Written observations of Germany

Case C-623/17 *

Document lodged by:

Federal Republic of Germany

Usual name of the case:

PRIVACY INTERNATIONAL

Date lodged:

13 February 2018

* Language of the case: English.

Federal Republic of Germany

Berlin, 13 February 2018

Thomas Henze
David Klebs
Agents of the Government
of the Federal Republic of Germany

ADDRESS FOR SERVICE
Preferably via e-Curia, or to:
Federal Ministry of
Economic Affairs and Energy
Department EA5
Scharnhorststr. 34 - 37
10115 Berlin
Germany
Fax: +49 30 18615 - 5334

EA5 – 81202/001#564

Court of Justice of the European Union
– Registry –
2925 Luxembourg

Via e-Curia

Written observations

In Case C-623/17

concerning the reference to the Court of Justice of the European Union by the Investigatory Powers Tribunal (United Kingdom) for a preliminary ruling made by order of 18 October 2017 in the proceedings pending before that court between

Privacy International

and

Secretary of State for Foreign and Commonwealth Affairs and Others,

we submit the following observations on behalf of and with the authorisation of the Government of the Federal Republic of Germany:

Table of contents

A. INTRODUCTION 4
B. LEGAL CONTEXT 5
I. Treaty on European Union 5
II. Directive 2002/58 5
C THE FACTS AND QUESTIONS REFERRED FOR A PRELIMINARY RULING 6
D. LEGAL ASSESSMENT 8
I. First question referred 8
1. Interpretation of the relevant provisions regarding the scope of EU law. 8
(a) Directive 2002/58 and Directive 95/46 8
2. Conferral under primary law and limits in respect of action of the European Union, in particular in Article 4(2) TEU 11
(a) No legal basis for conferring power on the European Union to regulate the activities of security and intelligence agencies 12
(b) Reservation of national security to the Member States (Article 4(2) TEU) 13
(c) The term 'national security' in the case-law of the ECtHR 14
(d) Interpretation of EU law by the Bundesverfassungsgericht (Federal Constitutional Court) 15
3. Conclusions for the present case 16
II. No answer to the second question referred – in the alternative: consequences of transferring the *Tele2* case-law to the activity of intelligence agencies 17
1. Activity of the intelligence agencies in Germany 17
2. Consequences of transferring the requirements of the *Tele2 Sverige and Watson* judgment to the activity of the intelligence services 20
3. No reduction in the level of protection of fundamental rights if Directive 2002/58 and the Charter of Fundamental Rights of the EU were not applied 21
E. CONCLUSION 21

1

A. INTRODUCTION

1 The main proceedings concern rules regarding the collection and analysis of bulk communications data by the security and intelligence agencies of the United Kingdom. This is data that provides information about the 'who, when, where, how and with whom' of telephone and internet use, including the location of the communication devices. It does not cover the content of communications.

2 By the first question referred, the Investigatory Powers Tribunal seeks clarification as to whether the national measure in dispute comes within the scope of EU law, such that, in particular, the requirements of Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [1] (hereinafter Directive 2002/58) and Articles 7 and 8 of the Charter of Fundamental Rights of the EU must be complied with.

3 The Federal Government takes the view that it follows from Article 4(2) TEU that the activities of the security and intelligence agencies of the Member States in relation to national defence and national security come within the sole responsibility and therefore rules of the Member States. The Member States and their security and intelligence agencies, however, remain subject to the provisions of the ECHR and of national constitutional law.

4 The Federal Government does not consider the findings of the Court in the *Tele2 and Watson* [2] judgment to be transferable to the present case, as that judgment does not relate to the activity of the national security and intelligence agencies, but rather relates to the processing of data by providers of communications services in public communications networks. Therefore, there is also no need to answer the second question referred.

5 Moreover, the Federal Government agrees with the referring tribunal's findings that applying the requirements that the Court imposed on operators of electronic communications services in the *Tele2 and Watson* judgment would make it very difficult for national security and intelligence agencies to safeguard national security. This would have significant repercussions, particularly for the combating of terrorist threats, espionage and comparable threats, as will be explained by the Federal Government below in the example of the possible effects on the activity of the security and intelligence agencies in Germany.

1 OJ 2002 L 201, p. 37.

2 Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970.

