PRIVACY INTERNATIONAL

The Right to Privacy in Estonia

Stakeholder Report
Universal Periodic Review
24th Session - Estonia

Submitted by Privacy International
June 2015

Introduction

1. This stakeholder report is a submission by Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. PI wishes to bring concerns about the protection and promotion of the right to privacy in Estonia before the Human Rights Council for consideration in Estonia's upcoming review.

The right to privacy

2. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from arbitrary State intervention and from excessive unsolicited intervention by other uninvited individuals. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2]

3. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[3] A number of international instruments enshrine data protection principles,[4] and many domestic legislatures have incorporated such principles into national law.[5]

4. In its resolution on the right to privacy in the digital age, adopted by consensus on 18 December 2014, the UN General Assembly called on all states to review their laws and policies regarding surveillance of communications with the view to uphold the right to privacy. The UPR review offers a significant opportunity for states to demonstrate that they are implementing this recommendation, by systematically reviewing states' compliance with their obligations to respect and protect the right to privacy.

---

1 Universal Declaration of Human Rights (Article 12), International Covenant on Civil and Political Rights (Article 17); regional treaties and standards including the African Charter on the Rights and Welfare of the Child (Article 10), the American Convention on Human Rights (Article 11), the African Union Principles on Freedom of Expression (Article 4), the American Declaration of the Rights and Duties of Man (Article 5), the Arab Charter on Human Rights (Article 21), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8).

2 See 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.

3 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).

4 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

5 As of December 2014, over 100 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (December 8, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

Follow up to the previous UPR

5. There was no mention of the right to privacy and data protection either in the National Report submitted by Estonia in 2010 or in the report of the Working Group following the consideration of the state report in 2011.

Domestic laws related to privacy

6. The Estonian Constitution guarantees the protection and respect of the rights to privacy.[6] Article 26 states that:

   "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."

7. 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.)[7]

8. Estonian current Personal Data Protection Act entered into force in 2008.

9. The 2005 Electronic Communications Act[8] requires internet and telecommunication companies to maintain the confidentiality of all information concerning subscribers and other persons who use communications services (see Article 102 on general principles of data protection.)

International obligations

10. Estonia has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR provides that *"no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation"*. The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "*adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."*[9]

11. Estonia ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108). As a member of the European Union, Estonia is also bound by the Charter of Fundamental Right of the European Union[10], and relevant EU norms on the protection of the right to privacy and personal

---

6 Available at: http://www.legaltext.ee/en/andmebaas/tekst.asp?loc=text&dok=X0000K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=constitution

7 Available at: http://www.legislationline.org/documents/section/criminal-codes/country/33

8 Available at: http://www.legaltext.ee/text/en/X90001K2.htm

9 Human Rights Committee, General Comment No. 16 (1988), para. 1

10 See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

data, including the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC.

Areas of concern

Data retention

12. According to Article 111 of the Electronic Communications Act (2005) relevant companies are required 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. The Article specifies the type of data to be retained by telephone (including mobile telephone) network services and internet service providers.[11] Further, the Article allows for extending the time limit of retention of such data for a potentially unlimited time the government deems it necessary in the interest of public order or national security.

13. Privacy International notes that since the EU Data Retention directive was declared invalid by the Court of Justice of the European Union (CJEU) in April 2014[12], there has been no changes in the provisions of data retention in Estonia.

14. 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.[13] The CJEU noted 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.[14]

15. The blanket retention of metadata provided for in the Electronic Communications Act is in breach of existing EU provisions protecting the right to privacy, such as the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC. Because of its untargeted and indiscriminate scope, the Act also fails to comply with the test of necessity and proportionality.

Surveillance of electronic communications

16. The Electronic Communications Act (2005) sets the conditions under which service providers shall provide communication data to security, surveillance

---

11 See text here: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/511042014005/consolide

12 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

13 See 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, and 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.

14 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

and other Estonian government agencies (Article 112) and to grant them access to their communications networks (Article 113.)

17. Article 112 requires relevant companies to provide the communication data retained within 10 hours for urgent requests and 10 days for other requests from the relevant agencies identified in the Act. Mobile telephone services are also required to provide real time identification of the location of the mobile used.

18. Requests by the agencies may be in writing or even orally. Significantly, the provision does not require prior judicial authorisation, except for criminal investigation, where the Criminal Procedure Code applies (see below.)

19. Article 113 regulates the conditions for access to the communication network by intelligence agencies and other bodies. The Article requires companies to grant access to the 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.

20. The law does not explicitly require that the request of personal data is authorised by a court or other judicial body. For criminal investigations, the Code of Criminal Procedure requires that surveillance of electronic communications are conducted only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings. Authorisation is given by the Prosecutor during the investigation stage and by a court if the proceedings have already reached the trial stage. While the authorisation shall set the period of time about which the requesting of data is permitted, there is no explicit maximum time limit.[15] According to the Estonian Human Rights Centre, a bill was under discussion in 2014 (the draft act 295 SE) amending the Code of Criminal Procedure, and significantly limiting the prosecution's options for surveillance activity, prescribing that surveillance is only justified on the permission of the court and for crimes in the first degree. Furthermore, the information that has been gathered by disproportionately breaching the person's fundamental rights, or by applying surveillance activities in the situation where more lenient measures would have sufficed, cannot be brought as evidence in criminal proceedings.[16] Privacy International could not confirm if this bill has been adopted.

