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

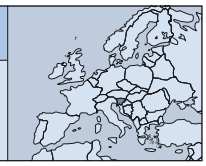
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

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

SLOVAK REPUBLIC

The quest for privacy in Slovakia: The case of data retention



European Information Society Institute (EISi)
Martin Husovec and Lubomir Lukic
www.eisionline.org

Introduction

Shortly after a series of coordinated suicide attacks in Madrid in 2004 and central London in 2005, the European Union reacted by passing the so-called Data Retention Directive in 2006. The directive obliged all EU member states to implement laws forcing telecommunications providers to monitor and store a wide range of metadata concerning the online and phone activities of their citizens for periods ranging from several months to years. The hope was that this data could help Europe to better fight terrorism and other serious crimes. Strong protests by citizens in some of the member states could not stop the scale of this imposed surveillance.

In September 2010, when the European Information Society Institute (EISi) was formed in the Slovak Republic (also known as Slovakia), the fight against surveillance in other member states had already been going on for several years. The German Constitutional Court in March of that year suspended Germany's implementation of the directive and many other national initiatives began appearing. Encouraged by the efforts and fruits of the labour of our colleagues, EISi decided to make litigation against data retention in Slovakia its first goal. There was, at the time, no civil society organisation to do the job in the country; there was virtually no public debate and very little, if any, public resistance against data retention.

Policy and political background

After the Data Retention Directive was implemented at the national level throughout the EU, the resulting legislation was subject to numerous challenges at the national level.[1] However, it took almost a decade to challenge the source of all of this: the directive itself. In April 2014, the Court of Justice of the EU (CJEU) – in its historical role as a constitutional court for the Union – repealed the entire Data Retention Directive[2] and also broadly quashed any future hopes for similarly far-reaching measures. This, however, did not exhaust the advocacy role for civil society groups. Today, there is a great need to sweep clean numerous post-directive consequences. In Slovakia, this entails the review of the Act on Electronic Communications and some other acts.

> This report outlines the struggle of launching a challenge against the implementation of the directive in Slovakia. It presents a picture of non-responsive local authorities, a lack of public awareness and little resistance to an invasion of privacy rights among Slovak civil society and ultimately citizens. It also illustrates a misuse of retained data and the real practice of disclosure, which is often distant from the letter of the law.

Challenging the implications of the Data Retention Directive at the local level

Soon after its launch, EISi authored a brief report pointing out the basic discrepancies between the Act on Electronic Communications ("the Act") and its data retention provisions, and the fundamental rights embodied in the Slovak constitution, the EU Charter of Fundamental Rights and Freedoms, and the Convention for the Protection of Human Rights and Fundamental Freedoms. This report was then presented in the form of a motion[3] to two local authorities, which were entitled to initiate proceedings before the Constitutional Court. These authorities were the General Prosecutor's Office and the Ombudsman.

Both of the local authorities, despite the evidence, reached the view that the data retention provisions do not lead to an interference with the fundamental rights and freedoms of citizens. And so they refused to initiate any proceedings before the Constitutional Court, which could review the constitutionality of the provisions of the Act.

When easier ways of initiating proceedings before the Constitutional Court were exhausted, EISi

1 Jones, C., & Hayes, B. (2013). *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*. secile.eu/data-retention-in-europe-case-study

2 Digital Rights Ireland C-293/12 and Kärntner Landesregierung C-594/12.

3 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/22-podanie-generalna-prokuratura

had to try more complicated and resource-intensive ways. We put together a submission for the Constitutional Court[4] and started asking for the support of members of parliament, who can also initiate such a constitutional review. The required number of signatures is relatively high – at least each fifth member of parliament needs to sign such a submission (a total of 30 MPs).

It probably does not need to be stressed too much that this requirement slowed down the process. Because EISi has no regular staff members, but only volunteers, it took a few years to both draft the submission and get the necessary support for it. And had the work on the submission not been supported by the research of one of its members, it could have taken even longer than that.

The ultimate aim of the submission, which was later presented to MPs, was to succinctly point out conflicts between the data retention provisions and fundamental rights and freedoms. The submission described the overall situation, the fundamental features of which are presented below.