B. LEGAL CONTEXT

I. Treaty on European Union

6 Article 4(2) TEU provides:

> '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.'

II. Directive 2002/58

7 Article 1 [Scope and aim] (1) and (3) reads:

> '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.
>
> […]
>
> 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.'

8 Article 15 [Application of certain provisions of Directive 95/46/EC] (1) of Directive 2002/58 reads:

> '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.

[…]'

9 Recital 11 of Directive 2002/58 reads as follows:

'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. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal 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. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.'

C THE FACTS AND QUESTIONS REFERRED FOR A PRELIMINARY RULING

10 The applicant is a non-governmental organisation that works to defend human rights at national and international levels. The defendants are the Secretary of State for Foreign and Commonwealth Affairs, the Secretary of State for the Home Department and the three security and intelligence agencies of the United Kingdom, namely the Government Communications Headquarters (GCHQ), the Security Service (MI5) and the Secret Intelligence Service (MI6).

11 The action before the Investigatory Powers Tribunal is directed, for no specific reason, against a provision of the Telecommunications Act 1984 (hereinafter: the 1984 Act). Pursuant to section 94 of the 1984 Act, the Secretary of State may give the 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. On the basis of such a direction, the security and intelligence agencies have

acquired bulk communications data (traffic and location data) from the network operators and protect it from unauthorised access by third parties. The data is evaluated by the agencies using special, non-targeted techniques (e.g. filters and comparisons).

12 The Investigatory Powers Tribunal has asked the Court of Justice to answer the following questions:

'In circumstances where:

a. the security and intelligence agencies' 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;

b. a fundamental feature of the security and intelligence agencies' use of the 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 bulk communications 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;

c. the provider of an electronic communications network is not thereafter required to retain the bulk communications data (beyond the period of their ordinary business requirements), which is retained by the State (the security and intelligence agencies) alone;

d. the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of bulk communications data by the security and intelligence agencies are consistent with the requirements of the ECHR; and

e. the national court has found that the imposition of the requirements specified in § § 119-125 of the judgment of the Grand Chamber in joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson and Others* […] ('the *Watson* Requirements'), if applicable, would frustrate the measures taken to safeguard national security by the security and intelligence agencies, and thereby put the national security of the United Kingdom at risk;

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 (SIAs)

of a Member State fall within the scope of Union law and of the e-Privacy Directive?

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 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?'

D. LEGAL ASSESSMENT

I. First question referred

13 By the first question referred, the Investigatory Powers Tribunal seeks clarification as to whether a direction from the public authorities to an operator of an electronic communications network to provide bulk communications data to the security and intelligence agencies under the circumstances set out in the question referred comes within the scope of EU law, in particular Directive 2002/58.

14 As can be seen from the grounds for the order for reference, this raises the question of whether the collection and described use – which the direction at issue is intended to enable - of the bulk communications data by the security and intelligence agencies for the purposes of safeguarding national security also come within the scope of EU law. The Federal Government takes the view that this is not the case, as Article 1(3) of Directive 2002/58 excludes the activities of such agencies from the scope of the directive in accordance with the provisions of Article 4(2) TEU.

1. Interpretation of the relevant provisions regarding the scope of EU law.

(a) Directive 2002/58 and Directive 95/46

15 Pursuant to Article 3 of Directive 2002/58, the Directive is to 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.

16 Pursuant to Article 1(3) of Directive 2002/58, activities which fall outside the scope of the Treaty establishing the European Community are excluded.

The Directive is not to apply in any case to activities concerning public security, defence and State security. This is also confirmed, in essence, by recital 11 of the Directive.

17 As also mentioned by the aforementioned recital, this definition of the scope of Directive 2002/58 follows on from the identical wording in the first indent 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 personal data and on the free movement of such data. [3] As Directive 2002/58 particularises and complements Directive 95/46, [4] it would seem natural that the directives correspond in terms of their material scope. The General Data Protection Regulation, [5] which will replace Directive 95/46 on 25 May 2018, also does not apply to activities that fall outside the scope of Union law, such as activities relating to national security for instance (Article 2(2)(a) in conjunction with recital 16).

18 Pursuant to Article 15(1) of Directive 2002/58, Member States may 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 […] to safeguard national security (i.e. State security), defence, public security', among other things, pursuant to Article 13(1) of Directive 95/46. The national legislative measures may in particular provide for exceptions from the obligations laid down in Articles 5, 6 and 9 of the Directive, in relation to the protection of the confidentiality of communications and resulting traffic and location data.

