Observations of the Netherlands

Case C-623/17 *

Document lodged by:

Kingdom of the Netherlands

Usual name of the case:

PRIVACY INTERNATIONAL

Date lodged:

15 February 2018

* Language of the case: English.

Ministry of Foreign Affairs
Legal Affairs Department
European Law Division
P O Box 20061
2500 EB The Hague
Netherlands

Reference MinBuZa-2018.314515

To:
the Court of Justice of the European Union in Luxembourg

WRITTEN OBSERVATIONS

of the Netherlands Government,
submitted pursuant to the second paragraph of Article 23(2) of the Protocol on the Statute of the Court of Justice of the European Union,

in Case C-623/17, *Privacy International*

In the abovementioned case the Netherlands Government, represented by Mielle Bulterman and Charlotte Schillemans, respectively head and official of the European Law Section of the Legal Affairs Directorate of the Ministry of Foreign Affairs in The Hague, has the honour of bringing the following observations to the attention of the Court.

I. Introduction

1 By order for reference of 18 October 2017, the United Kingdom Investigatory Powers Tribunal ('the referring court') referred questions for a preliminary ruling to the Court of Justice under Article 267 TFEU on Article 4(2) TEU and Directive 2002/58/EC of the European Parliament and 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; 'Directive 2002/58').

2 The questions have arisen in the context of proceedings between Privacy International, a non-governmental organisation working in the field of the protection of human rights, and the United Kingdom Government, including the security and intelligence agencies GCHQ, MI5 and MI6. At the heart of the dispute, as far as the referring court is concerned, is the lawfulness of a national measure on the basis of which an electronic communications network provider is

required to provide bulk communications data to the security and intelligence agencies.

3 That bulk communications data includes traffic and location data which provides information on social, commercial and financial activities and travel. The bulk communications data to be supplied under the measure does not include the content of such communications. The bulk communications data, once acquired, is stored securely and used by the security and intelligence agencies.

4 Privacy International has claimed that the acquisition and use of the bulk communications data by the national security and intelligence agencies is contrary to EU law, as interpreted in the judgment of the Court of 21 December 2016, *Tele2Sverige and Watson*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970 ('the *Tele2 and Watson* judgment').

5 In that context, the referring court poses the question to the Court of Justice whether EU law, and in particular Directive 2002/58, is applicable to a national measure such as the one at issue here. If EU law and the directive are applicable, the Court is requested to clarify whether the conditions laid down in the *Tele2 and Watson* judgment apply also to such a measure, which enables the acquisition and use of bulk communications data by the national security and intelligence agencies.

6 For a more detailed exposition of the facts and legal framework, the Netherlands Government refers to the order for reference.

II. Position of the Netherlands Government

7 The Netherlands Government will now explain that a national measure which is used for the acquisition of data by the national security and intelligence agencies does not, in its opinion, fall under EU law. The second question would then not need to be answered. Only in the alternative will the Netherlands Government argue, with regard to the second question, that the situation in the *Tele2 and Watson* case was fundamentally different from that in the present case. Therefore, the conditions formulated by the Court in that case cannot, by definition, be applied.

First question referred

8 As already stated, by its first question the referring court wishes to ascertain whether, having regard to Article 4(2) TEU and Article 1(3) of Directive 2002/58, 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 falls within the scope of EU law and of that directive.

9 According to the Netherlands Government, it appears from Article 4(2) TEU and Article 1(3) of Directive 2002/58 that a national measure such as the one at issue here does not fall under EU law (and therefore not under the directive, either). This will be explained below. First, Article 4(2) TEU will be examined, followed by Directive 2002/58, and it will last be concluded that the Charter is not applicable in a case such as the present, either.

(a) Article 4(2) TEU: national security the sole responsibility of the Member States

10 Article 4(2) TEU provides that the European Union is to respect essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. It is explicitly stated, in particular, that national security *remains the sole responsibility of each Member State.*

11 That article constitutes a guarantee against action by the European Union and must be regarded, in the context of the principle of conferral, as one of the fundamental principles of EU law (Article 5(1) TEU). Under that principle, the Union is to act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States (Article 5(2) and Article 4(1) TEU).

12 Under the TEU and TFEU, the Union does not have the competence to regulate the activities of the national security and intelligence agencies. According to the Netherlands Government, it is also clear from the designation of national security as the sole responsibility of each Member State that the competences relating to national security and, specifically, the regulation of the activities of the national security and intelligence agencies, have not been transferred to the Union. This is also explained by the fact that the responsibility of a Member State for the protection of its national security relates to the essence of the sovereignty of a State, the essential elements of which the Member States have not transferred to the Union.

