GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

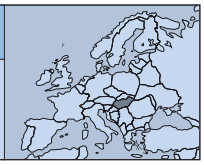
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

HUNGARY

Data retention and the use of spy software in Hungary



Éva Tormássy
tormassyeva@gmail.com

Introduction

After a series of coordinated suicide attacks in Madrid in 2004 and in central London in 2005, the European Union reacted by passing the so-called Data Retention Directive in 2006. Hungary as a member state of the European Union was obliged to introduce mandatory telecommunication data retention – that is, the retention of data generated or processed through the provision of publicly available electronic communications services or by public communications networks. As a result of the Data Retention Directive, all telecommunication service providers in Hungary have to collect and store so-called metadata, or data which shows who, when, where and with whom anyone tried to communicate or successfully communicated via email or phone. The Directive gave the freedom for the member states to choose the period of time their telecommunication service providers have to keep the data which, also according to the Directive, should be made available to the competent national authorities in specific cases when a suspicion of serious crime arises (e.g. an act of terrorism). According to the Directive, data made available for the purpose of the investigation, detection and prosecution of crimes should only be about the fact (who, where, when and with whom email was exchanged or communication took place by mobile phone), not the content. However, when the directive was implemented, Hungary failed to make the distinction between the fact and the content of the data. There is therefore a danger that the providers kept the content of the communication and the authorities received more information about certain citizens than they should have. The only good news for Hungarian citizens at the time of the implementation was that the decision makers chose the shortest possible period which was allowed, meaning the service providers have to keep the metadata for six months only in Hungary.

New times, old habits

Hungary was a member of the Soviet bloc before 1989, a so-called communist country where the surveillance of citizens by different authorities had a long history, even if this history was not as bloody as in certain other member states of the communist bloc. Most citizens had little personal experience of surveillance, and when the Berlin Wall collapsed in 1989 and the doors to the secret archives opened, many people must have been surprised how much the state knew about them and their private lives.

As a consequence of this, the newly adopted laws after the collapse of communism were very careful when it came to citizens' privacy and respecting the right to a private life. Before Hungary adopted the Data Retention Directive, the law on data retention was tied to judicial authorisation which was given in cases of suspicion of serious crimes. The police or any other authority had to submit a formal request for receiving the data from the service providers; however, with judicial authorisation they had the right to collect the data for three years.

The judicial authorisation was a strong safeguard which disappeared with the implementation of the Data Retention Directive. The implementation took place in 2008, under a socialist-liberal government, and the competent ministry which was responsible for the implementation chose the shortest possible period for data retention because the minister was delegated by the liberal party. But that was the last good news for Hungarian citizens.

The implementation forgot about the basic safeguards in the law. The text was not clear when it came to not storing the content of the data and did not mention the necessity of judicial authorisation, court oversight or any external supervisory mechanism. The law also forgot to prescribe the obligation to inform the person concerned about the use of his/her data, and to inform the person who was under surveillance, as well as the obligation to destroy the data after the end of legal proceedings. Lastly, there was nothing about who guards the guardians: who inspects or monitors the process of destroying the data when the retention time is over. Possibly the worst thing of all was that the authorities were granted direct access to the telecommunication

service providers' data rooms (a special technical connection has been set up between the companies and the national security authorities). And the security men sitting on the two sides of the table all knew each other from the past and understood each other. Hungary, which has never been able to get rid of its past of secret agents and spies, started its own time travel back into that past.

When Big Brother watches you

In his famous book 1984, George Orwell wrote that "Who controls the past controls the future." This quote – even if it was related to the communist era – expresses the basic societal concern about any state surveillance well. This recognition led many human rights activists to fight against the Data Retention Directive and its national implementation all over Europe. In Hungary, the Hungarian Civil Liberties Union (HCLU) protested against the implementation of the Directive in many ways – without significant result, effect or echo. They submitted amendments to the national law through members of parliament, published articles, and organised civic actions in which citizens asked the service providers to inform them whether they were under surveillance or not, but all attempts remained unsuccessful.

On the other hand, the conservative Hungarian government, which was first elected in 2010 and for a second time in April 2014, became more and more successful in controlling citizens. They knew well that those who control the past control the future. Hungary's parliament moved to increase surveillance of high-level public officials, with the modification of the National Security Law on 24 May 2013. It was designed to allow the state to identify any risks that could lead to someone influencing or blackmailing a person under surveillance, which would in turn cause state security issues, the law says. The range of positions in the secret service's focus is detailed: the people subject to such surveillance are ambassadors, state secretaries, heads of administrative bodies and councils, the management of parliament, the head of the military forces and army generals, police commanders and superintendents, and heads and board members of state-owned companies. The person in question needs to sign an approval for the surveillance to be allowed. Refusal to sign means they lose their jobs. The modification has raised concerns on the part of the ombudsman and civil rights groups, and sparked comments that the secret service's reach into people's private lives would now be "total". The bill also lifts the earlier requirement of a court nod for the secret gathering of information on people by opening their letters, making audio and video recordings or searching and bugging their homes.