19 These measures must be in accordance with the general principles of [EU] law, including those 'referred to in Article 6(1) and (2) of the Treaty on European Union'. According to established case-law, this reference includes in particular the fundamental rights now guaranteed by the Charter of Fundamental Rights of the EU, with the result that Article 15(1) of Directive 2002/58 must be interpreted in the light of those fundamental rights. [6]

3 OJ 1995 L 281, p. 31, last amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 adapting to Council Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in instruments subject to the procedure referred to in Article 251 of the EC Treaty, OJ 2003 L 284, p. 1.

4 Cf. Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 82.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ 2016 L 119, p. 1).

6 Cf. *Tele2 Sverige and Watson and Others* judgment, C-203/15 and C-698/15, EU:C:2016:970, paragraph 91 with further references.

20 At first glance, Article 1(3) and Article 15(1) of Directive 2002/58 conflict with one another. Whereas Article 1(3) excludes activities that serve specific objectives from the scope of the Directive, Article 15(1) allows a restriction of the rights and obligations set out in the Directive by measures that serve the same purposes as those specified in Article 1(3). In this respect, Article 15(1) sets specific conditions for such restrictions, in particular compliance with the Charter of Fundamental Rights of the EU, yet this requires that the scope of the Directive or of EU law be widened for such measures.

21 The Court acknowledged this conflict in its *Tele2 Sverige and Watson* judgment and resolved it in respect of the national legislation at issue in those proceedings in favour of a widening of the scope of Directive 2002/58 and compliance with the requirements of Article 15(1) thereof and with the fundamental rights protected in Articles 7, 8 and 11 of the Charter of Fundamental Rights of the EU. [7]

22 However, the proceedings concerned a government authority's order that obliged operators of communications services to retain traffic and location data for law-enforcement purposes. In this connection, the Court emphasised, making reference to Article 1(3) of Directive 2002/58, that the latter excludes from its scope 'activities of the State' in specified fields. [8] In relation to Article 3 of Directive 2002/58, it states, by contrast, that the Directive governs the activities of providers of electronic communications services in publicly available communications networks. [9]

23 The Federal Government takes the view that the statements of the Court are therefore based on the distinction as to whether the data processing affected by the national measure is carried out by the national security authorities themselves in relation to the objectives specified in Article 1(3) of Directive 2002/58 or whether the State imposes on the providers of communications services the obligation to retain data to achieve the similarly worded objectives in Article 15(1) of Directive 2002/58. In the former scenario, EU law and Directive 2002/58 are not applicable, but the latter scenario falls within the scope of EU law and therefore also the directive.

24 The Court had already drawn this distinction in the *Ireland* v *Parliament and Council* judgment. [10] In this judgment, it distinguished the data retention that

[7] *Tele2 Sverige and Watson and Others* judgment, C-203/15 and C-698/15, EU:C:2016:970, paragraph 78.

[8] *Tele2 Sverige and Watson and Others* judgment, C-203/15 and C-698/15, EU:C:2016:970, paragraph 69.

[9] *Tele2 Sverige and Watson and Others* judgment, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 70 and 74.

[10] Judgment of 10 February 2009, *Ireland* v *Parliament and Council*, C-301/06, EU:C:2009:68, paragraph 91.

Directive 2006/24/EC [11] obliged providers of electronic communications services to carry out from the transfer of passenger data that takes place within a framework instituted by the public authorities in order to ensure public security. [12]

25 In the *Tele2 Sverige and Watson* judgment, the Court emphasised that the provision of Article 15(1) of Directive 2002/58 must, as an exception, be interpreted strictly, as it enables the scope of the Directive's obligation of principle to ensure the confidentiality of communications and related traffic data to be restricted. [13]

26 In the context in the present case, the question of whether an activity is governed by EU law must be objectively determined on the basis of whether the Member States have conferred on the European Union the corresponding competences in the Treaties to attain the objectives set out therein (Article 5(1) and (2) TEU).

27 The European Union does not have legislative power in respect of legislation that falls outside the scope of EU law. The scope of the clarifying addition that the Directive is not to apply 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 must also be determined on the basis of the power conferred on the European Union under primary law and its limits.

