Remigiusz Rosicki, PhD
Faculty of Political Science and Journalism
Adam Mickiewicz University, Poznań

SURVEILLANCE AND DATA RETENTION IN POLAND

Abstract
The object of analysis in the present text is the issue of surveillance and data retention in Poland. The analysis of this issue follows from a critical stance taken by NGOs and state institutions on the scope of operational control wielded by the Polish police and special services – it concerns, in particular, the employment of "itemised phone bills and phone tapping."

Besides the quantitative analysis of surveillance and the scope of data retention, the text features the conclusions of the Human Rights Defender referred to the Constitutional Tribunal in 2011. It must be noted that the main problems concerned with the employment of surveillance and data retention are caused by: (1) a lack of specification of technical means which can be used by individual services; (2) a lack of specification of what kind of information and evidence is in question; (3) an open catalogue of information and evidence which can be clandestinely acquired in an operational mode. Furthermore, with regard to the access granted to teleinformation data by the Telecommunications Act, attention should be drawn to the wide array of data submitted to particular services.

Also, the text draws on open interviews conducted mainly with former police officers with a view to highlighting some non-formal reasons for "phone tapping" in Poland. This comes in the form of a summary.

Key words: *operational control, data retention, teleinformation data, police, secret services, phone tapping, civil liberties*

1. Introduction

In 2010 the police and other competent authorities made over 6,700 requests for surveillance. Only in 4% of all the cases did courts and prosecutors not order the monitoring or recording of conversations (courts refused in 0.7% of cases and the prosecutor's office in 3.2% of cases).[1] It means

[1] Calculations are based on the 2011 Chief Prosecutor's report. Percentage values are expressed to the second digit after the decimal place.

that only very few requests by individual institutions were not granted permission. 2011 saw an increase of over 1,000 requests for surveillance. It must be noted that quantitative data on tapping apply to trial cases, namely those cases where the acquired information can be submitted as evidence (with the intention of detecting and preventing crime). Apart from wiretapping, itemised telephone bills and text message records are also used. The European Commission, in its 2011 report evaluating the Directive on the retention of telecommunications data, indicated that, statistically, Poland comes first in terms of requests for telephone users' traffic data [9].

According to the information 14 member states submitted to the European Commission, Poland's activity amounted to 51% of all data retention requests in 2009. By contrast, France accounts for 25%, the Czech Republic for 13.6%, Lithuania for 3.5% and Spain for 3.4%. A significant number of requests in Poland can only partially be explained by the fact that the relevant authorities need to submit identical requests to each of the main mobile telephone operators.[2]

In 2012, however, all the authorities requested surveillance on 4,206 people (encompassing wire tapping, SMSes and MMSes). About 80% of requests received by the prosecutor's office were submitted by the police [7]. A drop in the number of requests can be attributed to some changes in the Code of Penal Procedure and the Police Force Act, which tightened prosecutor supervision over the operational techniques used by law enforcement services. Even so, it needs to be noticed that the ability to abuse law has not disappeared. This is connected with the list of offences whereby phone tapping and recording is enforceable (e.g. it is often claimed that other methods to combat organised crime groups have proved ineffective).

It is notable that in Poland there are 11 institutions with the power to wiretap citizens, which is unparalleled, not only on the European scale. It may also speak volumes about how policy-makers decide to develop control mechanisms and attempt to reduce the inefficiency of the state's structures and individual institutions by vesting special powers in them. The problem is that those special powers significantly affect citizens' rights. Moreover, the Polish foundation Panoptykon stresses that existing legislation on the availability of telecommunications data is used to circumvent

[2] The calculation is based on data provided by the European Commission. Percentage values are expressed to the second digit after the decimal place.

regulations on professional privileges – confidentiality of journalistic sources in particular [2]. Another problem is that some services refer to itemised phone bills in order to indicate perpetrators, which stems from the fact that, unlike in the case of wiretapping, a request for an itemised telephone bill is not subject to restrictions, whereby an offence has to be detected [14]. The abuse of the legislation is well exemplified in the case of B. Wróblewski (a journalist for the Polish newspaper *Gazeta Wyborcza*) versus the Central Anti-Corruption Bureau. In a civil trial the Warsaw Court of Appeal ruled that the Bureau illegally checked his phone records in 2007 and found it guilty of infringing Mr. Wróblewski's personal interests, his right to privacy and freedom to establish contacts [6].

