PRIVACY INTERNATIONAL

Stakeholder Report Universal Periodic Review
25th Session – Hungary

The Right to Privacy in Hungary

Submitted by Hungarian Civil Liberties Union and Privacy International

September 2015

I. Introduction

1. This stakeholder report is a submission by the Hungarian Civil Liberties Union (HCLU) and Privacy International (PI). HCLU is a human rights organisation that takes stand against undue interference and misuse of power by those in positions of authority. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

2. HCLU and PI wish to bring concerns about the protection and promotion of the right to privacy in Hungary before the Human Rights Council for consideration in Hungary's upcoming review.

The right to privacy

3. 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.

4. 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]

5. 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]

Follow up to the previous UPR

6. In the first UPR review of Hungary, the issue of privacy was not directly addressed in the state report, the UN report or other stakeholders reports. No recommendations pertaining to the right to privacy were made, although a number of recommendations related to freedom of expression were raised.

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

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 2013, 101 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

Domestic laws related to privacy

7. Article 6 of the Hungarian Fundamental law recognizes the right to privacy (paragraph 1.) and the right to protection of personal data (paragraph 2.). The means by which these fundamental rights are effected are laid down by Act CXII of 2011 on informational self-determination and freedom of information. Nonetheless, there are many sectoral laws affecting the rights to privacy and protection of personal data.

International obligations relating to privacy

8. Hungary ratified the International Covenant on Civil and Political Rights ('ICCPR'), which in Article 17 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".

9. Hungary is a member of the Council of Europe. It ratified the European Convention on Human Rights in 1992. Article 8 reads:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

10. Hungary also ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).

11. Hungary is bound to the Charter of Fundamental Rights of the European Union, Articles 7 and 8 of which relate to the right to privacy and the protection of personal data respectively.

II. Areas of concern

Inadequate authorisation of surveillance for the purpose of national security

12. There are two types of intelligence surveillance powers in Hungary: secret surveillance for the purposes of criminal investigation, and secret surveillance for the purposes of national security. There are differences between the two regarding the pre-conditions thereto, the relevant state agencies mandated to conduct such surveillance, the external authorization or warranty procedure, and the oversight and control mechanisms. The HCLU and PI's main concerns relate to surveillance for the purposes of national security, from which lack judicial authorisation and oversight are effectively absent

13. For the purpose of national security, Act 125 of 1995 on the National Security

Services[6] primarily allows the "National Security Services" to carry out secret surveillance. These are four agencies set up by the law with different duties: the Information Office, the Constitution Protection Office, the Military National Security Service and the Specialised National Security Service. According to Act XXXIV of 1994 on the Police,[7] the Counter Terrorism Centre, a separate part of the Hungarian police, is also allowed to use secret surveillance methods for criminal and non-criminal investigatory purposes.

14. The National Security Services and the Counter Terrorism Centre may request data from any public or private institutions or organisations, which are under a legal obligation to provide such information or allow the relevant agencies direct access to it. Further, according to the Act on National Security Services, the organisation or company disclosing data to the National Security Services and the Counter Terrorism Centre or allowing them to inspect data must not inform the person concerned or disclose any information (including aggregate data or statistics) in relation to such cooperation.

15. To facilitate surveillance, telephone or internet service providers have an obligation to store traffic data and make it available to national intelligence authorities (see further details in the section below.)

16. There is no requirement for prior judicial authorisation of surveillance for purposes of national security by the Counter Terrorism Centre and in some cases by National Security Services. Instead, the authorisation is provided by the Minister of Justice. This decision is not subject to appeal.

17. The Hungarian Constitutional Court did not find this lack of judicial authorisation contrary to the Hungarian Constitution and, following the Constitutional Court judgment, the case is now pending before the European Court of Human Rights.[8]

Computer Network Exploitation

18. Because of the secrecy surrounding state surveillance, the full range of digital surveillance techniques employed by the security services in Hungary are unknown. However, there are reports that sophisticated malware marketed by the Italian and German companies Hacking Team and Gamma International is currently or has previously been in use by security services in Hungary. In August 2014, it was revealed that the Hungarian secret service was on the list of clients of the Gamma International's Finfisher product. Freedom of Information requests by journalists to obtain the publication of some information on the deployment of these software were denied citing interests of national security. In July 2015, it was further revealed[9] that the Hungarian government bought[10] spyware from the Italian company Hacking Team.

