OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 15 January 2020 (1)

Case C-623/17

Privacy International

v

Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

(Request for a preliminary ruling from the Investigatory Powers Tribunal (United Kingdom))

(Reference for a preliminary ruling — Processing of personal data and the protection of privacy in the electronic communications sector — Directive 2002/58/EC — Scope of application — Article 1(3) — Article 15(3) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 51 and Article 52(1) — Article 4(2) TEU — General and indiscriminate transmission to the security services of connection data of users of an electronic communications service)

1. In recent years the Court of Justice has maintained a consistent line of case-law on the retention of and access to personal data, which includes the following landmark rulings:

The judgment of 8 April 2014, *Digital Rights Ireland and Others*, (2) in which the Court held that Directive 2006/24/EC (3) was invalid because it permitted disproportionate interference with the rights recognised by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

The judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, (4) in which the Court interpreted Article 15(1) of Directive 2002/58/EC. (5)

The judgment of 2 October 2018, *Ministerio Fiscal*, (6) in which the Court confirmed the interpretation of the same provision in Directive 2002/58.

2. The authorities in some Member States are concerned by these judgments (particularly by the second of them) because, in their view, the result is to deprive them of an instrument which they consider essential to the safeguarding of national security and countering terrorism. That is why some of those Member States argue that the case-law in question should be overturned or qualified.

3. That same concern has been highlighted by certain courts of the Member States in four references for preliminary rulings, (7) on all of which I deliver my Opinions today.

4. Primarily, the four cases pose the problem of the application of Directive 2002/58 to activities related to national security and counter-terrorism. If that directive were to apply in this field, one would then have to clarify the extent to which Member States can restrict the privacy rights that it protects. Finally, it will be necessary to examine to what extent the various national laws (the legislation of the United Kingdom, (8) Belgium (9) and France (10)) on this subject comply with EU law as interpreted by the Court of Justice.

I. Legislative framework

A. EU law

5. I refer to the relevant point of my Opinion in Joined Cases C-511/18 and C-512/18.

B. National law (applicable to the dispute in this case)

1. Telecommunications Act 1984 (11)

6. Pursuant to section 94, the Secretary of State may give an operator of a public electronic communications network such general or specific directions 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. Data Retention and Investigatory Powers Act 2014 (12)

7. Section 1 provides as follows:

The Secretary of State may by notice require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 [("RIPA")] .

A retention notice may—

relate to a particular operator or any description of operators,

require the retention of all data or any description of data,

specify the period or periods for which data is to be retained,

contain other requirements, or restrictions, in relation to the retention of data,

make different provision for different purposes,

relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.

The Secretary of State may by regulations make further provision about the retention of relevant communications data.

Such provision may, in particular, include provision about—

requirements before giving a retention notice,

the maximum period for which data is to be retained under a retention notice,

the content, giving, coming into force, review, variation or revocation of a retention notice,

the integrity, security or protection of, access to, or the disclosure or destruction of, data retained by virtue of this section,

the enforcement of, or auditing compliance with, relevant requirements or restrictions,

a code of practice in relation to relevant requirements or restrictions or relevant powers,

the reimbursement by the Secretary of State (with or without conditions) of expenses incurred by public telecommunications operators in complying with relevant requirements or restrictions,

…

The maximum period provided for by virtue of subsection (4)(b) must not exceed 12 months beginning with such day as is specified in relation to the data concerned by regulations under subsection (3).

A public telecommunications operator who retains relevant communications data by virtue of this section must not disclose the data except—

in accordance with—

Chapter 2 of Part 1 of [RIPA], or

a court order or other judicial authorisation or warrant, or

as provided by regulations under subsection (3).

The Secretary of State may by regulations make provision, which corresponds to any provision made (or capable of being made) by virtue of subsection (4)(d) to (g) or (6), in relation to communications data which is retained by telecommunications service providers by virtue of a code of practice under section 102 of the Anti-terrorism, Crime and Security Act 2001.'

