Written observations of Poland

Case C-623/17 *

Document lodged by:

Republic of Poland

Usual name of the case:

PRIVACY INTERNATIONAL

Date lodged:

15 February 2018

* Language of the case: English.

Warsaw, 15 February 2018

TO THE PRESIDENT AND MEMBERS
OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

WRITTEN OBSERVATIONS OF THE REPUBLIC OF POLAND

submitted pursuant to Article 23 of the Statute of the Court of Justice of the European Union
in proceedings for a preliminary ruling in Case

C-623/17
Privacy International
(national court or tribunal: Investigatory Powers Tribunal — United Kingdom)

Agent of the Republic of Poland:
Bogusław Majczyna

Address for service:
Ministry of Foreign Affairs
al. J. Ch. Szucha 23
00-580 Warsaw — POLAND

TABLE OF CONTENTS

I. SUBJECT MATTER OF THE CASE AND QUESTIONS REFERRED FOR A PRELIMINARY RULING

1 The request for a preliminary ruling in Case C-623/17 *Privacy International* was submitted by a court in the United Kingdom (the Investigatory Powers Tribunal — London). This court is hearing an action brought by Privacy International — a non-governmental human rights organisation — against the United Kingdom authorities (the Secretary of State for Foreign and Commonwealth Affairs, the Secretary of State for the Home Department, and three intelligence and security agencies, namely, GCHQ, MI5 and MI6).

2 Privacy International questions whether national legislation enabling the British intelligence and security services to acquire and use bulk telephone and internet communications data, including the location of mobile and landline phones from which calls are made or received and the location of computers that are used to obtain internet access, is compliant with EU law.

3 The referring court has doubts as to whether EU law, in particular Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)? [1] and the case-law of the Court issued on that basis, apply to the bulk acquisition of communications data by the security services. In the light of these doubts, the referring court has submitted the following questions to the Court of Justice:

In circumstances where:

(a) the capabilities of the Security and Intelligence Agencies ('SIAs') to use Bulk Communications Data ('BCD') supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;

(b) a fundamental feature of the SIA's use of the BCD is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of the BCD in one place; its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;

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

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

[1] OJ 2002 L 201, p. 37, as amended.

requirements of the Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR'); and

(e) *the national court has found that the imposition of the requirements specified in paragraphs 119-125 of the judgment of the Grand Chamber of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 119-125 ['the Watson Requirements'], if applicable, would frustrate the measures taken to safeguard national security by the SIAs, and thereby put the national security of the United Kingdom at risk;*

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

II. POSITION OF THE REPUBLIC OF POLAND

II.1. National security — an area that remains within the competence of Member States

4 In the opinion of the referring court, the activities of the British intelligence services challenged by Privacy International are necessary to protect the United Kingdom's national security and thus do not fall within the scope of EU law but remain within the exclusive competence of the Member State.

5 The Republic of Poland shares this position, which in its opinion is based on the provisions of the Treaties.

6 Pursuant to Article 4(2) of the Treaty on European Union (TEU), the European Union is required to respect 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.

7 Competence within the area of national security (internal security) is likewise reserved for the Member States in the provisions of the Treaty on the Functioning of the European Union (TFEU) concerning the area of freedom, security and justice (AFSJ).

8 Although, pursuant to Article 4(2)(j) TFEU, the AFSJ is among the areas of competence shared between the European Union and the Member States, the provisions of the TFEU relating to the AFSJ (included in Part Three, Title V, TFEU) do not apply to the activities of agencies responsible for ensuring national security. As indicated in Article 67 TFEU, the European Union's actions in respect of the AFSJ focus on framing a common policy on asylum, immigration and external border control, and on preventing and combating crime, racism and xenophobia, among others, through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments.

9 Article 72 TFEU, contained in Title V, Chapter 1, which defines the general principles for the AFSJ, states — in a similar way to Article 4(2) TEU — that Title V does not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

10 Furthermore, it follows clearly from Article 73 TFEU that cooperation and coordination between the competent departments and administrations responsible for safeguarding national security are organised by the Member States themselves and under their responsibility.

11 The cited Treaty provisions should be interpreted in the light of the principle of conferral referred to in Article 5(1) and 5(2) TEU, under which the European Union is to act only within the limits of the competences explicitly conferred upon it by the Member States.