Apart from allowing surveillance of a selected group of people without letting them seek legal remedy, the law provides no regulations that limit who can see the information, what can be done with it, or how long it can be stored. The law also allows for employees to be fired for conduct outside the workplace, for as yet unspecified reasons. It means that Hungary now allows investigation of particular individuals without any need to demonstrate a specific reason why every aspect of a person's life must be reviewed. That is unusual in democratic states. The new national security law has really created an Orwellian landscape in Hungary.

Hungary's ombudsman for basic rights, Mate Szabo, declared that the bill should give those under surveillance the right to appeal the matter and seek legal remedy against any encroachment of their rights in the process. But this remark was ignored in the final version of the law. The HCLU said that the new bill is unconstitutional even if the person in question signs a document to give their consent to the surveillance. The ombudsman is the only one who has the right to appeal to the Constitutional Court – civil rights groups do not. Last June, Szabo initiated a constitutional review. He raised concerns over a lack of external control over the monitoring process and the fact that agencies would not be required to provide a concrete reason or aim for the monitoring activity, which would give the state an unfair power advantage over the individual targeted in the surveillance. Despite the protests, the amendment was enforced on 1 August 2013. However, while the Constitutional Court decision made in March 2014 repealed the amendment, a new parliament set up in late May did not follow the court's decision, meaning that the amendment stood. The Constitutional Court declared in its decision that legislation allowing for secret observation on officials in positions requiring national security screening for 30-day periods twice a year is unconstitutional. According to the top court's ruling, permanent surveillance and secret information gathering would disproportionately restrict the target's privacy rights. The body also threw out stipulations that prevented targeted persons from seeking legal remedy, such as an appeal to a relevant parliamentary committee against the monitoring procedure.

The other story which shows the government's totalitarian attitude to the right to privacy is that in 2013 Hungary appeared on the list of those countries where the infamous governmental spy

software package called FinFisher is used, according to Citizen Lab. Citizen Lab is an interdisciplinary laboratory based at the University of Toronto (Canada), focusing on the intersection of information and communication technologies, human rights and global security. FinFisher's customers can only be governments and in using the software, Hungary joined a group of countries where oppressive regimes are in power. FinFisher is a very sophisticated software package which is able to create access to all data on the infected computer, including emails, document files, voice over internet protocol (VoIP) calls, etc. There were few reactions in Hungary when this news was published, but Átlátszó (Transparent),[1] a Hungarian NGO fighting for freedom of information, submitted a public information request to the Constitution Protection Office on 17 October 2013. It asked the Office to disclose the length of time and the number of times the government used spy software packages, and it asked it to list those that are in use. Within a week the Constitution Protection Office had sent a letter, and refused to respond to their questions, referring to national security interests. According to the website of the Office, "the aim of the Constitution Protection Office is to protect citizens and the constitutional order of Hungary, and to guarantee their security. (...) Its special duty is to provide Hungary with such information for decision making which is not obtainable from other sources."[2]

While all these unfortunate events happened in Hungary, the First European Constitutional Court suspended the Data Retention Directive after the decision of the Court of Justice of the EU (CJEU). The CJEU declared this April, among other objections, that the interference is not proportionate and that the Directive failed to apply those safeguards which were also missed in the Hungarian implementation and in other national legislation. However, the Hungarian authorities did not immediately react to the news (e.g. in neighbouring Slovakia the Constitutional Court preliminarily suspended the effectiveness of the Slovak implementation of the Data Retention Directive right after the decision of the CJEU).

Conclusions

The following conclusions can be drawn from this report:

- Data retention in general and by definition violates our right to privacy.
- It is necessary to apply certain safeguards: the need for judicial authorisation, court oversight, or any other external supervisory mechanism; authorities should not have direct access to data stored by service providers; there is an obligation to inform the person concerned about the use of his/her data; there is an obligation to inform the person who was under surveillance; there is an obligation to destroy the data after the end of investigative proceedings; and there is an obligation to delegate independent experts to inspect and monitor the process of destroying the data.
- Surveillance mechanisms which target innocent people by collecting information about them simply because they are in certain positions serving the state cannot be justified and should be taken as unconstitutional. One example of this is the amendment of the Hungarian National Security Law, which aims to surveil people who are completely innocent, simply to control them and their private lives. Such acts cannot be justified in a democracy.

Action steps

The following advocacy steps are taking place and recommended for Hungary:

- Citizens and human rights NGOs are planning to initiate a lawsuit against service providers in order to know what personal data is being retained by the providers.
- Following the recent decision by the CJEU, Hungary should revise its law on data retention.
- Hungary should get back onto the democratic road when it comes to surveillance and modify the National Security Law according to the Constitutional Court ruling.
- The use of spy software packages should be more transparent and regulated by law as well. The Constitution Protection Office should have an obligation to make such data publicly available for everybody.
- The need for transparency is obvious. The intersection between national security, surveillance, law enforcement, the role of private companies, citizens' private data and their right to privacy needs to be clear. Transparency reports prepared by companies involved in data retention can be one useful tool to know what is happening in this area. For example, Vodafone made an attempt to publish certain information on this in its worldwide report.

1 www.atlatszo.hu

2 ah.gov.hu/english