Katarzyna Szymielewicz [Panoptykon Foundation]

DATA RETENTION IN POLAND: THE ISSUE AND THE FIGHT

This paper is aims to give a brief overview of the following issues: (I) Polish data retention regime and its drawbacks; (ii) the use of data retention in practice and available data on the subject; (iii) campaign run by the Panoptykon Foundation over last two years; and (iv) political shifts that occurred in Poland.

(1) THE LAW AND ITS DRAWBACKS

The very concept of data retention for law enforcement purposes existed in Poland before the Data Retention Directive[1] was adopted. The obligation to retain basic telecommunications data has been in force since 2003. We witnessed political attempts to introduce an even more pervasive data retention regime than proposed in the Directive (retention up to 5 years) but they failed. The Directive was transposed into the Polish legal system in 2009 through the changes in the telecommunications Law, the Code of Criminal Procedure and a number of legal acts defining the powers of relevant law enforcement agencies[2].

It is important to note that Poland not only opted for the most privacy-intrusive solutions when implementing the Directive but also allowed for an over-implementation of the Directive in some respects, in particular with regard to the purpose of data retention. According to the Data Retention Directive itself, the EU-wide blanket retention regime was introduced in order to increase data availability for the purposes of investigating and prosecuting serious crimes (as defined by the national law). Since there is no common definition of “serious crime” the Directive left the Member States with considerable field of manoeuvre. Poland, however, decided to go even further and allow for the use of data retention by all law enforcement agencies in performing their statutory duties.

---

1 Directve 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retenton of data generated or processed in connecton with the provision of publicly available electronic communicatons services or of public communicatons networks and amending Directve 2002/58/EC.

2 Main sources: Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Law of 24 April 2009 amending the telecommunications Law, Journal of Laws of 2009, No 85 item 716); Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Regulaton of the Minister of Infrastructure of 28 December 2009 on a detailed specifcaton of data and types of operators of public telecommunicatons networks or providers of publicly available telecommunicatons services obliged for its retenton and storage, Journal of Laws of 2009, No 226 item 1828); Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz. U. 1997, Nr 89, poz. 555 ze zm.(Law of 6 June 1997 – The Code of Criminal Procedure, Journal of Laws of 1997, No. 89, item 555 with amendments).

Polish law does not specify kind of crimes that shall justify the use of traffic data for prosecution, nor is the access to such data conditioned by the gravity of charges. As a result, data retention is frequently used by the police in all sorts of cases, including those as minor as enforcement of child support obligations between divorced couples. What is more, telecommunications data of each and every citizen can be used for general crime prevention purposes[3]. The use of data retention for crime prevention clearly contradicts the goals set by the Directive. During the debate at the European level this particular purpose was taken into consideration but was also rejected due to its broadness and high risk of abuses.

The police and secret services are empowered to access billing and location data once retained without any control (e.g. judicial control, prosecutor's oversight or *ex post* control exercised by the citizens themselves)[4]. Law enforcement agencies have no obligation to inform the person in question that operational measures had ever been applied once the proceedings are completed. The law also creates a dangerous grey zone when it comes to practical aspects of accessing data retained by the operators. The draft law containing the technical specification of the interface used by the law enforcement agencies in order to access the data is yet to be adopted. Existing legal provisions are vague and all they require from telecommunications operators is that they be in cooperation with law enforcement agencies.

As far as the range of entities entitled to use data retention is concerned, Poland decided to include not only courts, prosecutors and the police but in fact all agencies dealing with investigation or intelligence, namely: Border Guard, Internal Security Agency, Military Intelligence Service, Military Counter-Intelligence Service, Military Gendarmerie, Central Anti-Corruption Bureau and Treasury Intelligence.

As far as data retention period is concerned, Poland opted for the maximum: we are the only EU Member State, where all types of telecommunications data are retained for 2 years. There is no reimbursement mechanism and all costs generated by data retention regime are covered by the operators themselves. As it was mentioned above, the law

3 Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. 2002, Nr 7, poz.58 ze zm. (Law of 6 April 1990 on the Police, Journal of Laws of 2002, No. 7, item 58 with amendments), in English at http://www.policja.pl/portal/pol/90/4889/Polish_Natonal_Police.html, compare art. 20.