According to the Act, an undertaking[5] is obliged to retain traffic data, location data and data of the parties who communicated. The data retention period was set to six months in the case of internet access, email and voice over internet protocol (VoIP), and 12 months in the case of other types of communications. The scope of the retained data is very broad. It can probably be best divided into the following categories: i) data necessary to trace and identify the source of a communication; ii) data needed to identify the recipient of communication or to identify the date, time and duration of communication and iii) data needed to identify the type of communication, the users' end equipment (or what seems to be their equipment) and the location of mobile devices.

In the opinion of EISi, the introduction of these obligations constituted a substantial encroachment upon the private life of individuals – especially because this mandated a blanket monitoring of all inhabitants of Slovakia, regardless of their innocence or prior behaviour. The data retention requirements mandated that every day the data about every inhabitant of Slovakia must be collected, amassing a profile of who called whom, to whom someone sent an SMS or email, when the person sent it, from which location, using what type of device or service, how long the communication took, and many other details. It is needless to say that the combination of this information made it possible to perfectly describe the movement of every inhabitant of Slovakia who uses a mobile phone or the internet. In this way, the behaviour, circle of acquaintances, hobbies, health, sexuality and other personal secrets of all the citizens can be predicted.

It therefore comes as no surprise that EISi considered the legislation to be entirely disproportionate and lacking any safeguards against the misuse of the sensitive data. The legislation created a regulatory free space which increasingly minimised citizens' privacy. Moreover, the main duties and details of data retention regulation were left to private companies, which are naturally more interested in minimising their costs, since the state did not reimburse them for the cost of this obligation.

The submission argued that in the light of the application of the proportionality test, the data retention legislation turns out to be clearly unconstitutional. It also argued that the retention of metadata can in a concrete way result in even more intrusive interference with the right to privacy than a scenario in which the content of the communication itself is retained.

Moreover, the legislation, in contrast with other legal requirements for criminal proceedings, did not exempt persons who are otherwise bound by professional secrecy (e.g. lawyers, doctors), or who cannot be surveilled or wiretapped when they perform certain activities (e.g. relationships between advocate and accused).

EISi argued that the national provisions on data retention were therefore in direct conflict with the principle that the restriction of fundamental rights and freedoms has to comply with their essence and meaning. The restrictions can only be implemented when there is a clear, stated aim. It is a violation of provisions if the state restricts fundamental rights and freedoms in a way that both lacks an achievable goal and, especially, threatens the very essence of those freedoms.

We furthermore believed that blanket data retention is unconstitutional for several reasons, and that the Data Retention Directive itself is invalid because of this. First of all, data retention is not a sufficiently effective tool to combat serious crime: it affects ordinary people more than the perpetrators of serious crimes. Therefore it disproportionately infringes on the right to privacy and the right to protection of personal data. It also disproportionately

4 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/28-vzorove-podanie-na-ustavny-sud-sr-vo-veci-plosneho-sledovania-obcanov

5 For the purposes of the Act on Electronic Communications, "undertaking" means every person who provides a network or service; undertaking activity means a network or a service provision in the electronic communications sector for a third party.

restricts freedom of expression and media freedom. Moreover, the length and extent of retained data was prescribed without the support of any empirical research.

EISi also argued that many provisions of both the Data Retention Directive and the Act are vague and provide too much room for abuse by both public authorities and the private sector. The real-life practice of Slovak service providers retaining and storing data was found to be entirely arbitrary, because often the data retention was not required by law and/or data was provided to authorities who have no legal right to request them. So both the scope of retention and scope of access often exceeded the law.

Access to stored data is not regulated by any precise legislation. This enables law enforcement authorities to take advantage of a messy legal situation and request data for less serious crimes. This is constitutionally incompatible with human rights such as the right to privacy and freedom of expression. EISi presented evidence which illustrated a real misuse of data when it comes to disclosures. It was established that the practice is often very distant from what the letter of the law says. This is especially the case given that there is very little supervision from the public authorities responsible for this.

The submission asked the Constitutional Court to file for a preliminary reference before the CJEU arguing that the Data Retention Directive itself is invalid.

After several months of negotiations with members of parliament, the required number of signatures was reached to support our initiative. Finally, after six months, EISi managed to get the submission before the Constitutional Court. At this point, however, it had already been three years since we had started the initiative.

