Translation C-623/17 - 22

Observations of Sweden

Case C-623/17 *

Document lodged by:

Kingdom of Sweden

Usual name of the case:

Privacy International

Date lodged:

14 February 2018

Regeringskansliet 2018-02-14

UDEUD2017/490

Utrikesdepartementet Court of Justice of the European Union

Rättssekretariatet

Written observations

lodged by the Swedish Government, represented by departementsrådet Anna Falk and rättssakkunniga Hanna Shev, Utrikesdepartementet, SE 103 39 Stockholm, in Case

C-623/17

Privacy International

concerning the request for a preliminary ruling under Article 267 FEUF made by the Investigatory Powers Tribunal, concerning whether certain measures intended to safeguard national security fall within the scope of EU law, including [Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in

* Language of the case: English.

the electronic communications sector; 'the e-Privacy Directive'], and if that is the case, how EU law is to be interpreted.

1. Background and the national court's questions

1 The case concerns the United Kingdom's Security and Intelligence Agencies' ('SIAs') acquisition and use of significant amounts of communications data, referred to in the UK case as bulk communications data ('BCD'). Such data include information on with whom, when, where and how the communication took place. BCD include communications via both telephone and internet. They include location data for mobile and landline telephones from which calls are made or to which calls are received and for computers which are used to connect to the internet. BCD do not, however, include the content of those communications. Access to their content requires a court decision.

2 Under section 94 of the UK Telecommunications Act 1984, a Secretary of State may give to an operator of a Public Electronic Communications Network ('PECN') such general or specific directions as appear to the Secretary of State to be necessary in the interests of national security. The SIAs acquire BCD from PECNs in accordance with those directions and hold them securely. A fundamental feature of many of the SIAs' techniques of interrogating BCD is that the techniques are non-targeted, i.e. not directed at specific, known targets.

3 The applicant has brought proceedings before the national court and argued that the SIAs' acquisition and use of BCD disregards Article 8 of the [European Convention on Human Rights] and runs counter to EU law. The defendants are of the opposite view and have argued that their measures are lawful and necessary, inter alia to protect national security by counter-terrorism, counter-espionage and nuclear non-proliferation measures.

4 Against that background, the national court referred two questions for interpretation to the Court, the first of which is the subject of the Swedish Government's observations here:

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 [SIAs] … of a Member State fall within the scope of EU law and of the e-Privacy Directive?

2. The position of the Swedish Government

5 As an introductory point, the Swedish Government notes that the referring court has ruled that the acquisition of BCD must be as comprehensive as possible if

their acquisition is to be effective and thus necessary to achieve their intended aim, [1] that the handling of data is surrounded by necessary safeguards as regards the arrangements for storing and retaining BCD, procedures for accessing BCD and disclosing BCD outside the SIAs, [2] and that acquisition of BCD and automated processing by the SIAs is less intrusive than other means of obtaining information. [3]

6 The Swedish Government is of the view that such requirements in directions given by a Secretary of State to a provider of an electronic communications network concerning the acquisition of BCD in order to safeguard national security does not fall within the scope of EU law. The Government sets out below the reasons for its view in more detail.

3. Assessment

3.1 National security is within the exclusive competence of the Member States

7 Under Article 4(1) TEU, in accordance with Article 5, competences not conferred upon the European Union in the Treaties remain with the Member States. Article 5(1) TEU provides that the limits of EU competences are governed by the principle of conferral. Under Article 4(2) TEU, the European Union is to respect the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, it is stressed that national security remains the sole responsibility of each Member State. That fact is also reflected in the list of the categories and scope of the EU competencies set out in Articles 2 to 6 TFEU, where questions of national security are *not* mentioned. Questions concerning national security are thus exclusively within the competence of the Member States.

8 The EU legislature has confirmed, in various ways, that division of competences in secondary legislation, concerning, inter alia, the Member States' measures for protecting their own essential State interests, particularly with regard to safeguarding national security. [4]

1 [Summary] request for preliminary ruling, paragraphs 3 and 4.

2 [Summary] request for preliminary ruling, paragraph 5.

3 [Summary] request for preliminary ruling, paragraph 6.

4 C.f., for example, recital 16 of 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) and Article 1(6) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

9 Article 1(3) of the e-Privacy Directive [5] states that it is not to 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.