6 Most recent English version available at: http://english.nmhh.hu/dokumentum/150102/125_1995_torv_eng_lekt_20070515.pdf
7 Available at: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99400034.TV
8 In a pending case against Hungary before the European Court of Human Rights the petitioners allege that the power to collect intelligence information upon citizens based on a simple ministerial authorisation but without a court warrant violates their rights under Article 8 of the European Convention on Human Rights. See case Szabó and Vissy v. Hungary, Application no. 37138/14, communicated on 12 June 2014.
9 Euronews, The buzz about the business of government surveillance – after the Hack Team hack, 8 July 2015. Available at: http://www.euronews.com/2015/07/08/the-buzz-about-the-business-of-government-surveillance-after-the-hacking-team/
10 Index, 7 July 2015. Magyarország 600 milliót fizetett a világ legostobább hekkereine. Available at: http://index.hu/tech/2015/07/07/600_milliot_fizettunk_a_vilag_legostobabb_hekkereinek/

19. These software programs can be used to hijack computer and mobile devices, whilst remaining undetectable to users, as they are designed to bypass common antivirus programmes and encryption. They can covertly collect, modify and/or extract data from the targeted device, including remotely turning on and control the microphone and camera of the device. As such they are a particularly intrusive form of electronic surveillance given the personal information that can be obtained from such access. There appears to be no explicit legislative authority in Hungary for the National Security Services to use such technologies.

Imposition of requirements to the communication and internet service providers

20. The Electronic Communications Act requires communications service providers to "cooperate with organizations authorized to perform intelligence information gathering and covert acquisition of data" and to "agree with the National Security Special Service about the conditions of the use of tools and methods for the covert acquisition of information and covert acquisition of data."[11]

21. Further, under the Government decree No. 180/2004 on the rules of cooperation between electronic communication, communications service providers must ensure, among other things, that all conditions necessary for the implementation of tools in relation to covert investigation operations are provided; e.g. a lockup room where the necessary equipment can be placed and non-stop technical assistance, if required.

22. Authorities can implement technical devices so that they have direct access to the networks of electronic communications service providers, without the personal assistance of the employees of the service providers.

Mandatory retention of metadata in violation of the right to privacy and data protection

23. In April 2014 the Court of Justice of the European Union (CJEU) declared invalid the Data Retention Directive on the retention of communication data by Internet and telephone service providers.[12] Despite the annulment of the EU directive, the Hungarian Act implementing data retention still remains in force.

24. The Hungarian Act on Electronic Communications establishes that service providers must retain telephone and Internet communications traffic data for six months. Communication traffic or "metadata" refers to the identity, location, the frequency of communications and other data of this kind of the individuals but not the contents of communications. However, such data allows for drawing accurate conclusions regarding the private lives, everyday habits, travel patterns and social environment of concerned persons, even without intercepting the contents of communications.

25. The interception, collection and use of metadata all 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

11 See Act C of 2003 on Electronic Communications, Article 92.
12 According to the decision, the directive had exceeded the limits of proportionality concerning the right to privacy and protection of personal data, as it failed to establish guarantees that counterweigh such limitations. 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 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.

26. Under the Hungarian law, everyone's communications data is retained irrespective of whether it relates to any serious crimes; the authorities can request communication data in bulks without having to provide any kind of justification; the concerned persons' right to being informed is not protected and they do not have the right to demand that their communication data is deleted.

27. As such, the data retention requirement under the Hungarian law does not meet the criteria of necessity and proportionality, and accordingly, the act allows for the unlawful interference with the right to privacy. Further, following the decision of the CJEU the blanket retention of metadata provided for in Hungarian law 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.

Ineffective oversight of surveillance powers

28. Parliamentary oversight of the National Security Services is conducted by the National Security Committee.[14] The chair of the National Security Committee is always a member of the parliamentary opposition

29. According to Article 14 of Act 125 of 1995 on the National Security Services, the Committee has powers to exercise parliamentary control through, inter alia, the following measures: requesting information from Ministers and from the general directors of the National Security Services, investigating complaints of unlawful activity by the National Security Services, and requesting that the minister carries out the investigation and informs the Committee of its results, if it presumes that the activity of a national security service is unlawful or improper.

30. Despite its relatively strong power, this parliamentary control is considered political and not easily accessible to average citizens. According to our information, these procedures have never been triggered. The HCLU is currently drafting a complaint under this legal framework to request the Committee to investigate the purchase and usage of malware designed for unlawful surveillance.