According to Panoptykon's data from 2011, state institutions issued over 1.85 million information requests concerning citizens' telecommunications contacts. This is up by about 500,000 compared with last year and by about 800,000 compared with 2009. This fact met with a reaction from Human Rights Defender, who drew the government's attention to the problem of disclosing wiretaps and phone records. In 2011, Human Right Defender twice made a request to the Constitutional Tribunal for a conformity check with the existing legislature. In 2013, the Constitutional Tribunal received from the Supreme Audit Office a report on the extent to which phone records data is acquired and processed. The Supreme Audit Office bluntly stated that current legislation does not protect citizens' rights and liberties sufficiently.

2. Human Rights Defender's requests to the Constitutional Tribunal in 2011

On the 29th July, 2011, Human Rights Defender filed with the Supreme Court a request to deem Article 19 Paragraph 6 Subparagraph 3 of the Police Force Act unconstitutional [10] (as well as its equivalent regulations in the Border Guard Act, Military Police Act, State Protection Office Act, Intelligence Agency Act, Central Anti-Corruption Bureau Act, Military Counterespionage Service Act and Military Espionage Service Act) [13]. The problem concerned the employment of technical devices enabling, by covert means, the acquisition and recording of information and evidence, in particular phone conversations registered by telecommunications networks (Article 19 Paragraph 6 Subparagraph 3 of the Police Force Act). What proved to be the main problem was the imprecision of the regula-

tion, which allowed some leeway for the authorities to use unspecified technical devices (e.g. GPS navigation systems). According to Human Rights Defender, the problem lay not in the wide extent to which the devices were used, but the fact that they served the purpose of obtaining unspecified information about citizens. Moreover, there was a lack of control, as the activities of individual authorities under the contested provision corresponded to operational activities, hence they were not considered procedural activities [13, pp. 2-4].

Under the then law on surveillance (nonprocedural proceedings) [13, p. 7][3] all technical devices which enabled the acquisition and recording of data and evidence were allowed. Human Rights Defender claimed that the problem lay in imprecisely outlining the following items:

1) technical devices that the services were permitted to use,
2) the information and evidence in question,
3) list of information and evidence that could be covertly acquired during operational procedures [13, pp. 5-6].

In this context, Human Rights Defender indicated that the following regulations enshrined in the Constitution of Poland might be being breached: Article 31 (the scope of constraints on constitutional rights and liberties), Article 47 (*inter alia* legal protection of privacy), Article 49 (freedom of communication and protection of its confidentiality), Article 50 (inviolability of domicile), Article 51 (an individual's right to disclose information), Article 52 (freedom of movement). Moreover, the powers exercised by border guards, fiscal controllers and the military police could result in a far-reaching encroachment on the image rights of an individual.

On the 1st August, 2011, Human Rights Defender filed another request with the Constitutional Tribunal; this time it regarded the access that individual authorities had to telecommunications data. The request intended to verify the unconstitutionality of Article 20 Paragraph 1 of the Police Force Act [4] as well as its equivalent regulations in the Border Customs Act, Military Police Act, Fiscal Control Act, State Protection Office Act, Intelligence Agency Act, Military Counterespionage Service Act and Military Espionage Service Act. This constitutionality was determined by the pow-

[3] Under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms the right to respect for correspondence can be constrained if it is 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.

ers established in communications law, precisely in Article 180c and Article 180d on data collection [11].

