Observations of the Czech Republic

Case C-623/17 *

Document lodged by:

Czech Republic

Usual name of the case:

PRIVACY INTERNATIONAL

Date lodged:

13 February 2018

Ministerstvo zahraničních věcí České republiky

(Ministry of Foreign Affairs of the Czech Republic)

Loretánské nám. 5, 118 00 Prague 1, tel. +420 224 182 310, fax +420 224 183 029, email okp_sekretariat@mzv.cz

Prague, 13 February 2018

WRITTEN OBSERVATIONS

submitted in accordance with Article 23 of the Protocol on the Statute of the Court of Justice of the European Union by the

CZECH REPUBLIC

represented by Martin Smolek, Jiří Vláčil and Ondřej Serdula

in Case C-623/17

Privacy International

concerning a request for a preliminary ruling submitted to the Court of Justice pursuant to Article 267 of the Treaty on the Functioning of the European Union by the *Investigatory Powers Tribunal*, United Kingdom, on 31 October 2017.

* Language of the case: English.

The Czech Republic submits the following written observations on the above case:

1 Facts of the case and proceedings before the national court

1 For details of the dispute, the Czech Republic refers to the text of the order for reference.

2 Relevant provisions of national and EU law

2 The Czech Republic refers to the relevant provisions of national and EU law set out in the order for reference.

3 Questions referred to the Court of Justice for a preliminary ruling

3 The following questions have been referred 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 SIAs' 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 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 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15 (EU:C:2016:970)] ('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 ('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?*

4 Position of the Czech Republic on the questions referred

4 By the questions referred, the referring court essentially asks whether the transfer of traffic and location data by the provider of an electronic communications service to the intelligence services, so that they may perform their tasks in the national security field, falls within the scope of EU law. If so, the referring court asks whether the criteria applied in the assessment of the proportionality of such a breach of the rights to privacy and to the protection of personal data correspond with those which the European Court of Human Rights ('ECtHR') has defined in this connection in the interpretation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, or whether some of the conditions which the Court of Justice defined in *Tele2 Sverige* [1] apply.

5 Should the Court of Justice consider the processing concerned to fall within the ambit of EU law, the Czech Republic hereby sets out its answer to the second question referred.

4.1 The criteria applied in the assessment of the proportionality of the data transfer

6 Were the Court of Justice to hold that EU law applies in the present case, the Czech Republic takes the view that the criteria applied to assess the proportionality of the breach of the rights to privacy and to the protection of personal data must be distinguished from those which the Court of Justice set out in *Tele2 Sverige*. The proportionality or not of processing personal data for the

[1] Judgement of 21 December 2016, *Tele2 Sverige* v *Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970.

purposes of safeguarding national security cannot be assessed on the basis of the same criteria as those relied on in cases concerning criminal investigations.

7 **First**, it is always necessary to analyse the proportionality of the breach of the right to privacy and protection of personal data having regard to the specific purpose of the data-processing. Thus certain purposes for which data is processed may justify a greater breach of fundamental rights than others. In this connection, it is necessary, according to the Czech Republic, to take into consideration both the nature and the seriousness of the threat which such data-processing is supposed to avert, and the possibility of combatting that threat by other means.

8 **Secondly,** threats to national security (in the case in question namely international terrorism, counter-espionage and counter-nuclear proliferation) [2] in general pose the highest degree of danger to society, even in comparison to serious crime, the investigation of which was the subject of the Court of Justice's assessment in *Tele2 Sverige*. Threats to national security are characterised by the fact that they are very difficult to combat without the use of modern methods such as, for example the analysis of traffic and location data. For those reasons, in paragraph 119 of the judgment in *Tele2 Sverige* the Court of Justice moreover expressly conceded, in connection with restricting access to personal data for the purposes of combatting crime, that if vital national security interests are threatened no judicial limitations need be applied.

