Observations of Latvia

Case C-623/17 *

Document lodged by:

Republic of Latvia

Usual name of the case:

PRIVACY INTERNATIONAL

Date lodged:

14 February 2018

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

WRITTEN OBSERVATIONS OF THE REPUBLIC OF LATVIA

In accordance with Article 23, second paragraph, of the Statute of the Court of Justice (the Court), the Republic of Latvia, represented by Irēna Kūciņa, assistant in charge of jurisdictional issues on behalf of Secretary of State at the Ministry of Justice and Viktorija Soņeca, lawyer at the office of the Agent of the Republic of Latvia, submits written observations in connection with the present request for a preliminary ruling in which, pursuant to Article 267 TFEU, questions were referred by the Investigatory Powers Tribunal (‘the UK Tribunal’) on 31 October 2017.

C-623/17

Privacy International

The Republic of Latvia accepts delivery of documents in the present case: (a) by letter to the following addressed: Ministry of Justice of the Republic of Latvia — Office of the Representative of the Republic of Latvia to the Court of Justice (address); (b) by fax: 00 371 670369211; (c) by email to the address estbirosjs@tm.gov.lv or (d) by e-Curia.

* Language of the case: English.

Table of contents

I. LEGAL PROVISIONS RELEVANT TO THE CASE

I.1. Provisions of European Union and International Law

1 The Treaty on the European Union ('the TEU') Articles 4, 5 and 6; [1]

2 The Treaty on the Functioning of the European Union ('the TFEU'), Article 16; [2]

3 The Charter of the Fundamental Rights ('the Charter'), Articles 7, 8 and 51; [3]

4 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 (Directive on privacy and electronic communications) (Directive 2002/58/EC'), recital 11, Articles 1 and 15; [4]

5 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 ('Directive 95/46/EC'), recital 13 and Article 3; [5]

6 The European Convention on the Protection of Human Rights and Fundamental Freedoms ('the ECHR'), Article 8.

I.2 The provisions of Latvian law

7 Article 71(1) of the Law on electronic communications [6]

'*Data that must be retained shall be retained and transferred to the authorities responsible for preliminary investigations, operational agents, national security services, prosecutors and courts in order to safeguard national security and public safety or to conduct criminal investigations, criminal prosecutions and the adjudication of criminal cases and to the Competition Council for the purposes of investigations regarding infringements of competition law taking the form of prohibited cartels'.*

[1] OJ 2010, C 83, p. 13.

[2] OJ 2010, C 83, p. 47.

[3] OJ 2010, C 83, p. 389.

[4] OJ 2002, L 201, p. 37.

[5] OJ 1195, L 281, p. 31.

[6] Latvijas Vēstnesis (Official Journal), 17 November 2004, No 183. Available at: https://likumi.lv!doc.php?id= 96611.

8 The Law on the national security services, Article 6, Article 19(1)(8) and Article 26(1) and (4) [7]

Article 6 of the Law on the national security services:

'*If a person considers that the national security services have, by their conduct, infringed his rights and freedoms enshrined by the Law, that person shall be entitled to lodge a complaint with the prosecutor who, after investigating that complaint, shall issue an opinion as to the legality of the conduct of the agent of the State security services, or shall institute proceedings (before a court).'*

Article 19(1)(8) of the Law on the national security services

'The agents of the national security services are entitled, within the scope of their competence, to receive, free of charge, information, documents and other necessary evidence relating to services supplied to individuals, including information from the holders of information resources and technical resources concerning the communications of individuals by post, telegraph, communications networks and data transmission'.

Article 26(1) of the Law on the national security services

'The Prosecutor General and prosecutors specially authorised by him shall oversee the procedure for operational activities, espionage and counter-espionage by the national security services and the system of protection of 'State secrecy'. When they carry out that supervision, they are authorised to access the documents, evidence and information which are in the possession of the national security services. The identity of sources of information is to be revealed only where they are *directly involved in the commission of a criminal offence, and only to the Prosecutor General and it shall be disclosed only to prosecutors specially authorised by him after authorisation by the head of the authority responsible for State security; the disclosure of the identity of sources of information in the course of surveillance procedure shall be prohibited.'*

Article 26(4) of the Law on the national security services

'The national security services shall be subject to judicial supervision in the situations and according to the procedures laid down by the Law on operational activities'.