12 In the opinion of the Republic of Poland, it follows unequivocally from the wording of Article 4(2) TEU and of Articles 72 TFEU and 73 TFEU that national security (internal security) remains within the exclusive competence of the Member States. This is not, therefore, a non-harmonised area in which the European Union has regulatory powers that it has not yet exercised, but an area that comes clearly within the exclusive competence of the Member States. This conclusion applies, in particular, to the activities of agencies responsible for national security. It is apparent from Article 73 TFEU that the European Union does not have competence even in respect of cross-border contacts between intelligence and security services. *A fortiori*, it cannot be claimed that the European Union is entitled to regulate or organise their own (internal) activities.

13 The foregoing interpretation, in the context of EU provisions on the protection of personal data and privacy, is confirmed by the wording of Directive 2002/58/EC.

According to recital 11 of that directive, certain areas, including State security, do not come within its scope. The recital is worded 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 …’

14 Article 1(3) of Directive 2002/58/EC provides that the Directive does 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.

15 Similar reservations are contained in other EU legal acts relating to the protection of personal data: Directive 95/46/EC [2] (recital 13 and Article 3(2)), Directive (EU) 2016/680 [3] (recital 14 and Article 2(3)) and Regulation (EU) 2016/679 [4] (recital 16 and Article 2(2)).

16 As the above observations show, activities in the area of State security are — at the level of both primary and secondary law — consistently come within the exclusive competence of the Member States.

17 Even if it were accepted that due to the existence of cross-border threats the European Union could, in the light of the principle of subsidiarity expressed in

[2] 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 L 281, p. 31), as amended.

[3] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

[4] 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).

Article 5(3) TEU, adopt certain regulations under the AFSJ aimed at protecting national security, under no circumstances should such regulations limit or render ineffective the activities of national agencies responsible for ensuring national security.

18 *A fortiori*, this must not be the effect of EU regulations adopted on a different basis, governing issues related to the internal market or to the protection of personal data. Yet this would be precisely the consequence of finding that it is possible to designate, by way of an interpretation of Article 15(1) of Directive 2002/58/EC, the principles and limits of access to telecommunications data by agencies responsible for ensuring national security.

II.2. The concept of national security

19 It follows from the discussion contained in section II.1 of these Observations that if it is established that a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the national security and intelligence agencies comes within the scope of activities aimed at safeguarding national security, then the provisions of EU law, including of Directive 2002/58/EC, will not apply to that direction.

20 In order to answer the first question referred for a preliminary ruling, therefore, the scope of the concept of national security must be determined.

21 That concept is not defined either in the Treaties or in Directive 2002/58/EC. Recital 11 and Article 1(3) of that Directive merely indicate that the concept covers the economic well-being of the State when the activities relate to State security matters.

22 The wording of Article 15(1) of Directive 2002/58/EC suggests that the concepts of national security and State security are used interchangeably. [5] In the opinion of the Republic of Poland, the concept of internal security, used in Article 72 TFEU, is also identical because that provision refers, on the grounds of the AFSJ, to Article 4(2) TEU.

23 On the other hand, as indicated in recital 11 and Article 1(3) of Directive 2002/58/EC, State security must be distinguished from public security and defence, which are listed separately in that article. Such an interpretation is justified by the provisions of the Treaties. It should be noted that Part Three, Title V, TFEU does not use those concepts. However, defence issues are included in Title V TEU, which refers to the European Union's foreign and security policy. Public security, in turn, is referred to in the provisions of the TFEU on the freedoms of the internal market (Articles 36, 45, 52 and 65) and on the movement of workers between the European Union and overseas countries and territories

[5] That provision mentions measures necessary 'to safeguard national security (i.e. State security)'.

(Article 202) as one of the grounds for derogation from general principles, and not as an area excluded from the competence of the European Union.

24 Therefore, in order to establish the scope of the concept of national security, referred to in Article 4(2) TEU, reference should be made to the case-law of the Court of Justice. However, although there exists a rich body of case-law in relation to the concept of public security in the context of internal market freedoms, [6] for the reasons set out above it does not seem to apply in the present case as regards distinguishing the competences of the Member States from those of the European Union under Article 4(2) TEU.

25 The Republic of Poland takes the view that it is up to the Member States to determine what is meant by national security in this situation. The interpretations adopted by individual States may differ slightly. Nevertheless, as a common basis we should assume that national security is one of the principal functions of every State and includes the issue of countering all manner of external and internal threats to the existence and development of the nation and the State. [7] It is beyond doubt, therefore, that national security covers at least the activities of intelligence and counter-intelligence services, the economic security of the State, counter-terrorism and counter-proliferation of weapons of mass destruction.