2. Conferral under primary law and limits in respect of action of the European Union, in particular in Article 4(2) TEU

28 The Federal Government takes the view that there is no legal basis for conferring on the European Union the power to regulate the activity of the security and intelligence agencies in order to safeguard national security. Article 4(2) TEU expressly leaves sole responsibility in this area to the Member States. As EU law is not being implemented, the Charter of Fundamental Rights of the EU also does not apply to such activities of the national security and intelligence agencies pursuant to the first sentence of Article 51(1) of the Charter.

[11] 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 105, p. 54), annulled by judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238.

[12] See, in this respect, judgment of 30 May 2006, *Parliament* v *Council and Commission*, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56 et seq.

[13] *Tele2 Sverige and Watson* judgment, C-203/15 and C-698/15, EU:C:2016:970, paragraph 89.

(a) No legal basis for conferring power on the European Union to regulate the activities of security and intelligence agencies

29 Directive 2002/58 was based on Article 95 EC (now Article 114 TFEU). Aside from the protection of fundamental rights, it serves to ensure the functioning of the internal market, as is clear from recital 8 thereof:

'Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.'

30 However, a connection with the internal market is ruled out if national provisions relating to the safeguarding of national security within the meaning of the third sentence of Article 4(2) TEU govern the specific activity of national security and intelligence agencies. Article 114 TFEU therefore cannot be used as a legal basis for the harmonisation of such provisions. The distinction made by the *Tele2 Sverige and Watson* judgment between requirements for activities of the State, on the one hand, and requirements for activities of the provider of electronic communications services, on the other hand, reflects the scope of the conferral of power on the European Union to lay down rules on harmonisation in the internal market.

31 Nor is there a legal basis elsewhere in the FEU Treaty for the regulation of national security within the meaning of the third sentence of Article 4(2) TEU.

32 Accordingly, Article 16(2) TFEU confers on the European Union the power to lay down rules relating to the protection of individuals with regard to the processing of personal data by Member States only when the latter are carrying out activities which come within the scope of EU law.

33 Although there is shared competence between the European Union and the Member States for rules relating to the area of freedom, security and justice pursuant to Article 4(2)(j) TFEU, the specific legal bases in Title V of Part Three of the FEU Treaty do not establish competence for the European Union to regulate the specific activity of the security and intelligence agencies of the Member States in relation to the safeguarding of national security.

34 As competences have not been conferred upon the European Union, responsibility in this area remains with the Member States (Article 4(1)

TEU). This also follows from Article 4(2) TEU and Article 73 TFEU, as will now be explained in more detail.

(b) Reservation of national security to the Member States (Article 4(2) TEU)

35 Pursuant to Article 4(2) TEU, the European Union is required to respect the 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.

36 The Court has not yet defined the term 'national security' – unlike the term 'public security', which is used in Article 36, Article 45(3), Article 52(1) and Article 65(1)(b) TFEU. [14] In particular, the *Promusicae* judgment [15] does not contain an interpretation of the term 'national security' within the meaning of Article 4(2) TEU, but instead merely repeats the definition of 'State security' in Article 15(1) of Directive 2002/58.

37 In terms of a systematic interpretation, the fact that the provision in which the term 'national security' is located is Article 4(2) TEU is indicative of a reservation of powers to the Member States. In a prominent place in Title I – Common Provisions – of the TEU, it is located in Article 4 TEU, in the provision that – together with the principles of conferral, subsidiarity and (power-limiting) proportionality laid down in Article 5(1) TEU – relates to the fundamental structure of the European federal system.

38 This interpretation is supported by Article 73 TFEU, which likewise uses the term 'national security'. According to this provision, 'it shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security'. This provision is intended to guarantee cooperation between the Member States in the area of internal security outside the EU's institutional framework. It is a primary-law reference to intergovernmental cooperation in the area of Title V of Part Three of the TFEU. In accordance with the second and third sentences of Article 4(2) TEU, therefore, an extension of the shared competence for the

[14] Cf., in this respect, judgment of 26 October 1999, *Sirdar*, C-273/97, EU:C:1999:523, paragraph 17; judgment of 11 January 2000, *Kreil*, C-285/98, EU:C:2000:2, paragraph 15; judgment of 13 July 2000, *Albore*, C-423/98, EU:C:2000:401, paragraph 18; judgment of 11 March 2003, *Dory*, C-186/01, EU:C:2003:146, paragraph 32.