9 Article 1 of the Law on national security [8]

[7] Latvijas Vēstnesis (Official Journal), 19 May 1994, No 59. Available at: https://likumi.lv!doc.php?id= 57256.

[8] Latvijas Vēstnesis (Official Journal), 29 December 2000, No 473/476 (2384/2387). Available at: https://likumi.lv!doc.php?id= 14011.

'1. National security is the result of joint and targeted measures implemented by the State and society, by which the independence of the State, its constitutional order, its territorial integrity, the possibility for society to develop without constraint, well-being and stability are guaranteed.

2. Guaranteeing national security is a fundamental obligation of the State'.

10 Article 9(5), Article 35(1) and Article 38 and point 7 of the transitional measures of the Law on operational activities [9]

'The acquisition of operational data from electronic communications operators — that is to say the acquisition of data in respect of which protection is legally provided for operators (data which must be retained) — shall be carried out with the consent of the person in charge of (head) of the body responsible for operational activities or an agent authorised by him, when he requests data from an electronic communications operator. If the data to be retained which relates to a person identified in a specific operational activity are requested for a period of more than 30 days in total, the body responsible for operational activities shall obtain the consent of the judge specially authorised by the Present of the District Court (of the city).'

Article 35(1) of the Law on operational activities

'The Prosecutor General and the prosecutors specially authorised shall oversee the procedures for operational activities. By overseeing those activities, they are themselves authorised to access information, documents and other evidence which is available to the body responsible for operational activities'.

Article 38(1) of the Law on operational activities

'When an opinion is issued on a complaint concerning the legality of the conduct of an operations agent, the prosecutor shall inform the complainant of the completion of the investigation and shall indicate (without further details) whether, during the investigation, illegal interference with the legal rights and freedoms of that person has been established. The prosecutor shall also inform him of his rights of appeal.

(2) Further information shall be provided in the communication relating to the oversight of the conduct of the operations agent only if notification to the person concerned is permitted under the conditions laid down by Article 24.1 of this Law, which authorises a person to be notified that an operational action was carried out in respect of him.

Point 7 of the transitional measures of the Law on operational activities

[9] Latvijas Vēstnesis (Official Journal), 30 December 1993, No 131. Available at: https://likumi.lv!doc.php?id= 57573.

'The amendments to Article 9(5) of this Law which provide for the acquisition of data which must be retained by the consent of the President of the District Court (of the city) shall enter into force on 1 January 2020'.

II. LEGAL ARGUMENTS CONCERNING THE QUESTIONS REFERRED BY THE UNITED KINGDOM COURT

11 In answer to the first question referred for a preliminary ruling by the UK Tribunal, the Republic of Latvia refers, first of all, to the provisions of Article 4(2) TEU, that the European Union is to respect the essential State functions. In particular, national security remains the sole responsibility of each Member State. Accordingly, it follows from the foregoing that it is for each Member State to adopt the measures necessary to safeguard national security and that the definition of national security does not fall within the competence of the European Union.

12 That argument is also supported by recital 11 in the preamble to Directive 2002/58 which states that that directive does not apply to issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law (now EU law), and by the provisions of Article 1(3) thereof, which provides that that directive does not apply to activities relating to State security.

13 At the same time, the Republic of Latvia points out that that conclusion also derives from the case-law of the Court of Justice. The first indent of Article 3(2) of Directive 95/46 [10] excludes from the scope of the directive the processing of personal data in the course of an activity which falls outside the scope of Community law (now EU law), such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security … [11]

14 The Republic of Latvia submits that, in the European Union, there is no one single conception of 'national security', and that each Member State defines that notion differently. However, regardless of that fact, there can be no doubt among Member States about the fact that activities directed against the independence of the State, its sovereignty, its territorial integrity, its constitutional order, the power of the State and the threats caused by espionage, terrorism, separatism and extremism, which threaten the territorial integrity of the State by anti-democratic means may be regarded as being a threat to national security.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995, L 281, p. 31).