26 The above activities are undertaken both by departments responsible for internal security in the broad sense, including the police, and by the intelligence services. These activities are primarily of a preventive nature and are designed to counter threats, especially terrorism and unlawful access to weapons (including weapons of mass destruction).

27 The assessment as to whether an activity is necessary to safeguard national security falls to the Member States and may be subject to scrutiny by national courts.

28 In the present case, the national court has already made such an assessment; it found that the activities of the security and intelligence services under dispute are necessary for the protection of national security. The activities in question should therefore be considered to come within the scope of Article 4(2) TUE.

II.3. Interpretation of Article 15(1) of Directive 2002/58/EC

29 Article 15(1) of Directive 2002/58/EC provides as follows:

‘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),

[6] Judgment of 24 June 2015, *T.*, C-373/13, EU:C:2015:413, paragraphs 76 to 78 and the case-law cited therein.

[7] Grzelak, A. in *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz LEX*, vol. 1, edited by A. Wróbel, Lex and Wolters Kluwer Business, Warsaw, 2012, pp. 1097 and 1098.

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.'

30 The explanations relating to the above provision are included in recital 11 of Directive 2002/58/EC, cited in point 13 of these Observations.

31 The explanations contained in the aforementioned recital unequivocally show that Directive 2002/58/EC does not address the protection of fundamental rights and freedoms linked to activities which remain within the exclusive competence of the Member States, including measures taken by the Member States to safeguard national security. Such activities are assessed solely on the basis of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

32 A different interpretation would deprive both Article 1(3) of Directive 2002/58/EC, which defines its material scope, and Article 4(2) TEU of *effet utile*. Contrary to the reasoning of the judgment in *Tele2 Sverige and Others*, [8] the Republic of Poland believes that it is Article 1(3) of Directive 2002/58/EC which defines the scope of the exceptions indicated in Article 15(1) of the Directive, and not the reverse. Limiting the material scope of Directive 2002/58/EC, as provided for in Article 1(3), would become meaningless if the requirements of that directive were applicable to areas excluded from its scope and falling within the exclusive competence of the Member States.

33 It should also be emphasised that secondary legislation, such as Directive 2002/58/EC, must not affect the competences of the Member States, since the Member States have not only not conferred those competences (in the area of national security) upon the European Union under the Treaties, but have also expressly reserved those competences for themselves. That would be a clear breach of the principle of conferral.

34 It is obvious, then, that Article 15(1) of Directive 2002/58/EC may apply only to measures that come within the material scope of the Directive, and not to measures that have been explicitly excluded from that scope. The rights and obligations referred to in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of Directive 2002/58/EC do not apply to areas excluded from the material scope of that directive by Article 1(3) thereof, including the area of State security. The introduction of a provision allowing derogation from those rights

[8] Judgment of 21 December 2016, *Tele2 Sverige and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 72 and 73.

and obligations in the aforementioned areas was essentially unnecessary. In this respect, Article 15(1) of Directive 2002/58/EC is a superfluous (and not very well formulated) provision, whose intention was to recall and highlight the competences of the Member States in areas excluded from the scope of that directive, including in the area of national security. It is not possible, therefore, to accept an interpretation of that provision that would deprive the Member States of their competences in those areas and thus have the effect of being completely contrary to the intentions of the EU legislature.

35 The reasoning of the judgment in *Parliament* v *Council and Commission* should apply to the present case. [9] When interpreting Article 3(2) of Directive 95/46/EC, on which Article 1(3) of Directive 2002/58/EC was based, the Court found that it excludes from the Directive's scope the processing of personal data in the course of an activity which falls outside the scope of Community law, and in any case processing operations that aim to safeguard, inter alia, State security. In the light of the above, the Commission's decision on adequate protection, [10] which concerns the processing of data deemed necessary to safeguard public security and to combat crime (and not the processing of data necessary for the provision of services), does not come within its scope.

36 Consequently, the Court acknowledged the legitimacy of the European Parliament's claim that the adoption of the Commission decision was *ultra vires* because the provisions laid down in Directive 95/46/EC had not been complied with; in particular, the first indent of Article 3(2) of the Directive, relating to the exclusion of activities which fall outside the scope of Community law, was infringed.