10 The e-Privacy Directive seeks to make more specific and to supplement 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. There is also a provision in that directive, corresponding to Article 1(3) of the e-Privacy Directive, which expressly excludes activities in certain areas from the scope of the directive. [6]

11 Directive 95/46/EC has now been replaced by Regulation No 2016/679. [7] The EU legislature has thereby continued to confirm the division of competences by stating in recital 16 of Regulation No 2016/679 that the regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of EU law, such as activities concerning national security.

12 It is therefore clear from the provisions of primary and secondary law, the meaning of which has been confirmed and almost strengthened over time, that the EU legislature was careful to exclude measures concerning national security from the scope of EU law. The reason for that is that the Member States, as sovereign States, must be guaranteed the freedom to exercise one of their truly central tasks in accordance with national law and to act to safeguard national security on the basis of the threat scenario and specific existing needs. It is by the State that the citizens require and expect their security to be safeguarded.

13 A direction from a Secretary of State on the transmission of BCD to a Member State's SIAs in order to safeguard national security thus does not, as such, fall within the scope of EU law.

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[6] See 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.

[7] 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.

3.2 The measures at issue intended to ensure national security do not concern the functioning of the internal market

14 The Court of Justice has held in case-law that the Member States' measures in a particular area cannot wholly be excluded from EU law on the sole ground that the measures are taken with a view to public security or national defence. [8] That has affected situations where the global question concerned the functioning of the internal market. [9]

15 On the question, for example, of duty-free imports of equipment for, inter alia, military use, judgment in *Commission* v *Italy*, C-387/05, the Court of Justice held that recognition of the existence of a general exception excluding all measures taken for reasons of public security would be liable to impair the binding nature of EU law and its uniform application. [10] A Member State cannot be allowed, for instance, to plead the increased cost of military material because of the application of customs duties on imports of such material from third countries in order to avoid, at the expense of other Member States who collect and pay the customs duties on such imports, the obligations which the principle of joint financing of the EU budget imposes on it. [11]

16 The Court of Justice followed a similar line of reasoning in the judgment in Dory, C-186/01. In that case, the Court held that it was clear that the Member States' decisions on the organisation of their armed forces could not be exempted from the scope of Community law. That applied particularly to questions of compliance with the principle of equal treatment of women and men as regards conditions of employment, inter alia, access to military professions. The Court underlined, however, that that does not mean that Community law governed the decisions which the Member States make with regard to their military organisation in the defence of their territory and/or their essential interests. It is for the Member States to decide on appropriate measures to safeguard internal and external security. [12]

17 The abovementioned cases differ from the present case, however, in which the measures are adopted in an area where the Member States have exclusive competence and for purposes different from those which are covered by EU law. Accordingly, those measures are without any connection to EU law.

8 See, for example, judgments in *Dory*, C-186/01, EU:C:2003:146, paragraph 30, and *Commission* v *Italy*, C-387/05, EU:C:2009:781, paragraph 45.

9 Judgment in *Commission* v *Italy*, C-387/05, EU:C:2009:781, and judgment in *Dory*, C-186/01, EU:C:2003:146.

10 *Commission* v *Italy*, C-387/05, EU:C:2009:781, paragraph 45.

11 *Ibid*, paragraph 50.

12 Judgment in *Dory*, C-186/01, EU:C:2003:146, paragraphs 35 to 36 and the case-law cited.

18 The present case concerns activity in which the SIAs are responsible for the storage of BCD and it is they, through their search techniques, who process the data in certain non-targeted ways. It is thus the State body and not the provider of telecom services which itself carries out the activity of processing the BCD in order to safeguard national security. That type of activity is not included in the harmonised area in the EU.

19 The fact that the data are requested from a provider whose activity is covered as such by the scope of the directive does not alter that assessment. The e-Privacy Directive does not govern the access to data or how that data may be used by the State authorities. [13]

20 The Court held, further, in Joined Cases C-317/04 and C-318/04, *European Parliament* v *Council and Commission*, that the transfer of the data in question, initially collected by companies in the framework of an activity which is governed by EU law, from those companies to an authority for processing concerning public security and State activities in the field of criminal law, was covered by Article 3(2) of Directive 94/46/EC. [14] The abovementioned provision excluded from the scope of the directive, as stated above in paragraph 10, the processing of personal data in the course of certain activities in a manner corresponding to the rule in Article 1(3) of the e-Privacy Directive. There is no reason to depart from the Court's assessment in that respect in the examination in the present case. Article 1(3) of the e-Privacy Directive cannot be deprived of its application *solely* on the ground that the competent authority requests access to BCD which is held by a provider.