[15] Judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 49.

area of freedom, security and justice to rules relating to the safeguarding of national security is implicitly ruled out.

39 Article 73 TFEU clarifies at the same time that the reservation of national security is directed in particular at the activity of the Member States' security and intelligence agencies in this area ('competent departments of their administrations responsible for safeguarding national security').

(c) The term 'national security' in the case-law of the ECtHR

40 Since, pursuant to Article 6(3) TEU, fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, are to constitute general principles of the European Union's law, the case-law of the ECtHR in relation to Article 8(2) and Article 10(2) of the ECHR can firstly be used to interpret the term 'national security'.

41 Accordingly, the ECtHR stated the following in its *Klass and Others* v *Germany* judgment: [16]

'Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.'

42 Furthermore, in its *Observer and Guardian* v *United Kingdom* judgment, [17] the ECtHR treated secret information of the British Secret Service MI5 as a matter of national security within the meaning of Article 10(2) ECHR.

[16] ECtHR, judgment of 18 November 1978 - 5029/71 - *Klass and Others v. Germany*, paragraph 48, to which the ECtHR made reference in its judgment of 5 July 2001 - 38321/97 - *Erdem v. Germany*, paragraph 64.

[17] ECtHR, judgment of 26 November 1991 - 13585/88 - *Observer and Guardian v. United Kingdom*, paragraphs 56, 69.

(d) Interpretation of EU law by the Bundesverfassungsgericht (Federal Constitutional Court)

43 Against the backdrop of the division of competence between the Member States and the European Union as described above, the German Federal Constitutional Court, for instance, also assumes that the establishment of a database for various German security agencies to combat international terrorist ('Antiterrordatei' – anti-terror database) falls solely within the competence of the Member States. In its judgment of 24 April 2013, it states the following in this regard: [18]

'The constitutional complaint does not give rise to a need for preliminary ruling proceedings before the Court of Justice of the European Union pursuant to Article 267 TFEU for the purposes of clarifying the scope of the protection of fundamental rights under EU law in relation to data exchange between various security agencies within a database, as governed by the Antiterrordateigesetz (Law on the anti-terror database). This is also the case with regard to the fundamental right to the protection of personal data pursuant to Article 8 of the Charter of Fundamental Rights of the European Union (Charter, CFR). The reason for this is that the European fundamental rights of the Charter are not applicable to the case here for decision. The contested provisions must be assessed against the fundamental rights of the Grundgesetz (Basic Law) simply because they are not determined by EU law (…). Consequently, this is also not a case involving the implementation of EU law, which is the only situation in which the Member States could be bound by the Charter (first sentence of Article 51(1) CFR).'

44 The Federal Constitutional Court also states that it was beyond doubt – and also not in need of further clarification according to the criteria of the *acte clair* case-law of the Court of Justice [19] – that cooperation between the German security agencies and intelligence agencies in the context of a database did not constitute implementation of EU law within the meaning of the first sentence of Article 51(1) of the Charter of Fundamental Rights of the EU. Regarding Directive 95/46, this was apparent from Article 3(2) alone, pursuant to which the processing of data concerning public security, State security and the activities of the State in areas of criminal law was expressly excluded from the scope of the directive.

45 The establishment and development of the anti-terror database was not determined by EU law in other respects either. A merely indirect effect on legal relationships regulated under EU law was not sufficient for an

[18] Federal Constitutional Court, judgment of 24 April 2013 - 1 BvR 1215/07 - (BVerfGE 133, 277, 313 f., paragraph 88).

[19] Judgment of 6 October 1982, *C.I.L.F.I.T*, 283/81, EU:C:1982:3351, paragraph 16 et seq.

examination in the light of EU law. [20] The applicability of the fundamental rights of the European Union was therefore excluded from the outset. It was directly apparent from both the wording of Article 51(2) of the Charter of Fundamental Rights of the European Union and Article 6(1) TEU that the Charter did not extend the field of application of EU law beyond the powers of the European Union, and it did not establish any new power or task for the European Union, or modify powers and tasks as defined in the Treaties. [21]

3. Conclusions for the present case

46 The Federal Government takes the view that the findings in the *Tele2 Sverige and Watson* judgment are not transferrable to the acquisition and evaluation of bulk communications data by the intelligence services that are the subject of the main proceedings.