37 Consequently, it should be acknowledged that it is likewise not possible to assess national provisions governing the issues listed in Article 3(2) of Directive 95/46/EC in terms of their compliance with the provisions of that directive. Since the provisions defining the scope of Directives 95/46/EC and 2002/58/EC were structured in the same way, and the subject of those directives is essentially the same, [11] the above conclusion will also apply in the present case. The regulations and the activities of national authorities referred to in Article 1(3) of Directive 2002/58/EC, and which remain within the competence of the Member States, are not therefore subject to assessment under the provisions of that directive.

[9] Judgment of 30 May 2006, *Parliament* v *Council and Commission*, C-317/04 and C-318/04, EU:C:2006:346, paragraphs 54 to 59.

[10] Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record (PNR) of air passengers transferred to the United States' Bureau of Customs and Border Protection (2004/535/EC) (OJ 2004 L 235, p. 11).

[11] Directive 2002/58/EC translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

38 An assessment of compliance with the conditions laid down in Article 15(1) of Directive 2002/58/EC means — as indicated by the judgment in *Tele2 Sverige and Others* [12] — an assessment of compliance with the general principles of EU law and Articles 7 and 8 of the EU Charter of Fundamental Rights. However, pursuant to Article 51(1) of the Charter, the provisions of the Charter are addressed to the Member States only when they are implementing EU law. [13] They do not, therefore, apply to the area of national security, which — as already explained in these Observations — remains within the exclusive competence of the Member States. Article 51(2) of the Charter confirms that its effect cannot be to extend the scope of EU law beyond the powers laid down in the Treaties. [14] Yet it is hard to deny that precisely such an effect would be achieved if the reasoning of the judgment in *Tele2 Sverige and Others* were applied to the present case.

39 In paragraph 104 of the judgment in *Tele2 Sverige and Others*, the Court stressed that the effect of the general obligation introduced by national legislation to retain telecommunications data is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58/EC requires the retention of data to be the exception. And since it is an exception, it should be interpreted restrictively. Thus, the Court de facto assessed a national measure in the light of Directive 2002/58/EC, which cannot occur in relation to matters that remain within the exclusive competence of the Member States.

40 Furthermore, even if it were assumed, *quod non*, that Article 15(1) of Directive 2002/58/EC applies in the present case, the assessment of the justification for, and proportionality of, measures adopted for the purpose of combating crime, made by the Court in paragraphs 102 and 103 of the judgment in *Tele2 Sverige and Others*, cannot be applied to activities concerning the protection of national security.

41 It must be borne in mind that the nature of activities related to combating crime and the nature of activities related to protecting national security are fundamentally different. The predominant criminal analysis model used in combating crime is based on ex-post data analysis, which means that in many cases police authorities already have a particular suspect (or at least a particular group of people who are suspects). By contrast, activities related to the protection of national security (State security) largely involve preventive actions aimed at countering threats, particularly terrorism and illegal and uncontrolled arms trafficking.

42 For example, identifying the perpetrator of a murder requires different techniques from those involved in establishing whether there is a risk of terrorist attack, since

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

[13] Judgment of 13 April 2000, *Karlsson and Others*, C-292/97, EU:C:2000:202, paragraph 37.

[14] Cf. the explanations to Article 51 included in the Charter.

the latter may be planned by unidentified individuals, at an unspecified point in time, in any location and using unknown methods.

43 The activities of agencies responsible for State security (both external and internal) include the use of data interrogation techniques that are non-targeted, in other words, not directed at specific, known targets, but rather at a wide range of entities, which may include entities engaged in activity that poses a threat to State security. As a consequence, the acquisition of bulk communications data, including, in particular, traffic and location data as well as social, commercial, financial, connection and travel data, is an essential element of the aforementioned preventive actions taken by the agencies concerned.

44 If the reasoning of the judgment in *Tele2 Sverige and Others* were also applied to the activities described above of agencies responsible for safeguarding State security, the effect would be to deprive those agencies of the tools necessary for the performance of their tasks and would pose a genuine threat to the national security of the Member States.

III. PROPOSAL FOR A DECISION

45 In the light of the foregoing considerations, the Republic of Poland proposes that the referring court's first question be answered as follows:

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 does not come within the scope of EU law or of Directive 2002/58/EC (Directive on Privacy and Electronic Communications).

Given the proposed answer to the first question, the Republic of Poland does not provide an answer to the second question.

Bogusław Majczyna
Agent of the Republic of Poland