Defender's position was determined by Article 159 Paragraph 1 of the Telecommunications Act which introduced the term 'confidentiality of communication', encompassing: user data, content of communications, traffic data (including location data), location data that goes beyond the data necessary for the transmission of a communication or billing, data about attempts at establishing a connection between network terminations. The relatively wide term 'data' encompassed not only the content but also the user's data and location data [12]. Any encroachment on the confidentiality of communication needs to be justified and clearly specified (vide Article 31 of the Constitution of Poland), otherwise Article 49 of the Constitution of Poland (freedom of communication and protection of its confidentiality) and Article 8 Paragraph 1 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the right to respect of the confidentiality of correspondence) would both be infringed.[4]

Article 159 Paragraph 2 of the Telecommunications Act stipulated that it was forbidden for anyone but the sender and the receiver to access, record, store, export or use protected content in any manner or data, unless 1) it was the subject of the service or it was necessary to provide the service; 2) the sender or the receiver of the data consented to it; 3) those activities were necessary in order to register the communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication; 4) it was necessary for different purposes stipulated in the Act or in separate provisions. Furthermore, Article 159 Paragraph 3 stated that disclosing and processing confidential content or data, other than those provided for in the Act, was tantamount to breaching confidentiality [11] [12].

According to Human Rights Defender, it was not the regulations of the Telecommunications Act that posed the problem, but the nature of surveillance i.e. their subsidiarity and confidentiality. Moreover, the checks were to be applied to precisely defined offences, and any materials obtained by those means needed to be destroyed when proved useless (Article 19 of Police Force Act). However, under Article 20c Paragraph 1 of the Police Force Act in order to prevent or detect offences, the police could provide telecommunications data which could then be processed [10; 12, pp. 5-6].

---

[4] This refers to the data specified in Article180c and 180d of the Telecommunications Act (Journal of Laws No. 171, item 1800 with amendments).

Under Article 180d of the Telecommunications Act, should the competent services request it, telecommunications companies were under the obligation of ensuring conditions for data access and recording, as well as the availability of the processed data (at their own cost) related to the telecommunications service provided and mentioned in Article 159 Paragraph 1 Subparagraph 1 and 3-5, in Article 161 Paragraph 9. Therefore, it needed to be noticed that individual authorities could access, among other things, traffic data and location data and data such as names, surnames, parents' names, date and place of birth, address, personal identification number, number and series of ID and information confirming the performance of the obligation towards the provider of telecommunications services. Moreover, the competent authorities could obtain different data: tax identification number, address, bank account number, email address and phone contact list with phone numbers.

Undoubtedly, the list of data made available for specified authorities was long. By the same token, the list of offences which constituted the legal basis for a disclosure request was equally long. The non-exhaustive list made it possible to circumvent certain constraints on information access connected with the principle of professional secrecy, such as journalistic confidentiality and legal or medical professional privilege. In addition, Articles 180c and 180d of the Telecommunications Act did not embrace the principle of subsidiarity, which meant that the telecommunications operator had to provide data not only in essential cases. In this context, the competent authorities did not have to seek the court's permission to access data protected by the confidentiality of communications regulations [12, pp. 12-13].

It could not be argued that the regulations in question facilitated the work of particular authorities, which also could not serve as an argument in a democratic state, governed by the rule of law (cf. Article 31, Paragraph 5 and Article 51 Paragraph 1 of the Constitution of Poland). Legislation on citizens' data collection which provided neither clear deadlines for the deletion of the data gathered, nor stipulated a clear purpose for storing it (in the case of the State Protection Office Act, Intelligence Agency Act, Central Anti-Corruption Bureau Act, Military Counterespionage Service Act and Military Espionage Service Act) should be seen as pathological.[5]

[5] In 2012 the Supreme Audit Office presented information on the control outcome entitled *Recruitment, Selection Procedure and Training of Newly-Employed Officials*

As regards the provisions in the Telecommunications Act (Article 180c and 180d inter alia) the Supreme Audit Office also voiced its concern, saying that the purpose of data retention needed to be specified because invoking the need to prevent and detect crimes was too general. The Supreme Audit Office, similarly to the Constitutional Tribunal, called for implementing the principal of subsidiarity – regulations which would allow the use of telecommunications data subject to the inability to use other means of control. Moreover, the Supreme Audit Office pointed out that there were no constraints as to the people targeted by data retention. *De facto*, it meant that those regulations clashed with safeguard principles such as professional privilege (e.g. legal or medical) [4].

3. Non-formal reasons behind telephone tapping in Poland[6]

Crime investigation is a significant element of police work which is intended to influence legal proceedings at a further stage. It needs to be stated that the quality of reconnaissance operations has decreased, which translates into the low efficiency of police investigation units.