[11] Judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/0 and C-318/04, EU:C:2006:346), paragraph 54.

15 The protection of national security falls within the responsibility of each Member State, which is why each Member State is entitled to establish specifically which characteristic circumstances and actions are perceived as threats to national security. Those are strongly influenced by the history of the State concerned, its geographical position, its geopolitical situation, its economic development and other factors.

16 For example, in the Republic of Latvia, 'national security' is understood as meaning 'State security', a situation which is achieved as the result of unified and targeted measures implemented by the State and by society, by which the independence of the State, constitutional order and territorial integrity, the possibility for society to develop without constraint, well-being and stability are guaranteed. Guaranteeing national security is the fundamental duty of the State [12].

17 In the Republic of Latvia, the identification and prevention of threats to national security are carried out by the national security services, namely the State institutions which, in order to carry out missions determined by the national security system, are responsible for espionage, counter-espionage and operational activities. In the Republic of Latvia, there are three national security services: the Office for Protection of the Constitution, the Security Police and the Espionage and Military Security Service [13] which act within the scope of their powers [14]. The Office for protection of the Constitution is in charge of espionage and counter-espionage. The Espionage and Military Security Service is responsible for military espionage and counter-espionage [15]; and the Security Police is the service responsible for counter-espionage and domestic security. [16]

18 The right of the national security services to acquire data to be retained for the purpose of national security from electronic communications operators is provided for by the Law on national security [17] and by the Law on operational activities [18]. The Prosecutor General and the prosecutors specially authorised oversee the procedures for operational activities of espionage and counter-espionage by the national security services. [19]

12 Article 1 of the Law on State security.

13 Article 11(1) of the Law on the national security authorities.

14 Article 1 of the Law on the Office for the Protection of the Constitution.

15 Article 14 of the Law on the national security services.

16 Article 15 of the Law on the national security services.

17 Article 19(1), point 8, of the Law on the national security services.

18 Article 9(5) of the Law on operational activities.

19 Article 26(1) of the Law on the national security services.

19 Operational data from electronic communications operators (data to be retained) is acquired by the national security services with the consent of the person responsible (head) of those services or the officer authorised by the latter and with the assent of a judge specially authorised by the President of the District Court (of the city) [20]. If the acquisition of data has a substantial impact on the right of person to privacy, the national security services must always obtain the agreement of the judge and, in every case, the Prosecutor General oversees the legality of the activities of the national security services.

20 Therefore, it follows from the foregoing that, in the framework of the legislation, the national security services not only have powers and rights, but also the obligation to respect the law and human rights. For example, if a person considers that, by their conduct, the national security services have infringed his legally prescribed rights and freedom, that person has the right to lodge a complaint with the prosecutor who, after an investigation, issues an opinion on the legality of the conduct of the national security services agent and may also bring legal proceedings [21].

21 The Republic of Latvia points out that, in the Explanations relating to the Charter of Fundamental Rights [22], it is stated that fundamental rights may be limited in order to attain objectives in the public interests. However, in relation to the foregoing, it must be observed that restrictions on fundamental rights cannot be disproportionate or constitute unjustified interference in the substance of those rights [23].

22 In the context of the present case, the Republic of Latvia notes that the acquisition of bulk communications data does not concern the acquisition of communications data to be retained concerning a particular individual, in the traditional sense, and which undermines an individual's right to privacy, but the acquisition of data on communication signals in a particular territory at a given moment.

23 The national security services use the information acquired for specific purposes, specifically to identify and prevent threats to national security. Therefore, the aim of acquiring data is to localise and identify the threat and not to confirm suspicions about one or more specific persons, as the law enforcement authorities do in the course of criminal proceedings.

24 As regards the second question referred, the Republic of Latvia takes the view that, in the light of its answer to the first question, there is no need to answer the

[20] Article 9(5) of the Law on operational activities.