47 The *Tele2 Sverige and Watson* judgment concerned the question of whether and to what extent there is an obligation for private providers of communications services to retain communications data and, on the instruction of the authorities, make it available to the State for law enforcement purposes, and thus concerned the storage and transfer of data by private providers of communications services. The situation to be considered in the present case, by contrast, relates to data collection and data processing by the intelligence agencies themselves. In particular, the Court's argument that, having regard to the general structure of Directive 2002/58, and for the sake of its practical effectiveness, it could not be assumed that the legislative measures referred to in Article 15(1) of Directive 2002/58 were excluded from the scope of that directive, as that provision necessarily presupposed that Directive 2002/58 was applicable to measures relating to the retention of data for the purpose of combating crime, is not transferable to the present case. [22] The reason for this is that Directive 2002/58 itself presupposes compliance with EU primary law, meaning that its application to matters of national security within the meaning of Article 4(2) TEU, which, moreover, are the sole responsibility of the Member States, is necessarily excluded.

[20] Here the Federal Constitutional Court refers to the judgment of 18 December 1997, *Annibaldi*, C-309/96, EU:C:1997:631, paragraph 22.

[21] Cf. Federal Constitutional Court 133, 277, 315, paragraph 90; cf. also judgment of 15 November 2011, *Dereci and Others*, C-256/11, EU:C:2011:734, paragraph 71; judgment of 8 November 2012, *Iida*, C-40/11, EU:C:2012:691, paragraph 78; judgment of 27 November 2012, *Pringle*, C-370/12, EU:C:2012:756, paragraphs 179 and 180.

[22] *Tele2 Sverige and Watson and Others* judgment, C-203/15 and C-698/15, EU:C:2016:970, paragraph 73.

48 The Federal Government takes the view that an obligation on the part of the provider of a communications service to make bulk communications data available to the security and intelligence agencies for the purposes of safeguarding national security does not come within the scope of Directive 2002/58 either if, on the basis of the direction, the provider merely provides a technical support service so that the intelligence agencies can perform their duties.

49 The provider of a communications service to which a direction can be given pursuant to section 94 of the 1984 Act is not obliged to retain data itself – unlike in the case according to the legislation at issue in the *Tele2 Sverige and Watson* cases.

50 Another difference vis-à-vis those proceedings is that the data in the present case is supposed to be provided for activities of the security and intelligence agencies in order to safeguard national security and not for the purpose of combating crime. Although Article 1(3) of Directive 2002/58 also restricts the scope of the directive in relation to the activity of the State in areas of criminal law, the special reservation of competence to the Member States in Article 4(2) TEU relates to national security. This reservation must be taken into account if a provider of a communications service is obliged to provide bulk communications data intended to enable the public authorities to identify threats to national security.

II. No answer to the second question referred – in the alternative: consequences of transferring the *Tele2* case-law to the activity of intelligence agencies

51 There is no need to answer the second question referred due to the outcome of the first question.

52 The referring tribunal has already explained the serious consequences that application of the requirements set out in the *Tele2 Sverige and Watson* judgment would have for the work of the security and intelligence agencies in the United Kingdom. The Federal Government concurs with the concerns expressed by the referring tribunal and would additionally like to demonstrate below that the intelligence services in Germany are dependent on access to bulk communications data in a comparable way. Transferring the requirements of the *Tele2 Sverige and Watson* judgment would also make their activities significantly more difficult.

1. Activity of the intelligence agencies in Germany

53 In Germany, in order to obtain intelligence from abroad that is of importance to the foreign and security policy of the Federal Republic of Germany, the Bundesnachrichtendienst (Federal Intelligence Service, BND) collects the

required information and evaluates it (Paragraph 1(2) of the Gesetz über den Bundesnachrichtendienst (Law on the Federal Intelligence Service; 'the BND Law' [23]). The task of the offices of the Federal Government and Federal States tasked with protection of the constitution is to collect and evaluate information, in particular factual and personal data, messages and documents regarding efforts directed against the free basic democratic order, existence or security of the Federal Republic or a constituent Federal *Land* (Paragraph 3(1) No 1 of the Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Law on cooperation between the Federal Government and the *Länder* in matters relating to the protection of the constitution and on the Federal Office for the Protection of the Constitution [24]).

