Observations of Portugal

Case C-623/17 *

Document lodged by:

Portuguese Republic

Usual name of the case:

PRIVACY INTERNATIONAL

Date lodged:

9 February 2018

[…]

OBSERVATIONS OF THE PORTUGUESE REPUBLIC

In the request for a preliminary ruling submitted by the Investigatory Powers Tribunal, London (United Kingdom), concerning the interpretation 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 ('the Directive on privacy and electronic communications' or 'the directive'), as regards the scope of the directive and the obligation of operators to provide bulk communications data to the Security and Intelligence Agencies of a Member State.

[…]

I. Facts and procedure

1 It is apparent from the information transmitted in the present case that the question referred to the Court of Justice for a preliminary ruling from the referring court essentially concerns the interpretation and application of the Directive on privacy and electronic communications in relation to the national security activities of the intelligence and security services of a Member State and, to that extent, to the applicability of the case-law of the Court of Justice resulting from the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15 EU:C:2016:970), with regard to the retention of bulk communications data and subsequent access by those services.

* Language of the case: English.

2 The findings of fact indicate that a non-governmental organisation working in the field of human rights ('the applicant') brought an action before the referring court against the United Kingdom authorities responsible for security and intelligence services, alleging that the acquisition and use by those services of bulk communications data ('BCD') infringes the right to privacy enshrined in Article 8 of the European Convention on Human Rights ('the ECHR').

3 The BCD includes traffic data and location data and information concerning 'who, where, how and with whom' the telephone or internet is used, including the location of mobile or fixed telephone from where calls are made or received, as well as the location of the computers used to access the internet. To that extent, the BCD provides information concerning, inter alia, social, commercial and financial activities, communications and travel, etc., but not concerning the content of the communications, which can only be obtained by means of a specific court order.

4 In accordance with the applicable law of the United Kingdom at issue in the main proceedings, that is, section 94 of the Telecommunications Act 1984, a member of the Government may give the operators of public electronic communications networks ('operators') such general or specific directions as appear necessary in the interests of national security.

5 In carrying out instructions of that nature, the intelligence and security services carry out searches in the BCD obtained from the operators. In contrast to their use for the purposes of criminal investigation, in which the suspect has already been identified and, therefore, the data concerned is more restricted, those searches are not directed at specific, known targets, which, in the opinion of the referring court, justifies that this data should be as comprehensive as possible in order to be useful.

6 On the basis of the evidence adduced, the referring court concluded that the BCD is essential to the work of the security and intelligence services in combating serious threats to public security, in particular in the areas of counter-terrorism, counter-intelligence and nuclear proliferation, and that the powers of those services with regard to BCD, including the power to obtain and process BCD, are indispensable for the protection of the national security of the United Kingdom.

7 The referring court further concluded that, in the light of the safeguards applicable to the acquisition and use of BCD by those services, that measure would be less intrusive than other means of obtaining information. In particular, unlike the regime considered in the *Watson* judgment, it should be pointed out that the law applicable in the present case provides that telecommunications data is to be delivered by the operator to the security and intelligences services and kept in their custody.

8 In that context, the referring court also relies on the provisions of Article 4 TEU and Article 1(3) of the Directive on privacy and electronic communications.

In summary, the case in the main proceedings essentially concerns the interpretation of that directive as regards its scope and the obligation for operators to provide BCD to the security and intelligence services of a Member State.

II. Questions raised by the referring court

9 In order to decide on the case before it, the referring court considers it appropriate to refer the following questions to Court of Justice of the European Union for a preliminary ruling:

1. Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the Directive 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 ('SIAs') of a Member State fall within the scope of EU law and of the Directive on privacy and electronic communications?

2. If the answer to the first question is answered in the affirmative, do any of the Watson requirements, or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? 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?

III Legal framework

EU Law

10 Article 4(2) of the TEU states 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.

11 Article 15(1) of the directive, entitled 'Application of certain provisions of Directive 95/46/EC', provides as follows:

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/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

IV Legal assessment

12 The directive concerns the processing of personal data and the protection of privacy in the electronic communications sector. It should be noted that the data concerned, namely the BCD, are generated in the context of the exchange of *electronic communications*.

13 In the terms employed by the referring court, the BCD may include information on the *'who, where, when and how'* of telephone and internet use, including the location of the mobile or fixed telephones from which calls are made or received, as well as the location of the computers used to access the internet.

14 Consequently, this concerns 'metadata', that is, data relating to the circumstances of the communication and not to the content itself, also defined as 'data about data'. In essence, this relates to traffic data and location data.

15 According to the settled case-law of the Court, although they do not reveal the content of the communications, that data *'allows for very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained* (...)', from which it follows that they must also enjoy adequate protection (judgment of 8 April 2014, *Digital Rights Ireland Ltd* and Others, C-293/12 and C-594/12 EU:C:2014:238, paragraph 27).

16 In accordance with Article 1(1) of the Directive on privacy and electronic communications, the purpose of the directive is to harmonise the provisions of the Member States referring to the *'processing of personal data in the electronic communications'* and, to that extent, in accordance with Article 1(2) thereof, it clarifies and complements 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.

17 To this end, in accordance with Article 3(1), the directive '*shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community*' including traffic data and location data, defined in accordance with Article 2(b) and (c), respectively.