13 According to the Netherlands Government, a measure for acquiring bulk communications data — data which, as the referring court explains, is essential for carrying out the activities of the national security and intelligence agencies — must regarded as the core of the sole responsibility of each Member State for its national security, in which the Union may not intervene.

14 It already follows from the foregoing that, having regard to Article 4(2) TEU, the competences relating to national security and, specifically, the activities of the national security and intelligence agencies, such as those for the acquisition of bulk communications data, do not fall under EU law. Since a directive cannot detract from a provision of the TEU, it is essentially unnecessary to discuss Directive 2002/58. Nevertheless, the Netherlands Government notes the following in that regard.

(b) Directive 2002/58 not applicable

15 Directive 2002/58 is aimed at the protection of personal data in the electronic communications sector. It applies to the processing of personal data in connection with the provision of publicly available electronic communications services (Article 3(1) of the directive).

16 Article 1(3) of Directive 2002/58 — just like Article 4(2) TEU — makes it clear that the directive does not apply to activities which fall outside the scope of EU law, such as those of the national security and intelligence agencies in the context of State security:

'*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.*'

17 Recital 11 of the directive explicitly states the following in that regard:

'*Like Directive 95/46/EC, this directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. ... Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. ...*'

18 Recital 11 includes reference to Directive 95/46.[1] That directive adopts a comparable approach whereby the provision of data to the national security and intelligence agencies and the processing of that data by them does not fall within the scope of EU law. Directive 95/46 is concerned with the processing of data as such (regardless of whether it is carried out by the national security and intelligence agencies). Article 3(2), first indent, of that directive provides that '*processing operations concerning public security, ..., State security*' are not covered by that directive.

19 That delimitation of the scope of Directive 2002/58 (and Directive 95/46) is in accordance with the provisions of the TEU on national security as the sole responsibility of the Member State. The directive must therefore also be

[1] 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).

interpreted in that context. After all, a provision in a directive cannot detract from a provision of the TEU.

20 With regard to Article 15 of Directive 2002/58, on which the Court of Justice ruled in the *Tele2 and Watson* judgment, the Netherlands Government notes the following.

21 The Netherlands Government submits that the present case differs emphatically from that of *Tele2 and Watson.* The judgment in that case concerned a measure whereby an electronic communications network provider was directed to retain traffic and location data, with a view to giving access to that data to the national authorities charged with combating crime and detecting and prosecuting serious criminal offences.

22 In that case, the Court did not rule on a measure for the provision of bulk communications data to the national security and intelligence agencies with a view to the protection of national security. Unlike the combating of crime and the detection of criminal offences, national security is explicitly mentioned in Article 4(2) TEU as the being the sole responsibility of each Member State. The Netherlands Government submits that that guarantee in respect of national security in Article 4(2) TEU means that, where measures in the area of national security are concerned, such as those in the present case, no significance can attach to Article 15 of Directive 2002/58.

23 On the basis of the foregoing, the Netherlands Government concludes that a measure such as that at issue in the main proceedings, which involves the exercise of the competences and activities of the national security and intelligence agencies, does not fall within the scope of Directive 2002/58.

(c) Charter not applicable

24 For the sake of completeness, the Netherlands Government notes that it follows from the foregoing that the Charter of Fundamental Rights of the European Union ('the Charter') is not applicable to a national measure such as that at issue here, either. After all, the provisions of the Charter are addressed to the Member States only in those situations in which they are implementing EU law (Article 51 of the Charter).

Conclusion with regard to the first question referred

25 With regard to the first question referred for a preliminary ruling, the Netherlands Government concludes on the basis of the foregoing that, having regard to Article 4(2) TEU, a national measure aimed at the acquisition of data by the national security and intelligence agencies does not fall under EU law, and in particular, under Directive 2002/58.

Second question referred

26 By its second question, should the answer to the first question be in the affirmative, the referring court wishes to ascertain whether, in addition to the requirements imposed by the ECHR, those formulated in the *Tele2 and Watson* judgment or any other requirements apply to a national measure such as the one at issue in the case at hand. If that question is answered in the affirmative, the referring court wishes to ascertain how and to what extent those requirements apply, taking into account the essential necessity of the security and intelligence agencies 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.

27 Given its answer to the first question referred, the Netherlands Government is of the view that the second question does not require an answer. Only to the extent that the Court of Justice might conclude that EU law and Directive 2002/58 are applicable to a measure on the basis of which an electronic communications network provider is directed to provide bulk communications data to the security and intelligence agencies, the Netherlands Government notes the following.