54 The BND operates the so-called 'strategische Fernmeldeaufklärung' (strategic signals intelligence). This is governed in German law in both the Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Law on the restriction of confidentiality of correspondence, mail and telecommunications; 'the Article 10 Law') and the BND Law and refers to the collection of data from data flows (e.g. data cables). Strategic signals intelligence is thus the umbrella term for so-called 'Ausland-Ausland-Fernmeldeaufklärung' ('foreign-foreign signals intelligence') pursuant to Paragraph 6 of the BND Law, that is to say, domestically gathering intelligence on foreign persons located abroad, and for strategic restrictions within the framework of the Article 10 Law (Paragraphs 5 and 8 of the Article 10 Law), which, unlike the 'foreign-foreign signals intelligence', relate to the communication, protected by Article 10 of the Basic Law, of German nationals, including domestic legal persons or foreign nationals residing in Germany.

55 Unlike in the case of telecommunications surveillance, strategic signals intelligence does not involve the surveillance of specific participants, or their telecommunications, in respect of whom there are factual reasons to suspect that they are planning, committing or have committed certain offences. Rather, the purpose of the measures – in line with the task of the BND – is to conduct advance surveillance of specific high-risk situations and to obtain intelligence from abroad that is of importance to the foreign and security policy of the Federal Republic of Germany. Accordingly, it does not involve an individualised or situation-specific need for the intelligence services to collect data due to a particular event.

[23] Law on the Federal Intelligence Service of 20 December 1990 (BGBl. I, p. 2954, 2979), last amended by Article 4 of the Law of 30 June 2017 (BGBl. (Federal Law Gazette) I, p. 2097).

[24] Bundesverfassungsschutzgesetz (Federal Law on the protection of the constitution) of 20 December 1990 (BGBl. I, p. 2954, 2970), last amended by Article 2 of the Law of 30 June 2017 (BGBl. I, p. 2097).

56 Pursuant to both the Article 10 Law and Paragraph 6(2) of the BND Law, content data regarding specific situations is collected only on the basis of appropriate and specific search terms, thus in a targeted manner. The search terms may lead to the targeted recording of one of several communication partners if, for example, a telephone number is used as a search term. However, another communication partner is either not recorded at all or is only recorded in a non-targeted manner, i.e. 'randomly', something which is technically and practically unavoidable, but also beneficial in terms of being able to understand the context of the communication.

57 In the case of the 'foreign-foreign signals intelligence' of the BND, traffic data can also be collected without the use of search terms. Traffic data whose necessity for the performance of the BND's tasks has not yet been specifically assessed can be stored by the BND for up to six months (Paragraph 6(6) of the BND Law). In this case, the traffic data is not collected in a general and indiscriminate manner within the meaning of the judgment of the Court of Justice in the *Tele2 Sverige and Watson* cases, but merely collected on routes that contain data of relevance to the BND's tasks.

58 In principle, data is collected by the BND itself. In individual cases, providers of telecommunications services may be obliged to extract data. In this case, however, the service provider's obligation to cooperate is limited to enabling surveillance of the data concerned by the BND. Under no circumstances are providers of telecommunications services obliged to store data themselves for such purposes. In this respect, the traffic data storage by the BND is not comparable with the so-called data retention by providers of telecommunications services, which was the subject of the judgment of the court in the *Tele2 Sverige and Watson* cases. Rather, the data relevant to the intelligence services is not stored by the telecommunications service providers, but is securely stored by the BND in its own systems.

59 The BND may collect and process traffic data only within the context of 'foreign-foreign signals intelligence' or in the context of restrictions pursuant to the Article 10 Law. Unlike in the case of data retention by private service providers, the statutory provisions that enable the intelligence services to store traffic data are directed at public authorities. By contrast, in the case of strategic signals intelligence, private service providers are merely obliged to tolerate the collection of data on their premises by the BND by means of technology to be provided by the latter. [25] Encroachment on the rights of the persons affected by data traffic storage is therefore attributable to the BND, not private service providers. Obligations of providers of

[25] Cf. Paragraph 27(3) of the Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Regulation on the technical and organisational implementation of measures for monitoring telecommunications), in the version published on 11 July 2017 (BGBl. I, p. 2316), which was amended by Article 16 of the Law of 17 August 2017 (BGBl. I, p. 3202).

telecommunications services that serve to support the BND in the performance of its duties are only governed in individual provisions, whereby these obligations to contribute are confined to enabling surveillance by the BND. The provider of telecommunications services is also not hindered in terms of its business activity that is relevant to the internal market. Accordingly, it does not have to retain any data itself, invest in data collection techniques or provide its own staff to collect, hold or even evaluate telecommunications data.