18 Article 1(3) of the Directive on privacy and electronic communications delimits its scope of application negatively, expressly excluding, inter alia, activities related to the defence and security of the state. National security remains a 'last stronghold' of the sovereignty of the Member States in the context of the Union, which is the sole responsibility of the Member States, as set out in the last sentence of Article 4(2) TEU.

19 By its first question, the referring court therefore asks whether the inclusion of the obligation, imposed by a direction of a member of the Government to an operator, to provide bulk communications data to the security and intelligence services of a Member State falls within the scope of EU law and the Directive on privacy and electronic communications, in the light of the said general exclusion of national security activities from the scope of EU law.

20 In that regard, it should be borne in mind that the provision of BCD by operators entails the prior processing of personal data, in the context of the supply of publicly available electronic communications services. That data processing means that it must be included within the scope of the Directive on privacy and electronic communications, and there appears to be no doubt that it comes within the material scope of the directive.

21 The acquisition or use of data for the purpose of defence and national security only arises at a second stage, naturally presupposing some form of prior processing, namely collection, recording or storage, in order to be subsequently *supplied* to security or intelligence services or *acquired* by them.

22 Thus, according to the information provided in the order for reference, it appears that this first stage of data processing and storage should not be classified as an activity related to the defence or security of the State, so that it would not fall within the scope of the exclusion of Article 1(3) of the directive.

23 However, the acquisition and use of BCD by the security and intelligence services, on the basis of a direction given by a member of the Government, in accordance with the abovementioned national law, for the purposes of the defence of national security, is included in the exceptions to the rules set out in Article 15 (1) of the directive. In particular, it is possible for Member States to derogate from Article 6 of the directive, as regards data retention, where that is a necessary, appropriate and proportionate measure in a democratic society, in particular to safeguard national security.

24 In other words, the conclusion that the processing of personal data in the context of the provision of publicly available electronic communications services falls within the scope of EU law and the Directive on privacy and electronic communications does not preclude a second conclusion, that imposing the acquisition and use of these data, addressed to the security and intelligence services, constitutes one of the exceptions that makes it possible to derogate from the general rules.

25 Notwithstanding that coincidence between activities which are, ab initio, excluded from the scope of the directive and activities which, because of the purposes pursued, may give rise to derogations from the general rules, the foregoing conclusion should not be confused with the conclusion, already discarded, of exclusion from the scope of the directive, as the Court held in paragraphs 72 to 75 of the judgment in *Watson*.

26 As mentioned, that ground for derogation reflects the general approach enshrined in the EU Treaty that national security activities continue to be recognised as within the competence of the Member States.

27 Accordingly, by way of derogation from the general rules, EU law does not provide a specific system for the purpose of safeguarding national security, in the same way as it provided for the prevention, investigation and prosecution of criminal offences under Directive 2006/24/EC 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 281, p.31) ('Directive 2006/24'). That ground for derogation is also provided for in Article 15(1) of the Directive on privacy and electronic communications.

28 The Court's analysis in the *Watson* judgment concerns the requirements which the national legislation implementing Directive 2006/24 must observe in the light of Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union ('the Charter').

29 Accordingly, since that case-law of the Court of Justice has a specific objective in view, the Court's view having been adopted on that basis, in reply to the second question, it does not seem possible to extrapolate from that case-law a general interpretation for all the systems that apply the exceptions provided for in Article 15 of the Directive on privacy and electronic communications, failing which the specificities of the objectives in question will not be taken into account.

30 Moreover, that case-law of the Court of Justice is based on earlier case-law concerning precisely the legality, in the light of EU law, of the system laid down for the application of Article 15 for the purposes of criminal prosecution, which falls within the remit of the Union, unlike that at issue in the main proceedings, which goes beyond the limits of that remit.

31 Finally, it should be pointed out that recital 11 of the Directive on privacy and electronic communications refers only to the need to ensure that the restrictive measures adopted for national security purposes comply with the ECHR.

V Conclusion

32 It follows from the foregoing and from the grounds set out above that the Portuguese Government proposes that the Court should answer the questions referred for a preliminary ruling as follows:

1. 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), in particular Article 1(3), must be interpreted as meaning that the processing and retention of traffic and location data from public electronic communications networks by operators, in the circumstances of the case in the main proceedings, fall within the scope of that directive, without prejudice to a direction given by a member of the government of a Member State, such as that at issue in the main proceedings, to require the operator of an electronic communications network to provide mobile communications data to the security and intelligence services for the purposes of national security, fall within the exceptions to the general rules provided for in Article 15(1) of the abovementioned directive.

2. The judgment of 21 December 2016, Tele2 Sverige and Watson and Others *(C-203/15 and C-698/15, EU:C:2016:970), examines the application of the requirements contained in Article 15(1) of the directive in the context of crime prevention and prosecution for the purposes of the implementation of Directive 2006/24/EC. It falls to the national court to assess whether legislation, on which a member of the government of a Member State bases a direction given for the purposes of safeguarding national security, as in the main proceedings, complies with the criteria set out in Article 15(1) of the directive, which seeks to provide the necessary, appropriate and proportionate restrictive measures within a democratic society to safeguard national security and the security of the State.*

The Agents of the Portuguese Republic

Luís Inez Fernandes Miguel Figueiredo Filipa Aragão Homem