The lower quality of operational and investigative work needs to be attributed to a poor training system, lower work standards, and insufficient control of superior police units over various local units [1] [3]. Poor performance on operational and investigative levels is connected with the misuse of basic investigation tools, e.g. preservation of evidence. It needs to be stated that police units, and the Central Bureau of Investigation on the regional level, hardly ever preserve evidence during the examination of a crime scene. Another problem is the poor performance of

---

of the Internal Security Agency, Central Anti-Corruption Bureau, Police and Border Guards [2]. The conclusions by the Supreme Audit Office are limited to the oversight of the recruitment and training system; therefore, they do not include the issues indicated in the in-depths interviews. The same limitation can be observed in case of 2012 Supreme Audit Office's report on *The Functioning of Schools and Training Centres in the Police, National Fire Brigades and Border Guard* [1].

[6] Based on in-depth interviews with former police officers (interviews were carried out in 2012). In 2013 the interview was conducted again, this time, however, with former police officers who found employment in the private sector (entities ensuring security of persons and property).

operational and investigation departments regarding sourcing proper comparative materials. The overall negligence affecting evidence and investigation results in numerous case dismissals where the accused is acquitted.

All the outlined problems have an effect on the policy of information gathering using ICT. It manifests itself in the excessive collection of suspects' phone records and resorting to surveillance tools such as wiretaps. The fact that Poland lacks actual control of superior police units, or the absence of interest in the matter, has led to a situation in which officers gather a significant amount of data about subscribers. This data, gathered for 2-4 years, is largely left unanalysed, as there is no technical possibility to process it into procedural material. As a result, volumes of case files mainly deal with phone records materials and wiretap materials and barely address the substance of cases.

This results in a situation where data on a subscriber's identity, his/her phone records, etc. is pointlessly and massively collected in operational case files until the case is closed. When the data is collected by the police, this situation may actually result in breaching Article 20c Paragraph 7 of the Police Force Act. In police jargon, this way of carrying out operations and investigations is referred to as a 'desk job'. Drawing on wiretaps and phone records grew to be a working method because of:

1) officers' poor competence,
2) low efficiency of operational and investigative work,
3) officers' ineptitude in recruiting informants.

The appraisal of officers' work is also shaped by what could be described as "the department's low level of work culture." Additionally, police officers are particularly motivated to use wiretaps and itemised telephone bills as they have to produce monthly, quarterly, six-monthly or yearly reports on the extent to which phone records, wiretaps or other means of operational work are used. The reports are assessed on a quantitative rather than qualitative basis, i.e. less importance is placed on its purpose and end result.

Despite all this, it needs to be stressed that the materials acquired in data retention enable the verification of other evidence. Data of this type facilitates verifying the whereabouts and alibi of a given person, or combating crimes committed over the phone or the internet. The Polish example, nevertheless, is one of abuse of wiretaps and phone records by the police and other authorities.

4. Abuse of telephone tapping[7]

Article 19 Paragraph 1 Subparagraphs 1-8 of the Police Force Act outlines cases in which police may resort to surveillance on a suspect [10]. In most cases, the checks are exercised by other authorities e.g. Central Bureau of Investigation, State Protection Office, Intelligence Agency and Central Anti-Corruption Bureau (the regulation thereof). In the case of Regional Police Headquarters and individual field offices of the Central Bureau of Investigation, it needs to be noticed that to use this operational strategy the authorities embark on operations with the premise of 'organised crime' i.e. they presuppose that they are dealing with this specific crime. This assumption is often routinely made so as to be given permission to use wiretapping. This can be exemplified by the activities of Central Anti-Corruption Bureau in 2007. It requested a warrant to wiretap three people (J. Netzl, J. Kaczmarek and K. Kornatowski) claiming international drug dealing to be the need for surveillance, while, in fact, the people in question were in no way involved in this sort of criminal offence.

It is also worth noticing how permission requests for surveillance are created. Police use templates – a consequence of using text editors – and officers store them on a data storage device. Elements of the request, such as the justification for the request, ineptitude or uselessness of other means or the legal precepts are already entered on the template. Often, in their requests, officials representing Central Bureau of Investigation, State Protection Office, Intelligence Agency, and Central Anti-Corruption Bureau cite 'urgency' (police officers invoke Article 19 Paragraph 3 of the Police Force Act).