4 Competences permitting the use of retention data are contained in the specific laws regarding particular services. For example, Art. 18.1 of the Law on Central Anticorruption Bureau states that: 1.The obligation to obtain a Court warrant does not concern information necessary to fulfill tasks of the CAB prescribed by law that consist of data regulated by Art. 180c and180 d of the Telecommunications Law; 2. The telecommunications operator is obliged to make the retention data accessible to the CAB with no charges: 1) on a written motion from the Head of the CAB or a person authorised by them; 2) on oral request of the CAB agent, possessing a written authorisation issued by the Head of the CAB or a person authorised by them; 3) through the telecommunications net to the CAB agent, possessing a written authorisation issued by the above mentioned persons.

does not provide for any external control mechanisms with regard to law enforcement agencies and their access to data. The only tool that can be used in order to control the way the whole regime operates is a reporting obligation imposed on the operators[5]. Every year (by the end of February) they are obliged to report to the Office for Electronic Communications ("OEC") the total number of requests received from law enforcement agencies, including the amount of requests that were refused and the age of data requested.

Summing up, the way in which the Data Retention Directive was implemented in Poland proves that it failed to set firm limits with regard to the purposes of data retention and its control mechanisms. On the other hand, it is clear that the Polish government used the European law as an excuse to introduce the regime it wanted anyway. In this context it seems worthwhile to look at the very process of implementing the Directive and the official justification as it was communicated to the society.

The Directive was transposed under the pressure of time without much public debate. This is, however, not an exceptional situation in the Polish legislative process. The deficiency of evidence-based policy making has been identified as a systemic problem in our country. Every legislative proposal needs to be backed with an impact assessment and an official justification stating its goals and the need to change the law accordingly. In practice, this duty is treated as a sheer formality: authors of the draft law hardly ever deliver a quality justification and impact assessment.

The quality of the official document backing the proposal to implement the Data Retention Directive is very low. Apparently, the government took the need to implement the new directive for granted and applied no additional scrutiny. The document contains only one concrete argument supposedly justifying the need to introduce data retention regime: because of its geographical location and military involvement in Afghanistan, Poland is likely to be used as a transfer point for trafficking heroine, especially by the soldiers themselves. This argument is based on the premise that not only Poland suffers from organised international crime in this specific area but also that this problem can be cured with data retention. Neither of these statements seems correct. Leaving the patterns of drug trafficking aside, the government didn't provide any data proving that it was necessary to keep the communication records of each and every citizen in order to fight international crime more effectively. Moreover, it wasn't explained why Poland opted for the longest possible data retention period and decided not to introduce any external control mechanisms with regard to the use of telecommunications data.

5 Compare article 180g (2) of the Polish Telecommunications Act (Polish Official Journal of 3 August 2004 [Dz.U.04.171.1800] with further amendments)

(2) PRACTICE

We know very little about the actual practices related to data retention and its use in Poland. This is due to systemic problems with the lack of democratic control over law enforcement agencies as well as the limitations of the existing data protection law, including its weak execution towards commercial entities. Allegedly, telecommunications data is stored for far longer periods than required by the law (currently 2 years) for both commercial and law enforcement purposes. The only reliable source of information about the use of data retention is the OEC.

As it was mentioned above, every year the OEC collects data about the amount of requests received by telecommunications operators from all entities entitled to use data retention for law enforcement purposes. On that basis the OEC prepares its report in accordance with Article 10 of the Data Retention Directive and communicates results to the European Commission. For the first time these statistics were generated in 2010 (covering requests served in 2009). The numbers we retrieved from the OEC using the law on free access to information (see the details of our campaign below) were striking. In 2009 Polish law enforcement agencies, including secret services, requested access to subscribers, traffic and location data as many as 1.06 million times, while the total population of Poland amounts to approximately 38 million. In 2010 the OEC registered an increase in the total number of requests received by the operators to 1 million and 400 000. The data for 2011 is not yet available.

Taking into account legal factors described above, i.e. the broad range of purposes for which telecommunications data can be requested, the list of authorities that can make such requests and the lack of efficient control mechanisms, these numbers come with little surprise. Unfortunately, all we know on the basis of data collected by the OEC is the total number of requests received by the operators. No breakdown into more meaningful categories like the type of request or the requesting entity is possible. We managed to learn a bit more through the public debate that started with the first release of the OEC data in 2010 (see the details below). According to the statements made by the police, over 300 plain officers have access to telecommunications data retained by the operators on a daily basis. Access to such data is performed via on-line interface, without the need to consult the operators' staff. Similar rules apply to other entitled entities, including secret services, military police and fiscal police[6].

On the basis of further investigation carried out by a dedicated working group set up by the Prime Minister in 2010 (more details will be given below), we learnt that 44% of all

6 Border Guard, Internal Security Agency, Military Intelligence Service, Military Counter-Intelligence Service, Military Gendarmerie, Central Anti-Corruption Bureau and Treasury Intelligence

requests in 2009 came from secret services, military police, fiscal police and the border guard[7]. On average, half of these requests concerned basic subscriber data, while the rest concerned both traffic and location data. It was calculated that the remaining 56% came from the police, courts and prosecutors. Unfortunately, no further breakdown was possible do to the fact that these entities were unable to produce relevant data even at the Prime Minister's request.