3. RIPA

8. Section 21 provides:

'…

In this Chapter "communications data" means any of the following—

any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

of any postal service or telecommunications service; or

in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

…

In this section "traffic data", in relation to any communication, means—

any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,

any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,

any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and

any data identifying the data or other data as data comprised in or attached to a particular communication,

…'

9. Section 22 provides that:

This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.

It is necessary on grounds falling within this subsection to obtain communications data if it is necessary—

in the interests of national security;

for the purpose of preventing or detecting crime or of preventing disorder;

in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;

in the interests of public safety;

for the purpose of protecting public health;

for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator—

if the operator is not already in possession of the data, to obtain the data; and

in any case, to disclose all of the data in his possession or subsequently obtained by him.

The designated person shall not grant an authorisation under subsection (3) or give a notice under subsection (4), unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.'

10. Under section 65, a complaint may be made to the Investigatory Powers Tribunal if there is reason to believe that data has been acquired inappropriately.

II. Facts and questions referred

11. According to the referring court, the main proceedings concern the acquisition and use by the United Kingdom Security and Intelligence Agencies ('SIAs') of bulk communications data.

12. That data relates to 'who' is using the telephone and internet, and to 'when, where, how and with whom' they are using it. It includes the location of mobile and fixed-line telephones from which calls are made or received, and the location of computers used to access the internet. It does not include the content of the communications, which may only be obtained under a court order.

13. The applicant in the main proceedings (Privacy International, a non-governmental human rights organisation) has commenced proceedings in the referring court, on the grounds that the acquisition and use of the aforesaid data by the SIAs are in breach of the respect for private life enshrined in Article 8 of the European Convention on Human Rights ('ECHR') and are contrary to EU law.

14. The defendant authorities (13) argue that the exercise of their powers in this field is lawful and essential, in particular, in order to protect national security.

15. According to the information in the order for reference, the SIAs, pursuant to directions given by the Secretary of State under section 94 of the 1984 Act, receive bulk communications data via the operators of public electronic communications networks.

16. That data includes traffic and location data, as well as information on users' social, business and financial activities, communications and travel. Once the data is in their possession, the SIAs retain it securely and use techniques (such as filtering and aggregation) that are non-targeted, that is, not directed at specific, known targets.

17. The referring court finds as a fact that those techniques are essential to the work of the SIAs in countering serious threats to public security, particularly terrorism, espionage and nuclear proliferation. The SIAs' capabilities to acquire and use the data are essential to the protection of the national security of the United Kingdom.

18. In the view of the referring court, the measures at issue are consistent with national law and with Article 8 of the ECHR. However, it has doubts about their compatibility with EU law, in view of the *Tele2 Sverige and Watson* judgment.

19. In that context, the referring court refers the following questions to the Court of Justice for a preliminary ruling:

Having regard to Article 4 TEU and Article 1(3) of Directive [2002/58], 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 ("SIAs") of a Member State fall within the scope of Union law and of Directive [2002/58]?

If the answer to Question (1) is "yes", do any of the *Watson* Requirements, [(14)] or any other requirements in addition to those imposed by the 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?'

20. The background to those questions is set out as follows by the referring court:

the SIAs' capabilities to use [bulk communications data] 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;

a fundamental feature of the SIAs' use of [bulk communications data] is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of [the data] 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;

the provider of an electronic communications network is not thereafter required to retain [bulk communications data] (beyond the period of their ordinary business requirements), which is retained by the State (the SIAs) alone;

the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of [bulk communications data] by the SIAs are consistent with the requirements of the ECHR; and

the national court has found that the imposition of the requirements specified in [the *Tele2 Sverige and Watson* judgment], 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.'

III. Proceedings before the Court of Justice

21. The reference for a preliminary ruling was lodged at the Registry of the Court on 31 October 2017.

22. Written observations have been submitted by the Belgian, Cypriot, Czech, Estonian, French, German and Hungarian Governments, Ireland, the Latvian, Netherlands, Norwegian, Polish, Portuguese, Spanish, Swedish and United Kingdom Governments, and by the European Commission.

23. A public hearing took place on 9 September 2019; it was held jointly with the hearings in Cases C-511/18, C-512/18 and C-520/18, and was attended by the parties to the four references for a preliminary ruling, the governments listed above, the Commission and the European Data Protection Supervisor.

