Suggestions for privacy-related questions to be included in the list of issues on Hungary, Human Rights Committee, 115th session, October-November 2015

7 August 2015

I. Introduction

Article 17 of the International Covenant on Civil and Political Rights 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. Interferences with the right to privacy can only be justified if they are in accordance with the law, have a legitimate objective and are conducted in a manner that is necessary and proportionate.

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.

This report focuses on Hungarian legislation and practices with regard to digital surveillance. The Hungarian Civil Liberties Union and Privacy International have on-going concerns about the practices of surveillance by Hungarian intelligence and law enforcement agencies.[1] National legislation governing surveillance is inadequate, leaving significant regulatory gaps and providing weak safeguards, oversight and remedies against unlawful interference with the right to privacy, including in relation to data retention provisions and the lack of judicial authorisation and oversight of the surveillance conducted for purposes of national security.

1 HCLU is a human rights watchdog NGO that takes stand against undue interference and misuse of power by those in positions of authority. Privacy International is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

II. Inadequate authorisation of surveillance for the purpose of national security

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 Hungarian Civil Liberties Union and Privacy International's main concerns relate to surveillance for the purposes of national security, from which lack judicial authorisation and oversight are effectively absent.

For the purpose of national security, Act 125 of 1995 on the National Security Services[2] 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,[3] 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.

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. Companies and private organisations may only lodge a complaint, without suspensory effect, to the competent Minister against the data inspection or disclosure order. 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.

Under the above mentioned legal regimes, forms of intelligence gathering include: searching residences in secret and recording observations with technical devices; observing and recording what is happening on the residence with the help of technical devices; opening letters and other postal items, inspecting their contents and recording them with technical devices; learning communication through a public telephone line or some other telecommunication service transmitting said communication and recording the relevant observations by technical devices;

2 http://english.nmhh.hu/dokumentum/150102/125_1995_torv_eng_lekt_20070515.pdf (English version, although the most current version is only available in Hungarian.)

3 http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99400034.TV (in Hungarian.)

learning, recording and using of data transferred or stored on IT devices or system. 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 on retention of metadata below.)

Unlike for the gathering of intelligence for criminal investigation purposes, 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.

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.[4]

The person subject to surveillance has no right to be informed about the decision, as the Minister of Justice must not inform the party concerned of his proceedings or of the fact of intelligence gathering.

Intelligence information gathering can be authorised for a maximum of 90 days per occasion. However, this deadline may be extended in justified cases by another 90 days. The law does not restrict the occasions of such extensions. Internal procedural and authorisation rules of intelligence information gathering are adopted by the relevant ministers these rules are not available to the public.

III. Imposition of requirements to the communication and internet service providers

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."[5]

Further, under the Government decree No. 180/2004 on the rules of cooperation between electronic communication service providers and authorities authorised for secret data collection electronic 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

4 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.

5 See Act C of 2003 on Electronic Communications, Article 92.

room where the necessary equipment can be placed and non-stop technical assistance, if required.

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.

Computer Network Exploitation

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[6] that the Hungarian government bought[7] spyware from the Italian company Hacking Team.

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.

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

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

6 http://www.euronews.com/2015/07/08/the-buzz-about-the-business-of-government-surveillance-after-the-hacking-team/

7 http://index.hu/tech/2015/07/07/600_milliot_fizettunk_a_vilag_legostobabb_hekkereinek/

and telephone service providers.[8] Despite the annulment of the EU directive, the Hungarian Act implementing data retention still remained in force.

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.

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 and the High Commissioner for Human Rights.[9] 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.

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.

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

8 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.

9 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.

Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC.

The Hungarian Civil Liberties Union started litigation in order to seek a judgment by the Hungarian Constitutional Court to repeal this provision. Regretfully, when finally seized with the issue (on request from the ordinary court before which the case was heard[10]), the Constitutional Court failed to rule on the merits of the case, arguing that the claim did not pertain the retention of communication data. While the proceedings in this case are not concluded (the case is now before the Hungarian Court of Appeal), the Constitutional Court judgment constitutes a significant obstacle for individuals and organisations to obtain effective remedy for the interference with their right to privacy. It also goes against trends in other EU member states, where courts have declared domestic data retention legislation as incompatible with the right to privacy and the right to personal data as provided for in the European legislation.[11]

V. Ineffective oversight of surveillance powers

Parliamentary oversight of the National Security Services is conducted by the National Security Committee.[12] The chair of the National Security Committee is always a member of the parliamentary opposition.

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.

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

10 Due to the reform of the jurisdiction of the Constitutional Court, HCLU could not directly refer the case to the Constitutional Court. Instead, it had to initiate a long process beginning litigation against Hungarian telephone and Internet service providers.

11 See, for example, the July 2015 judgment of the UK High Court declaring parts of the Data Retention and Investigatory Powers Act 2014 (DRIPA) in violation of the right to privacy and the protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights (https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf)

12 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.

drafting a complaint under this legal framework to request the Committee to investigate the purchase and usage of malware designed for unlawful surveillance.

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.)[13] 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 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[14] and its activities.

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

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.

A new whistleblower act came into force on 1 January 2014 (Act CLXV of 2013 on complaints and whistle-blowers).[15] 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.

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

13 http://naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf

14 http://tasz.hu/node/4113

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

forwards them to the body that is entitled to investigate and remedy the alleged violation. It then reviews the conduct of such investigations.

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.

VI. Introduction of CCTV with facial recognition capability without adequate safeguards against violations of the right to privacy and data protection

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 national security agencies (Special Service for National Security).[16] 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.

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.

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.[17]

16 http://www.nbsz.gov.hu/?mid=2&lang=en

17 http://tasz.hu/en/romaprogram/hungarian-city-openly-against-its-roma

VII. Proposed issues

Based on these observations, the Hungarian Civil Liberties Union and Privacy International propose the following questions to be addressed to Hungary:

Article 17:

- What measures is Hungary taking to ensure that its state security and intelligence agencies respect the right to privacy?
- In particular, how does Hungary 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?
- How does Hungarian authorities regulate the use of malware software (such as those reportedly provided by Gamma International and Hacking Team) as a tool for surveillance?
- Is Hungary planning to amend the Act on Electronic Communications to repeal the provisions that require blanket retention of communication data in violation of the right to privacy, data protection and EU legislation?
- What measures is Hungary planning to strengthen effective oversight over the surveillance practices of its state security and intelligence agencies?
- What measures are in place to 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?

Article 19:

- What measures is Hungary taking to strengthen the protection of whistleblowers and to ensure they are not prosecuted for disclosing information exposing wrongdoings of public or private bodies?