9 Accordingly, it must be noted that, unlike in criminal cases, in cases concerning national security even the actual identification of a threat is extremely difficult. That is because those threats change continuously and the expansion of communication technologies is contributing greatly to the speed of such development. Thus, in cases where there is a threat to national security, there is no list of crimes posing a more-or-less clearly identified danger to society which may be balanced against the potential breach of fundamental rights.

10 For those reasons, in cases concerning the security services the method of handling personal data must also differ considerably from the method used by the competent bodies in criminal proceedings. Whereas in criminal proceedings personal data is generally processed *ex post* (after the commission of a criminal offence), in safeguarding national security it is of critical importance that threats may primarily be identified *ex ante*, enabling preventative action to be taken where necessary. Therefore, the possibility to analyse data in bulk form is absolutely key to the security services' successful performance of their tasks.

11 Furthermore, the State bodies in that field are not always opposed by mere individuals or small groups of persons engaged in criminal activity, but in general by enemy non-State or even State actors, frequently operating on a global scale, whose potential to target the fundamental interests of the State is disproportionately greater than that of a normal criminal.

[2] See page 2 of the summary of the order for reference.

12 That field is also characterised by the fact that revealing the methods and procedures used by the intelligence services in one particular case may critically hinder or obstruct the execution of their activities in the future. There is therefore a much greater emphasis on concealing the activities and methods used by the intelligence services, which sometimes continues decades after a specific data breach. The procedural arrangements governing breaches of fundamental rights and freedoms (for example, in relation to the requirements to inform the data-subject or the review of the activities of the intelligence services) must usually be more flexible, precisely because of the essentially hidden character of the activities of the intelligence services, which is necessary in the interest of ensuring such activities are effective.

13 It thus follows from the above that the threats to national security are continuously evolving in line with the dynamics of international relations and the security environment, and the consequences of any disturbance of the protected interests are difficult to quantify. It is also true that those wishing to create threats now have considerably greater resources available to them, such resources often being comparable to the capacities of the States defending themselves against the threat.

14 **Third**, it must further be stated that there is a less of a breach of fundamental rights where personal data is processed by the intelligence services than in the field of criminal investigations. Thus, in the case of a criminal investigation, there can in principle be only two consequences of the use of information acquired by a breach of fundamental rights and freedoms – either the information is relevant for the decision on guilt or innocence, and is used for that purpose (that is to say, resulting in a further restriction on rights and freedoms, for example in the form of a prison sentence), or it is not relevant, and is therefore destroyed or restored. On the other hand, even where information is used with success for the purposes of the security and fundamental interests of the State, that usually does not impact directly on the fundamental rights and freedoms of persons in the above sense (such use may, for example, be purely for analytical purposes, or be such that its impact on the individual in personal terms is much less serious – for example the refusal of a visa).

15 It follows from the above that the test for assessing the proportionality of data-processing in connection with combatting threats to national security must be more flexible than that applied in the field of criminal investigations. The criteria applied to assess proportionality must therefore be distinguished from those defined by the Court of Justice in *Tele2 Sverige*. Having regard to the fact that there is an established line of case-law which has been developed by the ECtHR in this field, which reflects the abovementioned matters, the Czech Republic submits that the criteria applied to assess the proportionality of any data-processing should correspond with the test defined by the ECtHR in this field.

5 Answer proposed to the Court of Justice by the Czech Republic

The criteria defined in the judgment in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige v Watson and Others* are not to be applied to the transfer of traffic and location data by the provider of an electronic communications service to the intelligence services, so that the latter may perform their tasks in the national security field.

The criteria applied to assess the proportionality of the transfer of traffic and location data by the providers of electronic communications services to the intelligence services, so that the latter may perform their tasks in the national security field, are to correspond to those which the European Court of Human Rights have defined in this connection in the interpretation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

[signature]

Ondřej Serdula
Agent for the Czech Republic before the Court of Justice of the EU

Jiří Vláčil
Agent of the Czech Republic before the Court of Justice of the EU

Martin Smolek
Government Agent of the Czech Republic before the Court of Justice of the EU