21 In the Government's view, such a line of reasoning follows the general principles that the interpretation of an individual relevant provision of a directive must be made in the light of the provisions which define the scope of the whole directive. That interpretation must in turn be made in the light of the Treaties, having particular regard in that case to Article 4(2) TEU *in fine*.

22 If regard is not had to express restrictions on Union competences in the assessment of the scope of a directive, they become meaningless and lose their intended effect. In other words, a directive must not be applied to activities which are not carried out in the course of the harmonised rules under the directive.

23 In summary, the requirements in question concerning access to BCD accordingly do not concern the functioning of the internal market but are measures to safeguard national security, decisions concerning which are for the Member States alone to make.

[13] C.f. judgment in *Ireland* v *European Parliament*, C-301/06, EU:C:2009:68, paragraph 80.

[14] Joined Cases C-317/04 and C-318/04, *European Parliament* v *Council and Commission*, EU:C:2008:346, paragraphs 56 to 58, and judgment in *Ireland* v *European Parliament*, C-301/06, EU:C:2009:68.

3.3 The special status of national security interests

24 As stated above, it follows from the wording of both primary and secondary legislation that national security is an interest which has a special legal status in relation to other activities, such as, for example, State activity in the field of criminal law, since questions of national security are reserved to the competence of the Member States. Since the entry into force of the Treaty of Lisbon on 1 December 2009, it can be noted that questions in the field of criminal law, however, form part of the Union's supranational cooperation.

25 Nor can security and intelligence activities, which are fundamental to the ability to maintain a State's external and internal security, be compared, from a factual point of view, with, for example, the general combating of crime unconnected with national security. The Swedish Government wishes to point out the following in particular.

26 Intelligence activity concerning threats to national security, like all intelligence activity, sets out to discover in advance hidden factors and data pertinent thereto, within the framework of the relevant indications given by the requesting agency. That can involve, for example, data on new threats to that country's citizens or to confidential information which must not come into the hands of foreign powers. Intelligence activity also involves identifying factors already known and following changes in them in order to have early knowledge of the actors' new ambitions, intentions and capabilities. Typically, that is not observation of a particular person suspected of a crime, but the use of mostly non-targeted techniques, that is to say, techniques not directed against specific targets of which there is advance knowledge.

27 Intelligence activity concerning threats to national security is also a vital tool in identification after the event of incidents which occurred but were unforeseen, with a view to finding explanations for what happened and to identifying potential, previously-unidentified elements of an incident which took place. By such monitoring, further intelligence information can be produced which gives, on the one hand, a better understanding of the causes behind the incident and, on the other, supplementary information of elements not yet identified, for example other undiscovered threats. In that regard, access to BCD is particularly of the greatest importance so that the authority responsible can carry out effective intelligence work.

28 In the event that harmonisation in accordance with EU law of the processing of personal data and the protection of privacy were found to exist, as regards, in addition, intelligence activity concerning threats to national security, the risk is that it may not be possible to complete the identification of such threats. A reduction in access to BCD would mean a drastic worsening of the conditions under which intelligence activity provides support for the State's activity in safeguarding national security, including foreign, security and defence policy measures. The possibilities of protecting national security would be reduced,

including as regards protection against terrorism, foreign intelligence activity and IT threats. Lastly, restricted access to BCD would have significant consequences, making it less possible for intelligence activity to identify conflicts abroad which have consequences for international security and for Member States to participate in peace support and humanitarian operations.

3.4 The right to protection of privacy

29 The fact that national security activity falls outside the scope of EU law does not, however, mean that there is no protection for the privacy of individuals in the processing of their personal data. In addition to the national legislation in the present case and international legislation in the form, for example, of Council of Europe Data Protection Convention No 108, Article 8 of the European Convention has also been updated, as the English Court has pointed out. Whether the requirements under the provision are satisfied is something on the Court has no reason to rule, since that would assume that the case concerns facts involving EU law. [15] The Government notes, however, that the national court, so far as is clear from the request for a preliminary ruling, appears to consider that the requirements under the European Convention are satisfied.

4. Conclusion

30 In the light of the above, the Swedish Government is of the view that the national court's question should be answered as follows:

With regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications, a requirement in directions given by a Secretary of State to the provider of an electronic communications network, that the provider make bulk communications data available to a Member State's Security and Intelligence Agencies, is not regarded as falling within the scope of EU law, including Directive 2002/58/EC.

[Signatures]

Anna Falk Hanna Shev

[15] See judgment in *Bartsch*, C-427/06, EU:C:2008:517.