain acts, whilst also criminal, might be of such gravity and of such a nature that they put the fundamental interests of the State at risk. The prevention of such acts can then be considered to serve the interest of national security of the State.

54. Additional important indicators could be the specific features of the authorities that carry out the activity, i.e. the security and intelligence authorities, and, possibly, the use by such authorities of specific working methods, which could include monitoring activities aiming at the prevention of threats to the essential interests of the State. It should, however, be stressed that these two elements, together or in isolation, should not as such be considered conclusive in order to identify a genuine

---

[9] Cf. Judgment in Case C-601/15 PPU, *J.N.*, EU:C:2016:84, paragraphs 64-67 on Article 8(3) of Directive 2013/33 laying down standards for the reception of applicants for international protection, which in letter e, refers to the protection of national security or public order.

national security activity. For instance, in the hypothesis that certain tasks were entrusted to intelligence authorities rather than to the police, this organisational setup would not in itself rule out the possibility that the activities of the intelligence authorities could, in reality, be considered as being carried out predominantly with a view to the fight against serious crime or other law enforcement. This point is illustrated by the general notion of 'competent authorities' in Article 87(1) TFEU.

55. Once it is established that a measure pursues a genuine national security interest, the Member States should show that the measure is in fact capable of achieving the intended purpose.

56. It should be for the referring court to assess whether the national measure at issue genuinely serves the interests of national security, taking into account the above considerations.

3.2. The second question

57. With its second question the referring court wants to know, in the event that the first question is answered in the affirmative, whether, and, if so, how and to what extent, the substantive and procedural requirements set out by the Court of Justice in the *Tele2/Watson* ruling in relation to access to retained data by competent authorities also apply to a direction of the Secretary of State as in this case.

3.2.1. The requirements set out in the Tele2/Watson ruling

58. In paragraphs 113 to 125 of the *Tele2/Watson* ruling the Court of Justice addressed the implications of Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights, for national legislation on access by national authorities to data which telecommunications operators are required to retain, for the objective of combating crime.

59. According to the Court of Justice 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 (see paragraph 117). A measure of that kind must be legally binding under domestic law (*ibid.*).

60. In order to ensure that access to the retained data is limited to what is strictly necessary, the national legislation cannot be limited to requiring only that access

should serve one of the objectives referred to in Article 15(1) of Directive 2002/58. According to the Court, the national legislation also has to lay down substantive and procedural conditions governing the access of the competent national authorities to the retained data (see paragraph 118).

61. In that respect, in paragraphs 119 to 125 of the ruling, the Court of Justice identified the following substantive and procedural conditions:

a) Access should be granted only to retained data of individuals suspected of planning, committing or having committed a serious crime or being implicated in one way or another in such a crime (paragraph 119). In particular situations access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities. As examples, the Court mentions 'vital national security, defence or public security interests' (*ibid.*).

b) Access by the competent national authorities to retained data should be subject to prior review by a court or by an independent administrative body, following a reasoned request by those authorities, except in cases of validly established urgencies (paragraph 120).

c) The competent national authorities to whom access has been granted should notify the persons affected as soon as that notification is no longer liable to jeopardise the investigations being undertaken (paragraph 121).

d) A high level of protection and security of data retained by telecommunication providers should be ensured by means of appropriate technical and organisation measures. This, according to the Court, means that the data should be retained within the Union (paragraph 122).

e) Member States should ensure review, by an independent authority, of compliance with the level of protection guaranteed by Union law (paragraph 123). This requirement stems from Article 8(3) of the Charter of Fundamental Rights.

3.2.2. Applicability of the Tele2/Watson conditions in this case

62. The situation in this case differs from the situation in *Tele2/Watson* not only in terms of the objective pursued by the national measure concerned, but also in the way in which the measure is organised.

63. In this case, the national measure requires the PECN operators to transmit the BCD to the SIAs, following which the data are retained by the SIAs and further interrogated (see point 12 above). In the *Tele2/Watson* case, in contrast, the national measures required the telecommunications operators to retain the data, to which the competent national authorities could have access.

64. It follows that, if the response to the first question in the request for a preliminary ruling is that only the transmission of the BCD by the PECN operator to the SIAs is covered by Directive 2002/58, and not the retention and subsequent use of the data by the SIAs, the condition set out in point d of point 61 above (retention within the Union) is not relevant, since the data are stored by the SIAs who would not in that respect be subject to the security requirements in Directive 2002/58.