[21] Article 4 of the Law on the national security services.

[22] Explanations relating to the Charter of Fundamental Rights (OJ 2007 C 303, p. 17). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF.

[23] Judgment of 13 April 2000, *Karlsson and Others* (C-292/97, EU:C:2000:202), paragraph 45.

second. However, the Republic of Latvia points out that, in the *Watson* judgment [24], the Court's findings related to the investigation of serious crime and not the prevention of a threat to national security, which is why the findings in that judgment cannot be applied directly to the powers of the national security services to accomplish their task and safeguard national security.

25 The submissions set out above are without prejudice to the obligation of Member States to observe the right to privacy of persons guaranteed by the Charter and by the European Convention on the protection of human rights.

26 In accordance with the case-law of the European Court of Human Rights, the Member States have broad discretion in order to safeguard national security, which also includes means such as the acquisition and processing which follows of the bulk communications data and the fact that such actions constitute an interference in the rights of persons to the right to privacy and the confidentiality of communications.

27 In *Klass and Others* v *Germany* [25], the European Court of Human Rights held that the secret interception of private telecommunications constituted, without any doubt, interference to the right to privacy and the confidentiality of correspondence. However, the European Court of Human Rights authorises those activities if they are strictly necessary for safeguarding democracy, if they are carried out in accordance with the law and have the specific legitimate objective of safeguarding national security or combatting terrorism, and if they are proportionate to the objective pursued. In the *Klass* judgment the European Court of Human Rights ruled that combatting terrorism and threats related to espionage may require the States to adopt various modern and complex technological solutions, in particular, the interception and surveillance of private communications. Nonetheless, the Convention does not confer unlimited powers on the States to interfere with the fundamental rights of persons, regardless of the importance of the aim of the interference and the States must provide effective procedural guarantees to exclude the arbitrary and ensure proportionality.

28 The European Court of Human Rights expanded on those findings in *Weber and Saravia* v *Germany*, stating that the supervision of so- called 'strategic monitoring of communications' is carried out both by a parliamentary commission and an independent committee which receive a monthly report on the measures taken and which have the right to annul decisions which have approved the specific measures for the strategic monitoring of communications.

29 It is also important to note that it is specifically the lack of effective procedural guarantees, in particular, the lack of an independent oversight mechanism, was the reason for which the European Court of Human Rights held that the provisions of

[24] Judgment 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15

[25] Judgment of 6 September 1978, *Klass and Others* v *Germany* (Application No 5029/71).

the ECHR had been breached in *Szabó and Vissy* v *Hungary* [26]. The European Court of Human Rights stated that the modern technology available to the Hungarian authorities had enabled the interception of bulk communications data concerning an unlimited number of persons, including persons outside Hungarian territory. Those measures had been approved within the strict framework of executive power and the applicable legislation did not provide for *ex ante* and *ex post* control mechanisms independent of the institutions.

30 Therefore, taking account of the foregoing, the Republic of Latvia considers that the obligation deriving from the Convention on Member States to respect the human rights of individuals do not preclude interference by the State with the right to privacy and secrecy of correspondence, including the interception of bulk communications data, if such interception takes place in a regulatory framework with the objective of safeguarding national security.

III. ANSWERS TO THE QUESTIONS POSED BY THE UK TRIBUNAL

In the light of the foregoing considerations, the Republic of Latvia suggests that the Court should give the following answer to the UK Tribunal as follows:

(1) Having regard to Article 4(2) TEU and Article 1(3) of Directive 2002/58/EC, measures such as those examined in the case in the main proceedings and the requirement in the instructions given by the Secretary of State to an electronic communications network operator to supply bulk communications data to the security and intelligence services of a Member State do not fall within the scope of EU law and Directive 2002/58/EC, because they do not fall within the scope of the European Union.

(2) Having regard to the answer to the first question, there is no need to answer the second.

Riga, 15 February 2018

[26] Judgment of 29 June 2006, *Weber and Saravia* v *Germany* (Application No 54934/00).