PRIVACY INTERNATIONAL

Human Rights Committee 116th Session

The Right to Privacy in Estonia

Suggestions for right to privacy-related questions to be included in the list of issues prior to reporting on Estonia, Human Rights Committee, 116th Session

March 2016

Introduction to the right to privacy in Estonia and main concerns

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour or reputation. Any interference with the right to privacy can only be justified if it is in accordance with the law, has a legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human right.[1]

The right to privacy is enshrined in the Estonian Constitution as follows:

> **"Everyone has the right to the inviolability of private and family life. State agencies, local governments and their officials shall not interfere with the private or family life of any person, except in the cases and pursuant to procedure provided by law to protect health, morals, public order or the rights and freedoms of others to combat a criminal offence or to apprehend a criminal offender."**[2]

Further, Article 43 of the Constitution of Estonia provides for:

> **"Everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means. Exceptions may be made by court authorisation to combat a criminal offence, or to ascertain the truth in a criminal procedure, in the cases and pursuant to procedure provided by law."**

The Estonian Penal Code establishes a series of offences to protect the right to privacy, including violation of confidentiality of messages (Article 156), illegal disclosure of sensitive personal data and illegal use of another person's identity (Article 157).[3]

Despite these provisions, Privacy International has on-going concerns on the protection of right to privacy in Estonia. The blanket retention of metadata retention provided under the Electronic Communications Act (2005) fails to comply with the test of necessity and proportionality, and therefore violates the right to privacy and personal data protection. Further, Privacy International is concerned that there is no effective oversight of information sharing with foreign government and agencies.

Metadata retention under the Electronic Communications Act (2005)

Estonia enacted the Electronic Communications Act[4] in 2005 and replaced the

1 Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also Report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014. See also International Principles on the Application of Human Rights to Communications Surveillance, available at https://necessaryandproportionate.org.

2 Article 26 of the Estonian Constitution. Full text of the Estonian Constitution is available at http://www.legaltext.ee/en/andmebaas/tekst.asp?loc=text&dok=X0000K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=constitution

3 Full text of the Criminal Code is available at http://www.legislationline.org/documents/section/criminal-codes/country/33.

4 See for the text of the Electronic Communications Act (2005) here at https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/511042014005/consolide.

Telecommunications Act (1996). The Electronic Communications Act was later amended in order to fulfil Estonia's obligation to transpose the Data Retention Directive (2006/24/EC) which obliged the telecommunication companies to retain the communication related data of all subscribers and users for up to two years or more to be used for law enforcement purposes.[5]

The amended Article 111 of the Electronic Communications Act (2005) required internet and telecommunication service providers to retain for one year a wide range of communication data (metadata) for the purposes of identifying, inter alia, the source, destination, time, duration and location of the communication. This article specifies the types of data to be retained by telephone (including mobile telephone) network services and internet service providers. Further, this provision allows the government to extend the time limit of retention of such data for a potentially unlimited time if the government deems it necessary in the interest of public order or national security.

The provision imposes a blanket obligation to retain communications data, without any requirement of authorisation, notice, etc. or any limitations as for the grounds such data must be retained. As such this provision goes even beyond what was required under the EU Data Retention Directive (2006/24/EC) that was invalidated.

In April 2014 by the Court of Justice of the European Union (CJEU) for being in contravention to the right to privacy and personal data protection as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights.[6] Despite this judgement, there has been no changes in the provisions of data retention in Estonia.

Article 112 requires relevant companies to provide the communication data retained under Article 111 within 10 hours for urgent requests and 10 days for other requests from the relevant agencies identified in the Act.[7] Mobile telephone services are also required to provide real time identification of the location of the mobile used.[8] Requests by the agencies may be in writing or even orally. Significantly, the provision does not require prior judicial authorisation, except when Article 901 of the Criminal Procedure Code applies.[9]

The interception, collection and use of metadata interfere with the right to privacy, as it has been recognized by human rights experts, including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.[10] The CJEU noted in its decision on the invalidity of Data Retention

5 Data Retention Directive 2006/24/EC.

6 Joined Cases C 293/12 and C 594/12 Digital Rights Ireland v. The Minister for Communications, Marine and Natural Resources and Others [2013] CJEU, para. 71.

7 Article 1111 [Obligation to preserve]:"(11) The data specified in subsections (2) and (3) of this section are forwarded to 1) an investigative body, a surveillance agency, the Prosecutor's Office or a court pursuant to the Code of Criminal Procedure;2) a security authority;3) the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Security Police Board and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure;4) the Financial Supervision Authority pursuant to the Securities Market Act;5) a court pursuant to the Code of Civil Procedure and 6) a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act and the Aliens Act".

8 Article 112(3) of the Electronic Communications Act.

9 Article 901 of the Criminal Procedure Code; available at https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042015002/consolide.