There are some deadline regulations within the Penal Code on wiretapping, under which wiretaps in the so-called operational mode are meant to gather information about people and matters for no longer than five days. Those regulations limit excessive checks on citizens and are intended to vet the institutions which resort to wiretaps. However, it needs to be noted that officers competent to use wiretaps are quite open about how to circumvent those time limitations. Therefore, it gives rise to the situation in which a citizen's data can be gathered without a warrant. Such a warrant is indispensable when telephone tapping in an operational procedure is ex-

[7] Ibidem.

pected to last longer than five days. Should the warrant not be issued, all materials which cannot be used in the trial process must be destroyed. This leads to the possibility of use and abuse of these materials in other cases without quoting its source.

On some occasions insufficient supervision by a superior (e.g. due to frequent job rotation) has led to a situation in which procedures on deadline for requesting the warrant were not duly followed. As a result, officers enjoyed access to materials obtained during surveillance without abiding by the Protection of Classified Information Act. Information acquired in that way was used in other operations, and its real source was not always revealed.

Under the existing legislation surveillance should last no longer than three months (Article 19 Paragraph 8 of the Police Force Act), however, in justified cases the deadline can be extended by another three months – if and when the grounds are still valid. Moreover, Article 19 Paragraph 9 of the Police Force Act prescribes that the Chief Prosecutor may order surveillance for a definite duration even after the deadline indicated in Article 19 Paragraph 8 (in justified cases) [10].[8]

It needs to be stated that surveillance of suspects in Poland is abused in the course of operations. This means that the provisions of Article 19 Paragraph 13 of the Police Force Act are being consciously breached. What points towards this abuse is the rare application of Article 19 Paragraph 15 of the same act [10]. As a result, evidence gathered in the course of surveillance is only used in a few cases to institute criminal proceedings, or is of negligible importance for those proceedings.

Furthermore, cases where evidence is obtained in the course of surveillance are most likely not to observe Article 19 Paragraph 17 of the Police Force Act – so there are lengthy surveillance and delays in destroying the materials obtained thereby. Shortcomings in police performance in this area should be attributed mainly to a lack of supervision by superiors and inefficient staff policies of the police and prosecuting authorities.

---

[8] Another problematic issue is the fact that the police invoke 'new circumstances' believed to be vital in preventing and detecting crime or in identifying perpetrators or obtaining evidence – in accordance with Article 19 paragraph 8 and 9 of the Police Force Act enacted on 6.04.1990 (2007 Journal of Laws No. 43, item 277 with amendments).

5. Conclusions

The analysis presented should be followed by conclusions on surveillance and data retention in Poland. What immediately attracts attention are the numerous institutions vested with wide-ranging powers as regards checking and recording conversations or, in general, access to information and communications data. The tendency has not changed; additionally, in 2013 some legislative amendments were drafted in order to give further powers to the Military Police as a secret service. One cannot help but get the impression that the authorities are attempting to compensate for the inefficiency of individual authorities (police and separate secret services) by conferring various powers on them. This gives rise to ever-growing, highly powerful institutions, a trend which is reflected in the debate on the need to create a 'rubbish police' as a tool to meet the provisions of the Maintenance of Cleanliness in Communes Act passed in Poland in 2013.

Separate secret services and the police face particular problems using technical devices for surveillance. The main problems connected with legal regulations and the services' work encompass: (1) a lack of precisely-defined devices that the services may use; (2) no precisely-defined targeted information and evidence; (3) a non-exhaustive list of information and evidence that can be covertly obtained through operations. Moreover, since the Telecommunications Act allows for some data to be disclosed, a long list of that data made available to specific authorities cannot be overlooked. The data can be easily requested because the principle of subsidiarity is not in existence. Another risk concerns obtaining data without defining a targeted group, which may lead to violating professional privileges.