In October 2012, the submission[6] demanding a review of the data retention provisions embodied in the Act was officially submitted to the Constitutional Court.[7] Shortly after the submission was filed, a preliminary submission concerning the constitutionality of the Data Protection Directive was filed before the CJEU. The referring Austrian and Irish courts made a reference similar to the one EISi proposed for the Slovak Constitutional Court in the proceedings before it. Due to the inactivity of the Slovak Constitutional Court, it soon became clear that the Court had decided to wait for the decision of the CJEU first. In April 2014, the CJEU annulled the Data Protection Directive.[8]

Conclusions

By repealing the Data Retention Directive, the CJEU not only invalidated a single act of the Union's secondary law, but also defined the scope of their discretion. Slovak transposing acts, which are at the moment under the scrutiny of the Slovak Constitutional Court, were thus not only deprived of the reason for transposition, but are now also in a direct contradiction with the explicit standard set by the CJEU in Digital Rights Ireland C-293/12 and C-594/12.

According to the decision of the CJEU, any kind of blanket data retention that does not distinguish between persons who can be connected to major criminal activity and other persons, does not conform with the rights to privacy and protection of personal data.

In terms of future legislation:

- Any kind of metadata retention must (i) be aimed at specific persons or circle of persons, and (ii) have a specific time period and/or (iii) geographical area.
- Access to data must be restricted to investigating acts of a serious nature that can justify the significant interference with fundamental human rights such as the respect of private and family life and protection of personal data.
- Access to data must be subject to judicial supervision or the supervision of an independent administrative body which can allow such access based only on a substantiated application to the courts.
- Data retention must reflect the special status of persons bound by a duty of confidentiality conferred by national law, such as attorneys or doctors.
- When grounds for data detention are not relevant anymore, the particular person must be notified of the fact that he/she was under surveillance in the past.
- The period and types of retained data in a specific case must be adapted to what is necessary for achieving a particular aim.
- The data retention must provide clear safeguards against possible misuse or unauthorised access to this data.

6 PL. ÚS 10/2014

7 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/49-slovak-case-on-data-retention

8 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/74-us-data-retention-suspension

- Legal regulations must clearly describe how the data can be stored and how the data will be destroyed after it is used.
- Any kind of access and subsequent use of metadata must fall within a clearly defined scope and be for a clearly defined aim.

On 23 April 2014, the Slovak Constitutional Court preliminarily suspended the national implementing Act. This measure means that the retention laws are still formally in place, but have no legal effect until the Court decides on the merits of the complaint. However, at the same time, data that has already been collected will not need to be destroyed, and it remains open to interpretation whether service providers may or may not hand over data collected in the past to state authorities upon request.

On the other hand, the Slovak Parliament came up with a proposal to amend the Penal Procedure Code, which is one of the acts regulating the access to this type of information. The proposal fails to live up to the standard set by the CJEU. Yet no civil society organisation, and very few in the mainstream media, picked up on the topic. This creates little pressure on legislators. It appears that even after the landmark decision of the CJEU and our efforts, sensitivity to privacy rights is still rather low in Slovakia. Even less significant copyright developments enjoy better coverage in the media and garner more public interest than most privacy-related issues.

Action steps

Slovakia still lacks a strong privacy advocacy group. EISi, as a think tank focusing more on litigation, is not well suited to fulfil this role. Our example shows that the presence of expertise and litigation coming from civil society does not necessarily improve social sensitiveness to the issues among the general public. Slovakia needs, in our view, the following:

- A strong privacy activist group needs to be established.
- The work of the Slovak Data Protection Authority needs to be improved. Currently, it is not only failing to act *ex officio*, but also in cases when data is requested by the authorities, and its work is marked by a lack of expertise.
- The opportunity for civil society to object to legislation before the Constitutional Court, even without political support, needs to be legislated in Slovakia. When the general public is not sensitive to certain issues, neither are the public authorities.

All this will be important after the decision by the Constitutional Court is made, when the debate will again be shifted to the national parliament. In the absence of broader interest by civil society, the strength of the pro-privacy opposition will remain very small and we will witness a race to the bottom.