65. As regards the other conditions set out in point 61 above, in as far as relevant for the activities of the PECN operators, the Commission takes the view that those conditions do not necessarily apply as such to the present situation. This is due, not only to the different factual situation, but also to the specific features of the objective of safeguarding national security, and the fact that according to Article 4(2) TEU national security remains the sole responsibility of Member States. This could merit a different approach with regard to the conditions formulated by the Court in the *Tele2/Watson* ruling as set out in point 61 above.

66. That being said, as stated in point 33, the PECN operators can only transmit the BCD to the SIAs if the conditions of Article 15(1) of Directive 2002/58 are met. Article 15(1), read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights, requires the following three main conditions to be met, in order for the obligation on PECN operators to transmit BCD to the SIAs to be lawful:

a) the measure should be laid down in a legislative measure which meets the requirements of quality of law;

b) the measure should genuinely meet the objective of safeguarding national security;

c) the measure should be necessary, appropriate and proportionate to achieve the objective of safeguarding national security.

67. In order to satisfy the first condition, the obligation on PECN operators to transmit BCD to the SIAs should be laid down in a legislative measure which meets the requirements of quality of law and lays down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards (see *Tele2/Watson*, paragraphs 109 and 117, see also the opinion of the Court of Justice on the draft agreement between the EU and Canada on the transfer of PNR data, A-1/15, ECLI:EU:C:2017:592, paragraph 141).

68. In this case, the requirement on PECN operators to transmit data to the SIAs is laid down in a direction of the UK Secretary of State based on section 94 of the 1984 Act. It is for the national court to assess whether that measure can be considered as legally binding under domestic law. Next, it should be assessed whether clear and precise rules are laid down governing the scope and application of the measure.

69. The second condition requires that the measure genuinely pursues the objective of safeguarding national security. The assessment of whether this condition is met is to a large extent similar to the assessment set out in section 3.1.3 above. The Commission refers the Court to its analysis in that section.

70. As to the third condition (the measure should be appropriate, necessary, and proportionate to achieve the objective of safeguarding national security) in the Commission's view, where the national measure genuinely pursues and is capable of achieving the objective of safeguarding national security, the further assessment of proportionality should be limited to considering whether there has been a manifest error of assessment or a misuse of powers (see, by analogy, Case C-266/05 P, *José María Sisón*, ECLI:EU:C:2007:75, para 64).

71. In this case, the question would be whether the requirement on a PECN operator to transmit BCD to the SIAs would, as such, constitute a manifest error of assessment under the principle of proportionality or a misuse of powers. In that respect, the level of intrusion constituted by the transmission of the BCD as such, the nature of the data, the number of persons concerned, the purpose of the transmission and the necessary working methods of the SIAs should all be taken into account.

72. It is the task of the referring court to determine whether and to what extent the national legislation at issue satisfies the requirements stemming from Article 15(1) of Directive 2002/58, as set out above (see also *Tele2/Watson*, pt. 124).

73. On these grounds, the Commission would suggest that the Court answer the second question as follows:

'Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as requiring that a direction by a Secretary of State to a provider of an electronic communications service that it must provide bulk communications data to the Security and Intelligence Agencies of that Member State for reasons of national security is based on a legislative measure which meets the requirements of quality of law, genuinely meets the objective of safeguarding national security, and is necessary, appropriate and proportionate to achieve the objective of safeguarding national security.'

4. CONCLUSIONS

74. On the basis of these observations, the Commission would suggest that the Court of Justice answer the two questions from the referring court as follows:

'1. A requirement in a direction by a Secretary of State to a provider of an electronic communications service that it must provide bulk communications data to the Security and Intelligence Agencies of that Member State for reasons of national security, such as in the present case, falls within the scope of Directive 2002/58 in so far as the transmission by the provider is concerned.

2. Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as requiring that a direction by a Secretary of State to a provider of an electronic communications service that it must provide bulk communications data to the Security and Intelligence

Agencies of that Member State for reasons of national security is based on a legislative measure which meets the requirements of quality of law, genuinely meets the objective of safeguarding national security, and is necessary, appropriate and proportionate to achieve the objective of safeguarding national security.'

Martin WASMEIER, Piedade COSTA DE OLIVEIRA, Herke KRANENBORG and Daniele NARDI

Agents of the Commission