More valuable information about the practical use of data retention came from the media. In 2010 and 2011 media reported a series of political affairs involving systematic surveillance of journalists. It was established that a number of times data retention was used by secret services in order to trace back journalistic sources in high-profile cases. Several well-known journalists were subjected to this form of surveillance over significant period of time[8].

Further examples of how traffic data and location data tends to be used in practice can be found in numerous journalistic reports and press interviews with former security agents and prosecutors published in 2010[9]. These informants confirmed that all law enforcement agencies are allowed to request traffic data records in a rather informal manner, without the need to justify such request or undergo any transparent legal procedure. Also according to the telecommunications operators, procedures used by policemen and security agents while accessing data do not fulfill proper security and control standards. The retained data is accessed through simple interfaces established on telecommunications networks lacking any registration procedures in the network provider's systems.

Finally, on the basis of the reports coming from the media, the Data Protection Commissioner, attorneys and judges, we know that more and more often traffic and location data is requested by the parties in civil disputes such as divorce and alimentary

7 Detailed breakdown: Border Guard - 15%; Internal Security Agency - 13%, Central Anti-Corruption Bureau - 4%, Military Counter-Intelligence Service- 11%. Source: http://www.panoptykon.org/sites/default/files/Material_Cichocki_sprawdzenia_luty2011_0.pdf

8 See e.g. Gazeta Wyborcza, Wojciech Czuchnowski, „Dziennikarze na celowniku służb specjalnych" [http://wyborcza.pl/1,75478,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html] Wiadomości24, Monika Olejnik, "Podsłuchiwano mnie i dziewięciu innych dziennikarzy" [http://www.wiadomosci24.pl/artykul/monika_olejnik_podsluchiwano_mnie_i_dziewieciu_innych_163217.html];

9 Gazeta Wyborcza, Ewa Siedlecka, „Władza staje na straż y swojego interesu" [http://wyborcza.pl/Polityka/1,103836,8506779,Inwigilacja_dziennikarzy___wladza_staje_na_strazy.html] Gazeta Wyborcza, Wojciech Czuchnowski „Speckomisja: można inwigilować dziennikarzy"[http://wyborcza.pl/1,75478,8506756,Speckomisja__mozna_inwigilowac_dziennikarzy.html]; Gazeta Wyborcza, Monika Olejnik, Agnieszka Kublik„10 mln. Za wojnę bogów [http://wyborcza.pl/1,75480,8542355,10_mln_za_wojne_bogow.html?as=7&startsz=x]

disputes. Systematic use of data retention for civil cases proves that even judges themselves tend to abuse existing legal mechanisms and show little sensitivity towards such values as privacy and confidentiality of communication.

The rudimentary official data collected by the OEC is not sufficient to assess how often, for what purposes and with what results for crime investigations the traffic data is being used by the police or secret services. This also means that we cannot make a well-grounded assessment to what extent blanket data retention regime can be justified at all. However, what we know from both statistics and individual stories reported by the media allows to draw one conclusion: the way this particular instrument was implemented in Poland have lead to systematic infringements of the fundamental right to privacy and data protection principles.

(3) OUR CAMPAIGN

Over last two years Panoptykon Foundation have been involved in the debate and activism concerning data retention regime. In fact, it was us who brought this topic into the mainstream public debate. Our activity in this field started with the EU-wide campaign related to the evaluation and expected revision of the Data Retention Directive. The European Commission announced the evaluation process at the time when Panoptykon Foundation was set up as a professional NGO and joined European Digital Rights coalition ("EDRi"). Thus, the campaign against blanket data retention became our flagship activity in 2010 and 2011.

The first stage was gathering knowledge and collecting information. Using new contacts from the EDRi network and our own research we prepared a comparative analysis of the law on data retention, looking at Poland and a few other European countries. We commissioned a renowned Polish expert in criminology, prof. Andrzej Adamski to write an opinion supporting our critical arguments against blanket data retention regime. Last but not least, we asked (using Polish law on access to public information) the OEC to reveal statistical data about the use of data retention by all entitled entities (i.e. police, secret services, military police, fiscal police, courts and prosecution). As it was mentioned above, the OEC collects this data directly from telecommunications operators. On the basis of the data we obtained it became clear that Poland was the European leader in terms of abuse or misuse of data retention. The official number of requests served by the telecommunications operators in 2009 amounted to 1 million (versus tens or – at the most – a few hundreds of thousands in other Member States)[10].