The in-depth interviews with a relatively limited group of former police officers in 2012 and 2013 form the basis for an analysis which concludes that telephone tapping has become common in Poland due to (1) the lower quality of operational and investigative work; (2) bad methods of supervision over application of individual operational techniques; (3) poorly trained officials in recruiting informants; (4) the abuse of existing regulations (also the provisions of the Telecommunications Act); (5) the abuse of justification of control requests (officials often cite the need to prevent and detect organised crimes).

References

1. Funkcjonowanie szkół i ośrodków szkoleniowych w policji, państwowej straży pożarnej i straży granicznej – Warszawa: NIK, 2012.
2. Ile razy państwo sięgało po nasze dane telekomunikacyjne w 2011 roku? http://panoptykon.org/wiadomosc/ile-razy-panstwo-siegalo-po-nasze-dane-telekomunikacyjne-w-2011-roku-publikujemy-najnowsze – 3.04.2012.
3. Nabór, postępowanie kwalifikacyjne i szkolenie nowo przyjętych funkcjonariuszy ABW, CBA, Policji i Straży Granicznej, Warszawa: NIK, 2012.
4. NIK na temat bilingów – http://www.nik.gov.pl/aktualnosci/bezpieczenstwo/nik-na-temat-billingow.html – 20 sierpnia 2013.
5. Panoptykon [Strona internetowa fundacji]: (dane uzyskane od polskiego Urzędu Komunikacji Elektronicznej) – http://panoptykon.org/sites/default/files/retencja_danych_2011.pdf – 3 kwiecień 2012.
6. PAP, 26 kwiecień 2013.
7. Prokuratura Generalna [dane statystyczne] – http://www.pg.gov.pl/ – 30 wrzesień 2013.
8. Siedlecka E., Polska – mistrz w śledzeniu /E. Siedlecka// Gazeta Wyborcza – 2 kwiecień 2012.
9. Sprawozdanie KE dla RE i PE "Sprawozdanie z oceny dyrektywy w sprawie zatrzymania danych" (dyrektywa 2006/24/WE), Bruksela 18.04.2011. – KOM (2011).
10. Ustawa o Policji z dnia 6 kwietnia 1990 r. (Dz. U. Nr 43, poz. 277 ze zm.).
11. Ustawa Prawo telekomunikacyjne z dnia16 lipca 2004 r. (Dz. U. Nr 171, poz. 1800 ze zm.).
12. Wniosek RPO do TK w sprawie dostępu poszczególnych służb do danych telekomunikacyjnych – 1 sierpnia 2011 r. [Wniosek RPO z 1 sierpnia 2011 r.].
13. Wniosek RPO do TK w sprawie stosowania przez poszczególne służby w ramach kontroli operacyjnej środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie – 29 czerwca 2011 r. [Wniosek RPO z 29 czerwca 2011 r.].
14. Zieliński R., Służby zaplątały się w nasze bilingi /R. Zieliński// Dziennik Gazeta Prawna – 16-18 marzec 2012.

Резюме

Предметом анализа в статье является проблематика операционного контроля и ретенции данных в Польше. Анализ этой проблематики вытекает из критического отношения неправительственных организаций и государственных учреждений в сфере использования оперативного контроля польской полиции и спецслужб, в частности это касается сферы применения "выписок со счетов" и так называемых "прослушек".

В тексте, кроме анализа количественного контроля операционных данных и данных из сферы ретенции, представлены выводы омбудсмена, направленные в Конституционный Суд в 2011 г.

Следует указать, что главные проблемы, связанные с применением операционного контроля и ретенцией данных вытекают из: (1) отсутствия определения технических средств, которыми могут пользоваться отдельные службы, (2) отсутствие определения того о какой информации и доказательствах идет речь, (3) открытого каталога информации и доказательств, которые могут быть скрыто получены в оперативном режиме. Кроме того, в связи с предоставлением данных связи и телекоммуникации на основании Закона о телекоммуникациях, следует обратить внимание на широкий спектр данных, доступных определенным службам.

В тексте использованы также так называемые "открытые интервью", проведенные главным образом с бывшими сотрудниками полиции, с целью показать неформальные причины использования "прослушек" в Польше – что было представлено в форме краткого содержания.

Ключевые слова: *операционный контроль, защита данных, данные связи и телекоммуникации, полиция, секретные службы, прослушивание телефонов, гражданские свободы*