28 The Netherlands Government takes the position that the conditions formulated by the Court of Justice in the context of Article 15(1) of Directive 2002/58 in the *Tele2 and Watson* judgment cannot be applied to a measure for the acquisition of bulk communications data for the purposes of protecting national security. Namely, those purposes must be treated differently from the purposes relating to the combating of crime and the detection and prosecution of serious criminal offences which were at issue in the *Tele2 and Watson* judgment. The essential differences between, on the one hand, activities in the interests of national security and, on the other hand, the detection of criminal offences, will be set out in paragraphs 29 to 33 below. The Netherlands Government will then explain that the *Tele2 and Watson* judgment leaves room for a different approach to national security other than one based on detection, room which must be utilised (paragraphs 34-39 below). The Netherlands Government concludes with the remark that, for measures for the acquisition of bulk communications data by the national security and intelligence agencies, no conditions other than those arising from the ECHR should apply, including those under Article 15 of Directive 2002/58 in conjunction with Article 7 of the Charter (paragraphs 40 to 43 below).

(a) National security versus detection of criminal offences

29 As already stated, there are essential differences between the activities of the State to protect its national security and the activities of national authorities to combat crime and detect and prosecute criminal offences. The latter activities are concrete, in the sense that there is a concrete reason for the action taken: the planning or commission of a criminal offence. What is to be deemed criminal is determined in advance and by law. The criminal offence is followed by detection and prosecution of one or more suspects. The activities in the area of detection

and prosecution of criminal offences are therefore a targeted and delineated process.

30 The activities of the State in the context of national security are different in nature and have a different purpose. Taking care of national security involves, inter alia, investigating organisations and persons who, by the aims they pursue or by their activities may constitute a danger to the survival of the democratic legal order or to security or to other important interests of the State (also, for example, to interests relating to defence). In that regard, it is irrelevant whether criminal offences are planned or committed; in the Netherlands, for example, the security and intelligence agencies thus do not have detection competences as defined under criminal law.

31 As also recognised by the ECtHR, threats to national security can vary in character and are by their nature difficult to identify in advance (case of *Kennedy* v *The United Kingdom*, 26839/05 [2010]). As an example of a diffuse threat, the Netherlands Government refers to cyber threats, by which attempts are made to influence democratic processes, including, for example, the influencing of elections by hacks.

32 In order to be effective, the investigation carried out by the security and intelligence agencies is, in principle, secret in nature. If the subjects of the investigation by the security and intelligence agencies knew they were being investigated, they could adapt their behaviour accordingly and thus remain under the radar of the security and intelligence agencies. In addition, the investigations by the security and intelligence agencies are often necessarily long. They in fact involve continuous search for, monitoring of and bringing under control of activities which may pose a danger to national security.

33 It is essential in that regard that the security and intelligence agencies can have the information necessary for that purpose. To that end, they need to have — as is at issue in the present case — far-reaching competences for the acquisition and further processing of data, which must be provided by law. It may involve the processing of information which relates very specifically to a particular subject under investigation. However, the possibility of acquiring and processing large data files (such as bulk communications data) is also necessary for the proper performance of duties. The analysis of such files, whether or not in combination with each other, makes it possible to compile threat profiles and to search for patterns. In addition, on the basis of historical traffic and location data, it is possible to make a reconstruction of activities which (may) constitute or may have constituted a threat. In that manner, it may be possible to gain an insight into, for example, the (terrorist) network behind an attack or cyber threat. Furthermore, it may be possible on that basis to develop a timely awareness of (previously-unknown) present threats, so that effective action may be taken to protect national security.

(b) *Tele2 and Watson* judgment not for national security

34 The Netherlands Government submits that, in the light of the foregoing, the conditions formulated in the *Tele2 and Watson* judgment pursuant to Article 15(1) of Directive 2002/58 for a measure relating to detection cannot be applied to a measure such as that at issue in the present case, which is taken in the context of actions for the purpose of protecting national security. If those conditions were fully applied, Member States — which bear the sole responsibility for national security — would be severely hindered in carrying out that responsibility.