The second stage was outreach and communication with key stakeholders. We got in

10 Compare the official report prepared by the European Commission on the implementation of the Data Retention Directive: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

touch with the EC officials responsible for the evaluation process (DG Home) and arranged for a meeting in Brussels in order to present them with our concerns and arguments. The same week when our first Brussels trip occurred, we released information about the outstanding number of requests for telecommunications data made in 2009 to the Polish media[11]. It immediately became the front page news. In the following months we took part in numerous public debates and official meetings as described below.

(4) POLITICAL SHIFTS

As a result of media attention and civic pressure, the Prime Minister commissioned an investigation into the use of data retention by all entitled entities. The results were released to the public, and proved that there are systemic problems with the use of this instrument, namely the lack of effective control mechanisms, very broad range of purposes for which data retention can be used, broad range of entitled entities, unnecessarily long retention period etc.. We were invited by the Ombudsman to meet and present her with our arguments against blanket data retention. Soon after the Ombudsman organised a public debate on the issue, inviting us to confront the Minister responsible for supervising secret services.

In the following months the Ombudsman issued a formal appeal to the Prime Minister calling the government to change data retention law[12], while the Data Protection Commissioner and the Supreme Chamber of Attorneys organised critical conferences devoted to this problematic[13]. At Panoptykon Foundation we continued our advocacy, using the opportunity that in 2011 we had frequent meetings with high rank government officials and the Prime MInister himself devoted to the broader problematic of internet regulation[14].

Probably as a result of such multi-channelled pressure, the Prime Minister announced the shift in approach to data retention and promised changes in legal regulation, backed by adequate evidence[15]. During a public meeting we heard that he would demand more

11 Ewa Siedlecka, Całe nasze życie na podglądzie (All our life on a preview), Gazeta Wyborcza 2010-10-07 and Ewa Siedlecka, Nasze bilingi i internet pod lupą służb (Our billings and internet under the secret services' surveillance), Gazeta Wyborcza 2010-11-09

12 Source: http://www.sprawy-generalne.brpo.gov.pl/pdf/2010/12/662587/1540465.pdf

13 http://www.panoptykon.org/content/polskie-obchody-dnia-ochrony-danych-osobowych-dyskusja-o-retencji-danych;http://www.panoptykon.org/wiadomosc/retencja-danych-konferencja-raport-nra-i-odpowiedz-ministra-cichockiego

14 http://www.panoptykon.org/taxonomy/term/190

15 http://www.panoptykon.org/wiadomosc/relacja-video-z-debaty-z-premierem; http://www.panoptykon.org/wiadomosc/regulacja-internetu-co-dalej-final-dialogu-z-premierem; http://www.panoptykon.org/wiadomosc/premier-przestawiliscie-mi-optyke-na-prawa-

evidence from secret services to justify their scope of powers with regard to the use of telecommunications data. The Prime Minister said his intention was to “decrease the oppressive potential” of this apparatus and increase its “human rights sensitivity”.

A dedicated working group chaired by the minister supervising secret services was set up in order to analyse the implications of existing data retention law (including potential abuses) and propose adequate legal changes. After four months of deliberations the working group announced their vision of necessary reform. The report addressed many issues and critical comments made by the Ombudsman[16]. Although we were not entirely satisfied with this proposal (we presented the government and the media with very detailed opinion explaining which elements of the proposal require further consideration and why[17], we appreciated its direction. We have been witnessing a positive shift in the official paradigm, from unquestionable belief in the necessity of blanket data retention to critical approach framed by the discourse of proportionality.

The proposal prepared by the governmental working group has not been implemented yet. Soon after it was announced came the elections. The person then acting as the minister supervising secret services became the minister of internal affairs. The first step towards changing the data retention regime has been taken by the Ministry of Administration and Digitalisation. It proposed a reduction of the retention period to 1 year and the change in access rules to the effect that only criminal courts would be able to use the retained data.[18] This limited proposal is pending in the Parliament. We are now preparing to resume our campaign and demand much more on the basis of the new statistical data, which will be made available by the OEC within the next couple of days.

---

podstawowe-w-internecie

16 http://www.panoptykon.org/wiadomosc/minister-cichocki-proponuje-ograniczenie-uprawnien-sluzb-specjalnych-ale-przy-utrzymaniu-r; http://www.panoptykon.org/sites/default/files/zespol_retencyjny_sprawozdanie_z_pracy.pdf

17 http://www.panoptykon.org/sites/default/files/panoptykon_msw_retencja-danych_stanowisko_23-12-2011_0.pdf

18 http://www.panoptykon.org/wiadomosc/maic-w-ofensywie-nowe-prawo-telekomunikacyjne-i-nowe-przepisy-o-\