10 Report of the UN Special Rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014; Report of the UN High Commissioner for Human Rights, Right to privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

Directive that metadata may allow 'very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained' and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[11]

The blanket retention of metadata provided for in Article 111 of the Electronic Communications Act is in breach of existing EU provisions protecting the right to privacy and data protection, such as the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC, as well as the EU Charter of Fundamental Rights.[12] Because of its untargeted and indiscriminate scope, the provision constitutes an unnecessary and disproportionate interference with the right to privacy in violation of Article 17 of the International Covenant on Civil and Political Rights.

Interception of communications

Article 113 of the Electronic Communications Act regulates the conditions for access to the communication network by intelligence agencies and other bodies for the purpose of interception of communications. The Article requires service providers to grant access to their communication network in order for the agencies to conduct surveillance activities. Access to the network shall enable the surveillance agencies to select messages and to transmit them to the agencies devices in an unchanged form and in real time. Such transfer should ensure the preservation of independent log files concerning the actions performed by the central surveillance device (time, type, object and number of action) for a period of at least five years.

The Electronic Communications Act (2015) does not explicitly require that these surveillance activities are authorised by a court or other judicial body. For criminal investigations, Article 1267 of the Criminal Procedure Code provides that a preliminary investigation judge grants permission for "wire-tapping" for up to two months (renewable).[13]

Surveillance for intelligence and counter-intelligence is regulated by the Security Authorities Act.[14] Estonian Internal Security Service and Information Board are defined as 'security authorities' under this Act and are empowered to carry out acts that restrict the right to confidentiality of messages and to inviolability of home, family and private life as guaranteed under the Constitution (mentioned above). Those acts can only be carried out within the competence of those security authorities to ensure national security and constitutional order. Article 25 to 27 provide the conditions for those restrictive acts. Should a security authority needs to restrict the right to confidentiality of messages such as by way of 'wire-tapping', authorisation to do so must be given by an administrative court without holding a court sessions.[15] Permission may be granted for a period of up to two months for the same period at a time. However, the restriction on the right to inviolability of home, family and private life by

11 Digital Rights Ireland CJEU (n 6) para. 27 and 34.
12 Article 7 and 8 of the EU Charter of Fundamental Rights.
13 Article 1267 of the Criminal Procedure Code, available at https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042015002/consolide.
14 Security Authorities Act available at https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/507042015002/consolide.
15 Article 27(1) and (2) of the Security Authorities Act.

collecting personal, traffic or location data as well as entering or searching one's computer without one's consent do not require a judicial authorisation, but rather an order by the head of a security authority or an official authorised by him or her. This order may be given for a period of up to two months.[16] In any case, the person whose right to confidentiality of messages or private life are restricted has the right to be notified of the measures causing the restrictions.[17]

Parliamentary oversight of surveillance agencies

The Estonian Parliament Security Authorities Surveillance Select Committee is the Parliamentary body mandated to oversee the practices of surveillance agencies and security agencies.[18] Its report released in 2013 noted over 7,400 cases of requests for information based on court orders in 2012, an increase of 9 percent from the previous year. Concern was expressed in the media by the chairperson of the Committee that only three applications for surveillance were rejected by the court.[19]

According to a comparative survey on the parliamentary oversight of intelligence agencies in the EU[20], the Estonian Security Authorities Surveillance Select Committee lacks oversight powers related to the sharing of information with foreign entities and information sharing and cooperation agreements signed with foreign governments and agencies.

The intelligence agencies' sharing of information with foreign entities clearly needs to be carefully regulated and overseen.[21]

This lack of oversight is of particular concern taking the revelations on the existence of US mass surveillance programmes into account. According to Privacy International's knowledge no preliminary investigations or court proceedings have been initiated on the allegations of US NSA's surveillance on Estonians.[22]

Recommendations

Based on the above observations, Privacy International proposes the following questions for the List of Issues prior to reporting:

- What measures is Estonia taking to review its legislation on data retention to ensure its compliance with the right to privacy and protection of personal data in line with international human rights standards?

16 Article 27(3) of the Security Authorities Act.
17 Article 29 of the Security Authorities Act.
18 Article 36 of the Security Authority Act.
19 'Number of Covert Surveillance Warrants rises by 9%', news.err.ee, (19 February 2013), available at http://news.err.ee/v/society/5b832d0d-f75b-4aae-b3e2-9eaae1ff286a.
20 European Parliament, 'Parliamentary oversight of security an intelligence agencies in the European Union', (Brussels 2011), p. 115, available at http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf.
21 Report of the Special Rapporteur on the promotion of human rights and fundamental freedoms while countering terrorism, UN doc. A/HRC/10/3, 4 February 2009.
22 'PRISM Scandal: The Question That Ansip Should Answer', news.err.ee, (17 June 2013), available at http://news.err.ee/v/2f9e698a-d50d-4784-a639-7a4f8141ce2e.

- What measures is Estonia planning to strengthen effective oversight over the surveillance practices of its state security and intelligence agencies and to investigate allegations of mass surveillance of Estonians by foreign intelligence agencies?