35 In that regard, the Netherlands wishes to point out that the *Tele2 and Watson* judgment also leaves room for a different approach in the interests of national security and to promote the effectiveness of measures. For example, the Court of Justice considered in paragraph 119 of the judgment:

'*However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, 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.*'

36 It follows from paragraph 121 of that judgment that the effectiveness of the measures is a relevant factor:

'*Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities.*'

37 The impracticality of the conditions, as inferred from paragraphs 119 to 125 of the *Tele2 and Watson* judgment, for any investigation by the national security and intelligence agencies, is apparent, in particular, in the condition limiting non-targeted access to bulk communications data (paragraph 119 of the *Tele2 and Watson* judgment). It is in fact essential that the security and intelligence agencies should be able to scrutinise such data (certain defined sets of traffic and location data) in order to safeguard national security. As threat is diffuse and difficult to identify in advance, it is important to be able to search broadly and to look back in time. Based on historical traffic and location data, connections can be established in (terrorist) networks, thus making it possible to identify (in a timely manner) threats to national security (cf. also paragraph 31 above and paragraphs 3 and 4 of the order for reference).

38 Furthermore, an obligation to give prior notification to the relevant subjects of an investigation (paragraph 121 of the *Tele2 and Watson* judgment) could do great harm to an investigation by the security and intelligence agencies. As already stated, such an investigation is, in principle, secret in nature and must indeed be so in order to be effective (see paragraph 32 above; also recognised in the judgment of the ECtHR in the case *Klass and others* v *Germany*, 5029/71 [1978]).

39 The Netherlands Government submits that, in the light of the foregoing, to the extent that a measure relating to national security falls under Article 15 of Directive 2002/58, conditions other than those formulated in the *Tele2 and Watson* judgment must be laid down. As will be explained below, the determining factor in that regard is the level of protection that stems from the ECHR.

(c) Measures for national security purposes and the level of protection under the ECHR

40 As the referring court recognises in the second question referred, a measure for national security purposes such as that at issue in the present case must also satisfy the conditions that follow from the ECHR (as interpreted in the case-law of the ECtHR). The relevant provision in that regard is Article 8 ECHR, which — within the framework of EU law — corresponds to Article 7 of the Charter.

41 In the context of activities which limit the right to respect for private and family life as laid down in Article 8 ECHR, the following requirements should be satisfied: the measures of the Member States for the purpose of protecting national security must have their basis in law, they must be necessary in a democratic society in the interests of national security, they must satisfy the requirements of accessibility and foreseeability and they must offer adequate safeguards against the abuse of power (see, for example, the ECtHR case *Kennedy* v *United Kingdom*, previously cited, paragraphs 151 to 153).

42 Where the measure concerned satisfies those requirements, there is — as the ECtHR held — a suitable balance between the right to respect for private and family life and the possibility for the State to take the measures necessary for the protection of (inter alia) national security. It is clear from recital 11 of Directive 2002/58 that that balance cannot under any circumstances be altered by the directive.

43 The Netherlands Government therefore submits that, also in the context of Article 15 of Directive 2002/58 in conjunction with Article 7 of the Charter, no conditions may be imposed on a measure such as that at issue in the present case other than those arising from the ECHR.

In the alternative: Conclusion with regard to the second question referred

44 In so far as the Court feels obliged to answer the second question referred, the Netherlands Government concludes in its answer thereto that the conditions which the Court formulated in the *Tele2 and Watson* judgment cannot be applied to the acquisition of communication data for the purpose of protecting national security. A national measure such as that at issue in the main proceedings must, in the context of Article 15 of Directive 2002/58 in conjunction with Article 7 of the Charter, satisfy the level of protection arising from the ECHR.

III. Conclusion

45 In the light of the foregoing, the Netherlands Government proposes that the Court of Justice answer the first question as follows:

'*1. In the light of Article 4(2) TEU, a national measure which is used for the acquisition of data by the national security and intelligence agencies does not fall under EU law, in particular, Directive 2002/58.*'

46 In so far as the Court feels obliged to answer the second question, the Netherlands Government proposes suggests that the Court answer that question as follows:

'*2. The conditions formulated by the Court of Justice pursuant to Article 15(1) of Directive 2002/58 in the* Tele2 and Watson *judgment cannot be applied to the acquisition of communications data for the purposes of protecting national security. A national measure such as that at issue in the main proceedings must, in the context of Article 15 of Directive 2002/58 in conjunction with Article 7 of the Charter, satisfy the conditions arising from the ECHR. The measures of the Member States relating to the protection of national security must therefore have their basis in law, they must be necessary in a democratic society in the interests of national security, they must satisfy the requirements of accessibility and foreseeability and they must offer adequate safeguards against the abuse of power.*'

Mielle Bulterman Charlotte Schillemans

Agents

The Hague, 15 February 2018