IV. Analysis

A. The scope of application of Directive 2002/58 and the exception for national security (first question referred)

24. In the Opinion which I also deliver today in Joined Cases C-511/18 and C-512/18, I explain why, in my view, Directive 2002/58 'applies, in principle, when electronic services providers are required by law to retain their subscribers' data and to allow public authorities access to it. This position remains unchanged where the requirements are imposed on providers for reasons of national security'. (15)

25. In developing my arguments, I address the impact of the judgment of the Court of 30 May 2006, *Parliament* v *Council and Commission*, (16) and the *Tele2 Sverige and Watson* judgment, and argue for a holistic interpretation that covers both judgments. (17)

26. In that Opinion, having first stated that Directive 2002/58 applies, I examine the exception for national security included in it and the impact of Article 4(2) TEU. (18)

27. Without prejudice to the arguments set out below, I refer to what I have said in that Opinion and in my Opinion in Case C-520/18.

1. The application of Directive 2002/58 in this case

28. Under the legislation at issue in these proceedings, providers of electronic communications services are under an obligation not only to retain, but also to process the data they possess as a consequence of the service they provide to users of public communications networks in the European Union. (19)

29. Those operators are subject to a mandatory requirement to transmit that data to the SIAs. The point at issue here is whether, in view of its purpose, the effect of Article 15(1) of Directive 2002/58 is that that transmission can automatically be excluded from the scope of EU law.

30. In my opinion, it cannot. The retention of that data and its subsequent transmission can be classed as processing of personal data performed by providers of electronic communications services, meaning that these activities naturally fall within the scope of Directive 2002/58.

31. National security concerns cannot, as suggested by the referring court, prevail over that conclusion, with the result that the requirement at issue would not come within the scope of EU law. I reiterate that, in my view, providers are required to process data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, which is precisely the scope of application of Directive 2002/58, as set out in Article 3(1) of the directive.

32. Once that premiss has been established, the next issue for debate is not the activities of the SIAs (which, as I have noted above, could fall outside the scope of EU law if they did not affect electronic communications operators), but the retention and subsequent transmission of the data held by those operators. From this perspective, at stake are the fundamental rights guaranteed by the European Union.

33. Once again, the key factor in resolving this debate is the requirement for general and indiscriminate retention of data to which the public authorities are given access.

2. The invocation of national security

34. As the referring court places particular emphasis in this case on the activities of the SIAs connected with national security, I would like to reproduce some of the points I made on this issue in my Opinion in Joined Cases C-511/18 and C-512/18, which is also delivered today:

'77. National security … is addressed in two ways in Directive 2002/58. First, it is grounds for excluding (from the application of the directive) all activities of the Member States specifically "concerning" it. Secondly, it is grounds for imposing restrictions, which must be adopted by legislative measures, on the rights and obligations provided for in Directive 2002/58, that is, in connection with private or commercial activities falling outside the sphere of activities reserved to the State.

78. To what activities does Article 1(3) of Directive 2002/58 apply? In my opinion, the Conseil d'État (Council of State) itself provides a good example when it cites Articles L. 851-5 and L. 851-6 of the Internal Security Code, referring to "information collection techniques which are applied directly by the State but which do not regulate the activities of providers of electronic communications services by imposing specific obligations on them". …

79. I believe that this is the key to determining the scope of the exclusion provided for in Article 1(3) of Directive 2002/58. The provisions of the directive will not apply to *activities* which are intended to safeguard national security and are undertaken by the public authorities themselves, without requiring the cooperation of private individuals and, therefore, without imposing on them obligations in the management of businesses.

80. The range of public authority activities that are exempt from the general regime governing the processing of personal data must, however, be interpreted narrowly. Specifically, the notion of *national security*, which is the sole responsibility of each Member State under Article 4(2) TEU, cannot be extended to other sectors of public life that are, to varying degrees, related to it.