21. However, surveillance carried out outside the criminal investigation do not require prior judicial authorisation. The Surveillance Act (amended in 2004), which regulates the activities of surveillance agencies, does not require a court order to authorise surveillance. Instead, surveillance proceeding shall be commenced following a decision made by the head of a surveillance agency or an authorised official, upon request from a range of investigative actors, including surveillance agencies, the public prosecutor, Interpol, etc.

---

15 See Article 90 of the Criminal Procedure Code, available here: http://www.legislationline.org/topics/country/33/topic/3

16 See report of the Estonian Human Rights Centre, available here: http://humanrights.ee/en/annual-human-rights-report/human-rights-in-estonia-2013/right-to-respect-for-family-and-private-life/

Parliamentary oversight of surveillance agencies

22. The Estonian Parliament Security Authorities Surveillance Select Committee is the Parliamentary body mandated to oversee the practices of surveillance agencies and security agencies.[17] 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.[18]

23. According to a comparative survey[19] on the parliamentary oversight of intelligence agencies in the EU, 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.

24. The Intelligence agencies' sharing of information with foreign entities clearly needs to be carefully regulated and overseen.[20] However, the Security Authorities Surveillance Select Committee has no legal mandate to scrutinise information sharing with foreign entities.

25. This lack of oversight is of particular concern: the question about whether and to what extent the Estonian security services have been connected to the U.S. mass surveillance programmes not been adequately addressed, despite allegations of NSA's surveillance on Estonians.[21] According to Privacy International's knowledge no preliminary investigations or court proceedings have been initiated despite concerns about personal communications of Estonians being subjected to mass surveillance programs. In this regard, the annual report of the Estonian Human Rights Centre noted how the Chairperson of Security Authorities Surveillance Select Committee assertion that no illegal surveillance has been detected was met with scepticism.[22]

Data protection

26. The Estonian Information System Authority's, the body mandated to develop information security and address security incidents on the Estonian computer networks, annual report 2014 revealed that cyber-security incidents in Estonia, e.g. malware, phishing, "have become more dangerous in nature, affecting organizations and users alike."[23] The Internal Security Service report expressed concerns "that the existing security policy of numerous institutions is unacceptably weak"[24].

---

17 Section 36, Security Authorities Act.
18 See http://news.err.ee/v/society/5b832d0d-f75b-4aae-b3e2-9eaae1ff286a
19 See Wills & Vermeulen (2011), Parliamentary oversight of security agencies in the European Union. European Parliament, p. 115: http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf
20 See Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc. A/HRC/10/3, 4 February 2009.
21 See http://news.err.ee/v/2f9e698a-d50d-4784-a639-7a4f8141ce2e
22 See http://humanrights.ee/en/annual-human-rights-report/human-rights-in-estonia-2013/right-to-respect-for-family-and-private-life/
23 See http://news.err.ee/v/1c0f2c7b-8f3d-49cf-9cf3-c04b4f0a4171. Full 2014 annual report available at: https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf
24 See Annual Report 2014, p.19, available at: https://www.kapo.ee/cms-data/_text/138/124/files/kapo-aastaraamat-2014-en.pdf

27. This raises concerns for the protection of privacy, particularly as "e-infrastructures" such as the ID-card, e-Health, and e-Voting systems collect and process a high amount of sensitive personal data in Estonia.[25]

28. On this regard, a security evaluation of the Estonian E-Voting system - based on election observation, code review, and laboratory testing – showed that the architecture has alarming gaps and that it is open to cyber-attacks. Considering that the threats of such attacks have shifted significantly since the Estonian system was designed in 2005, the study recommends to improve or discontinue the system.[26]

Recommendations

29. Privacy International that the government of Estonia:

- Undertake a review of the communications surveillance laws, policies and practices with the view to uphold the right to privacy in line with international human rights standards as enshrined in the International Principles for the Application of Human Rights to Communications Surveillance;[27]
- Require prior judicial authorization for any communication surveillance interfering with the right to privacy;
- Amend laws that regulate surveillance to bring them into line with international human rights standards to protect the right to privacy, including by repealing the requirement for mandatory data retention;
- Strictly regulate in law intelligence sharing, in ways that respect the right to privacy and review the mandate of the Parliamentary Security Authority Select Committee to ensure it can effectively monitor collaboration and information sharing with foreign intelligence services;
- Review the data retention framework in order to ensure its compliance with the European and international standards
- Review and strengthen the protection of personal data collected by the government and introduce effective data security measures to systems such

[25] According to the Freedom on the Net 2014 report (Freedom House) Estonia is among the most wired and technologically advanced countries in the world, with widespread e-commerce, and e-government services.

[26] See https://estoniaevoting.org/findings/summary/

[27] Available here: https://en.necessaryandproportionate.org/text