60 By contrast, in the case of the data retention that was the subject of the judgment of the court in the *Tele2 Sverige and Watson* cases, there is a triangular relationship between law enforcement authorities, providers of telecommunications services and the person concerned: the law enforcement authorities would like to use the data under certain conditions. The service provider retains the data using its own infrastructure of technical and human resources and releases it to the law enforcement authorities upon request. The person concerned is exposed to two parties here – unlike in the case of traffic data storage by the intelligence services.

2. Consequences of transferring the requirements of the *Tele2 Sverige and Watson* judgment to the activity of the intelligence services

61. In the *Tele2 Sverige and Watson* judgment, the Court of Justice imposed a series of requirements on the access of law enforcement and security authorities to traffic data: restriction of access to bulk communications data, prior authorisation for the access, obligation to inform the person concerned, storage of all data within the EU. If these requirements were to be transferred to the activity of the intelligence services, which is of a different nature and oriented towards advance surveillance, the intelligence services would be significantly hindered in the proper performance of their tasks.

62 In particular, a restriction of the non-targeted access to bulk communications data so that it is based on ‘special situations’ and ‘specific cases’ is not transferrable to the automated bulk processing of such data by the BND. This is because non-targeted access to telecommunications data serves to identify initially unknown threats to national security via the use of appropriate filter criteria as well as the subsequent identification of networks in the case of a threat not identified until a later point.

63 A restriction of the possibility for the intelligence services to collect data would lead to significant losses of information for the BND and could for instance prevent the timely identification of accomplices in attacks. If access to this data were restricted, these possibilities, which are important for national security, would be lost and it would lead to significant losses of intelligence. If the data protection acquis under EU law were to be applicable whenever providers of telecommunications services are involved

in the activity of the intelligence services in some way, Article 4(2) TEU would be impermissibly restricted if an intelligence service has to work together with private third parties in its activity in the interests of national security.

64 For the requirement of prior authorisation on a case-by-case basis, the Federal Government – like the referring tribunal – also identifies considerable difficulties in determining the point in time, as the activity of the intelligence services that is oriented towards the acquisition of information from abroad is not dependent on specific offences or investigative procedures. Considerable practical problems can also be seen here if a form of general obligation to inform the persons concerned were to be adopted. Specific obligations to inform are already governed in the sectoral laws for the intelligence services. The persons concerned are regularly located abroad; there is often a threat to national security irrespective of the identity of an individual person and irrespective of the circumstances of a specific investigative procedure. A general obligation to inform could therefore result in confidential information regarding the methodology for obtaining information having to be disclosed. This would have considerable consequences for the BND's ability to acquire information and, in a comparable manner, for the Federal Office for the Protection of the Constitution, with the result that important intelligence sources would dry up.

3. No reduction in the level of protection of fundamental rights if Directive 2002/58 and the Charter of Fundamental Rights of the EU were not applied

65 Non-application of Directive 2002/58 and of the Charter of Fundamental Rights of the EU will not lead to a reduction in the level of protection for the fundamental rights of the telecommunications users affected by measures of intelligence services. It is true that reserving competence in matters of national security to the Member States means that the scope of EU law does not include activities of the security and intelligence services, and the Charter of Fundamental Rights of the EU is therefore inapplicable pursuant to the first sentence of Article 51(1) thereof.

66 The national (constitutional) law of the Member States, including the fundamental rights guaranteed in that law, applies instead.

67 The guarantees of the ECHR also apply.

E. CONCLUSION

68 Against this background, the German Federal Government takes the view that the first question referred should be answered as follows:

A direction by a public authority 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 for the purposes of safeguarding national security falls, in the light of Article 4(2) TEU, within the sole responsibility of each individual Member State.

[signature]

Henze