…

82. I believe … that guidance can be found in the criterion contained in Framework Decision 2006/960/JHA … Article 2(a) of which distinguishes between law enforcement authorities in the broad sense — which include "a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities" — and "agencies or units dealing especially with national security issues". …

…

84. There … is continuity between Directive 95/46 and Directive 2002/58 with regard to the competence of Member States over national security. Neither directive is intended to protect fundamental rights in this specific area, in which Member States' activities are not "governed by [EU] law".

85. The "balance" referred to in recital [11 of Directive 2002/58] arises from the need to respect the competence of the Member States over national security matters, where they exercise that competence *directly, using their own resources*. By contrast, where, even for those same reasons of national security, the involvement of individuals, on whom certain obligations are imposed, is required, that circumstance dictates inclusion within an area (namely the protection of privacy required of those private operators) governed by EU law.

86. Both Directive 95/46 and Directive 2002/58 seek to achieve that balance by allowing the rights of private individuals to be restricted by legislative measures adopted by Member States pursuant to Article 13(1) and Article 15(1) respectively of those directives. On this point there is no difference between them.

…

89. Those public authority activities must necessarily be defined narrowly, so as not to deprive EU privacy law of its effect. Article 23 of Regulation No 2016/679 makes provision — in line with Article 15(1) of Directive 2002/58— for restricting, *by way of a legislative measure*, the rights and obligations established by the regulation, where necessary in order to safeguard, among other objectives, national security, defence or public security. Once again, if the protection of those objectives were sufficient grounds for exemption from the scope of application of Regulation No 2016/679, there would be no need to invoke national security as grounds for introducing legislative measures to restrict the rights guaranteed by that regulation.'

3. The consequences of applying the Tele2 Sverige and Watson judgment to this case

35. The referring court has focused on the interpretation given by the Court in the *Tele2 Sverige and Watson* judgment, and describes the difficulties that it believes would arise if that interpretation were to be applied in this case.

36. The *Tele2 Sverige and Watson* judgment set out the conditions that must be satisfied by national legislation that establishes a requirement to retain traffic and location data for subsequent access by public authorities.

37. Just as in Cases C-511/18 and C-512/18, and for similar reasons, I believe that the national legislation cited in this reference does not satisfy the conditions established in the *Tele2 Sverige and Watson* judgment, because it involves general and indiscriminate retention of personal data that readily provides a detailed account of the life of the persons involved, for a lengthy period of time.

38. In the Opinion in those two cases I consider whether it would be possible to qualify or expand on the case-law set out in that judgment, in view of its consequences for counter-terrorism or the protection of the State from other similar threats to national security.

39. Again, I reproduce some of the points made in that Opinion where, in essence, I argue that, while that case-law can be qualified, its essential content should be endorsed:

'135. While it is difficult, it is not impossible to determine precisely and on the basis of objective criteria the categories of data that it is deemed essential to retain, and the circle of persons who are affected. It is true that the most *practical and effective* option would involve the general and indiscriminate retention of any data that might be collected by the providers of electronic communications services, but … resolving the issue is not a matter of *practical effectiveness* but of *legal effectiveness* within the framework of the rule of law.

136. The task of determining these questions is inherently a matter for legislation, within the limits set by the case-law of the Court of Justice. …

137. Starting from the premiss that the operators have collected the data in a manner that complies with the provisions of Directive 2002/58 and that it has been retained in accordance with Article 15(1) of the directive, … access to that information by the competent authorities must take place in accordance with the requirements that have been laid down by the Court of Justice, which I examine in the Opinion in Case C-520/18, to which I refer.

138. Therefore, in this situation too, the national legislation must establish the substantive and procedural requirements governing access by the competent authorities to the retained data. … In the context of these references for a preliminary ruling, those requirements would allow access to the data of persons suspected of planning, of being about to commit, of having committed, or of being involved in, an act of terrorism. …

139. In any event, the fundamental point is that, other than in duly substantiated cases of urgency, access to the data in question must be subject to prior review by a court or an independent administrative authority whose decision should be made in response to a reasoned request by the competent authorities. … In this way, where a question cannot be judged in abstract by the law, there is a guarantee that it will be judged on its specific terms by that independent authority, which is committed both to safeguarding national security and to defending citizens' fundamental rights.'