31. In theory, the activities of the National Security Services are not excluded from the application of the general data protection act (Act CXII of 2011 on informational self-determination and freedom of information.)[15] Therefore data protection remedies and redress mechanisms are applicable, including investigation by the National Data Protection and Freedom of Information Authority (DPA). However, the Act on National Security Services states that in the interest of national security or to protect the rights

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 For the Military National Security Service, the oversight is in co-operation with the Committee for Defence and Law Enforcement, although it is the National Security Committee that is responsible for the parliamentary control over the Military National Service's classified activities.

15 Available at: http://naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf

of others, the general director of the national security service may refuse the request to disclose data processed by the National Security Services or included in the data forwarding records; or to delete his/her personal data or to learn data of public interest managed by the National Security Services. There are serious concerns about the independence of the DPA following the circumstances of its establishment[16] and its activities.

32. The Commissioner for Fundamental Rights has also powers investigating complaints related to secret surveillance. Despite his powers, the Commissioner has never conducted any investigation on secret surveillance or other privacy matters since the establishment of the DPA. Instead, the Commissioner either refers the case to the DPA or quotes the DPA's legal opinion.

Lack of effective whistleblower protection in Hungary

33. This weak oversight over the secret surveillance of intelligence agencies is compounded by the lack of effective protection for whistleblowers and, more generally, significant restrictions on the lawful exercise of the right to freedom of expression in Hungary.

34. A new whistleblower act came into force on 1 January 2014 (Act CLXV of 2013 on complaints and whistle-blowers).A[17] However, the law fails to provide meaningful protection, as whistleblowing is defined not as the disclosure of information but reporting a problem to the responsible authority. Hence, whistleblowers seeking to publish information disclosing wrongdoings are not protected under the act and can even be prosecuted for a breach of confidentiality or charged with defamation.

35. Procedurally, the 2014 law introduced a new power to the Office of the Ombudsman, to which whistleblowers can report their complaints. However, the Ombudsman does not take the content of these reports into consideration but forwards them to the body that is entitled to investigate and remedy the alleged violation. It then reviews the conduct of such investigations.

36. While the act suggests that when a report is filed, the whistleblower is protected from any detrimental measure against them, it does not explicitly provide a defence for the disclosure of confidential information, nor from the opening of criminal proceedings against them.

Introduction of CCTV with facial recognition capability without adequate safeguards

37. During the 2014 national election campaign, the mayor of District 8 of Budapest (an area with high Roma population and high level of poverty) launched a HUF 250 million (approximately USD 1 million) worth project to set up 70 new CCTVs with facial recognition capabilities. It is claimed by the local government that the additional 70 cameras provide full coverage of the district. There is no law providing the legal basis for collection and processing of such data. Further, while the cameras are purchased by the local government, the responsible authority for data processing is one of the Hungarian

16 Hungarian Civil Liberties Union, The Hungarian data protection authority was conceived in sin, 10 April 2014. Available at: http://tasz.hu/node/4113

17 Available at: http://corruptionprevention.gov.hu/download/7/a2/90000/KIM%20555_2013-4.pdf

national security agencies (Special Service for National Security).[18] Consequently, every detail of the capabilities of the cameras and the data processing (including the time of retention, persons with access to the footage) is confidential.

38. The project included a "social consultation" campaign in which the local government sent letters to inhabitants of the district to ask for proposals about the location of the new cameras. However, the whole process remains shrouded in secrecy: although the purchase is covered by public money, every Freedom of Information request regarding the tender or the cameras has been denied by the local government on the basis that this information is confidential due to national security reasons.

39. Besides the obvious and very severe interference with the right to privacy and the right to data protection, the installation of these types of CCTV cameras in a neighbourhood with high Roma population may be discriminatory and facilitate the discriminatory practice of the Hungarian police against Roma people.[19]

18 See: http://www.nbsz.gov.hu/?mid=2&lang=en
19 Hungarian Civil Liberties Union, Hungarian City Openly Against Its Roma, 14 July 2015. Available at: http://tasz.hu/en/romaprogram/hungarian-city-openly-against-its-roma

III. Recommendations

HCLU and PI recommend that the government of Hungary:

1. Ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards and respect the right to privacy;

2. Ensure that all interception activities are only carried out on the basis of judicial authorisation and communications interception regime complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are intercepted;

3. Strengthen effective oversight over the surveillance practices of its state security and intelligence agencies;

4. Strengthen the protection of whistleblowers and to ensure they are not prosecuted for disclosing information exposing wrongdoings of public or private bodies;

5. Review the data retention law in order to ensure its compliance with the European and international standards;

6. Ensure that the deployment of CCTV cameras with facial recognition technology comply with the requirements of right to privacy and protection of personal data and do not result in discrimination against the Roma.