B. The second question referred

40. In the event that the answer to the first question is 'yes', the referring court asks a second question. In these circumstances, it would like to know what 'other requirements in addition to those imposed by the ECHR' or arising from the *Tele2 Sverige and Watson* judgment should be imposed.

41. In that regard, it asserts that the imposition of the requirements in the *Tele2 Sverige and Watson* judgment 'would frustrate the measures taken to safeguard national security by the SIAs'.

42. As I suggest that the answer to the first question is 'no', there is no need to address the second question. As noted by the referring court, this latter question is conditional upon a finding that the 'bulk acquisition and automated processing techniques' applied to the personal data of all users in the United Kingdom, which the operators of electronic communications services would be required to transmit to the SIAs, is compatible with EU law.

43. If the Court of Justice were to consider it necessary to reply to the second question, I believe that the Court should endorse the conditions in the *Tele2 Sverige and Watson* judgment referred to above as regards:

he prohibition on general access to the data;

he need for access to the data to be subject to prior authorisation by a court or independent authority;

he requirement to inform affected parties, unless this would compromise the effectiveness of the measure;

he retention of the data within the European Union.

44. I reiterate that it would suffice to confirm these mandatory requirements, for the reasons I have set out in the Opinions in Joined Cases C-511/18 and C-512/18 and Case C-520/18, and that there is no need to establish 'any other' additional requirements as alluded to by the referring court.

V. Conclusion

45. In the light of the above, I recommend that the Court of Justice should reply to the Investigatory Powers Tribunal (United Kingdom) in the following terms:

Article 4 TEU and Article 1(3) 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) should be interpreted as precluding national legislation which imposes an obligation on providers of electronic communications networks to provide the security and intelligence agencies of a Member State with 'bulk communications data' which entails the prior general and indiscriminate collection of that data.

As a subsidiary issue:

Access on the part of the security and intelligence agencies of a Member State to data transmitted by the providers of electronic communications networks must comply with the conditions established in the judgment of 21 December 2016, *Tele2 Sverige and Watson* (C-203/15 and C-698/15, EU:C:2016:970).

Original language: Spanish.

---

2 Cases C-293/12 and C-594/12, 'the *Digital Rights* judgment', EU:C:2014:238.

---

3 Directive of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

---

4 Cases C-203/15 and C-698/15, 'the *Tele2 Sverige and Watson* judgment', EU:C:2016:970.

---

5 Directive 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 2002 L 201, p. 37).

---

6 Case C-207/16,'the *Ministerio Fiscal* judgment', EU:C:2018:788.

---

7 In addition to this one, the cases in question are C-511/18 and C-512/18, *La Quadrature du Net and Others*, and C-520/18, *Ordre des barreaux francophones et germanophone and Others*.

---

8 *Privacy International*, C-623/17.

---

9 *Ordre des barreaux francophones et germanophone and Others*, C-520/18.

---

10 *La Quadrature du Net and Others*, C-511/18 and C-512/18.

---

11 'The 1984 Act'.

---

12 'DRIPA'.

---

13 The Secretary of State for Foreign and Commonwealth Affairs, the Secretary of State for the Home Department and the three United Kingdom SIAs, namely Government Communications Headquarters (GCHQ), the Security Service (MI5) and the Secret Intelligence Service (MI6).

---

14 That is, the case-law established in the *Tele2 Sverige and Watson* judgment.

15 Opinion in Joined Cases C-511/18 and C-512/18, point 42.

16 Cases C-317/04 and C-318/04, EU:C:2006:346.

17 Opinion in Joined Cases C-511/18 and C-512/18, points 44 to 76.

18 *Ibidem*, points 77 to 90.

19 Under Article 2 of Directive 2002/58, for the purposes of that directive, the definitions in 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 personal data and on the free movement of such data (OJ 1995 L 281, p. 31) apply. Under Article 2(b) of the latter, 'processing of personal data' means 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, *disclosure by transmission*, dissemination or otherwise *making available*, alignment or combination, blocking, erasure or destruction' (italics added).