Joanna Trela-Zielińska[1]

DATA RETENTION AS A COUNTER-TERRORISM INSTRUMENT. THE ANALYSIS IN THE CONTEXT OF CIVIL RIGHTS PROTECTION

Keywords: telecommunications data retention, terrorism, civil rights, privacy.

ABSTRACT: The article analyses the legitimacy of citizens telecommunications data retention usage in the fight against terrorism. Data retention, that is the preventive storage of information on the source, data, hour and duration of a connection, type of the connection, communication tool and location of a recipient, is a powerful source of knowledge about citizens and their use should be soundly justified. However, both the European Union and Polish practices show that behind this interference in privacy there is neither a guarantee that the data stored would be used exclusively to fight terrorism and severe crimes, nor a sufficient access control mechanism. The efficiency of data use in the fight against organized crimes, including terrorism, is also dubious.

In her work the author analyses Polish studies concerning information disclosure issues, Internet publications of the European Union and American reports on retention programmes, as well as Polish and foreign positions of non-governmental organizations engaged in the civil rights protection in this respect.

[1] Joanna Trela-Zielińska, University of Szczecin, Faculty of Humanities, Institute of Political Science and European Studies, trela.joanna@gmail.com.

INTRODUCTION

The article is devoted to the evaluation of effectiveness of so called "data retention", that is a preventive telecommunications data storage (information covering the source of the connection, its recipient, data, hour and duration, device and its location) in the context of the fight against terrorism. The author examines whether data retention is an effective counter-terrorism instrument, that may *ipso facto* justify the limitation of the right to privacy and freedom of expression. This dilemma was recognised by an acclaimed expert on terrorism, Tomasz Aleksandrowicz, who declared that: "The threat of terrorism is treated as a justification for a country to exercise an ongoing control over its citizens, both in the form of restricting the access to information and infringement of privacy rights" (2015, p.55). The condition described by Aleksandrowicz indicates that the protection of national security is impossible without interfering with the right to privacy of both suspects of pursuing criminal activity (terrorism included) and innocent citizens. This preventive character of retention is also illustrated by an outstanding lawyer Andrzej Adamski: "Let's suppose we are creating a profile of a terrorist residing in Holland (16 million citizens), descending from outside of the Western Europe (1.7 million citizens), an adherent of Islam (850,000 citizens) and the second generation immigrant (147,000 citizens), it is estimated that 1% of the people who fit the profile are the extremists. If among this group the following 10% constitute a real danger to the rest of the society, then basing on the profile and assumptions 147 people should be subjects to surveillance. What it implies in practice is that most of them, for no reason, would be deprived of part of their privacy" (Adamski, 2015, p. 2).

*T*he problem of the contemporary surveillance confines to intentional – concerning the services – and unaware – from the side of society – forfeiture of liberal values, that western democracy bases on. The author assesses this phenomenon through the research on data retention efficacy. Its starting point is the analysis of legislation overviews, sanctioning the use of telecommunications data retention. The further step is the exploration of examples of international actions foiled with the use of information deriving from the programs of data retention. The materials used in the

article were released by the EU (including Polish) public institutions and non-governmental organizations, the author based also on publications on the national security.

The author recognises the vastness of the topic and the fact, that the article does not exhaust all of its aspects, nevertheless, decided to concentrate on those issues that concern Poland, particularly in the context of new provisions in the Polish law adopted in 2016.

LEGAL REGULATIONS ALLOWING FOR TELECOMMUNICATIONS DATA STORAGE

The USA Patriot Act – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, passed on 26 October 2001 after the World Trade Center attack, was the first commonly known document to allow collecting and monitoring telecommunications and Internet data of the citizens suspected of terrorism. The Act was widely criticized for human rights and freedom of speech violation and its final revoking occurred after issuing the top secret data of the National Security Agency (NSA) by Edward Snowden. According to the Snowden's publication, the NSA together with the British Intelligence Agency – GCHQ, used a spying program *Prism* to gather the data of Google and Facebook users, mobile applications (such as Angry Birds) users as well as to record conversations of citizens, foreign politicians and in order to organise cyberattacks (Boussios, 2016, p. 39).

In May 2015, the USA Court of Appeals ruled illegality of the programme, and a month later the Patriot Act itself was terminated, being superseded by *the USA Freedom Act – Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act* – the following day. Pursuant to the above, these are telecommunications companies, not the NSA, that are obliged to store the data of the US citizens, which in principle should diminish the collective invigilation of private users. The access shall be granted only by the Foreign Intelligence Surveillance Court – FISC, what shall

verify the application concerning its connection to terrorism. The resolutions were applied 180 days after implementing, on 28 November 2015.

European regulations on data retention and storage began in 2006, as a result of the attacks held in London and Madrid. Then, on 15 March 2006 the European Parliament and the Council of the European Union introduced Directive 2006/24/EC. The directive, commonly known as the Retention Directive, imposed an obligation on the EU countries to formulate provisions for operators to gather and provide data of their clients to the investigative authorities. The value of the information stored was proven by the research of the Massachusetts Institute of Technology (MIT), according to which telecommunications data are in 90% of the cases a sufficient ground to reconstruct the network of contacts and the identity of a given individual, and in 95% cases to determine their location in the next 12 hours (the Panopticon Foundation, 2016). Until the annulment of the directive, governed by The Court of Justice of the European Union on 8 April 2014, private data of over 500 million of Europeans (European Digital Rights, 2016, p.23) were gathered and stored without their knowledge and consent.

The sensitive information released in June 2013 by Edward Snowden pertained also to Poland. According to Snowden, the project called *Orangecrush/Buffalogreen* has been operating in Poland since 2009, allowing an unidentified unit of the Polish government to pass Polish telecommunications metadata to the NSA. At one point of this cooperation, Poland is said to have transferred 3 million of telecommunications data a day (Obem, Szymielewicz, 2014). As a response to the leaks, in October 2013 three non-governmental organizations: Amnesty International Poland, the Helsinki Committees for Human Rights and the Panopticon Foundation addressed to various national institutions *(i.a.* president, the Prime Minister, the Ministry of Foreign Affairs) over one hundred inquiries on surveillance (the Panopticon Foundation, 2016). The requests considered *i.a.* the information on actions that the Polish government undertook concerning the American spying program *Prism*, granting an asylum for

Edward Snowden and the information on the flow of personal data within the Transatlantic Trading and Investment Partnership (TTIP). Most of the questions remained unanswered.

In Poland the obligation of data retention was established on 24 January 2003, when on the grounds of the directive of the Ministry of Infrastructure, operators were obliged to retain telecommunications data for the duration of 12 months. When in 2006 the European Union introduced the Retention Directive, Polish legislation implemented its provisions in the maximum scope. Except for the telecommunications data, Polish services had free access to the location of a subscriber, their data and billings. As one of three countries in the European Union Poland had no control over the data accessibility and the storage duration was of a maximum 24 months period. In January 2013 the storage was shortened to 12 months, nevertheless, the problem of uncontrolled access to the data has remained unsolved.

On 30 July 2014, the Constitutional Tribunal on the request of the Polish Ombudsman and the General Prosecutor imposed the change of provisions regulating data retention. The ruling pointed the infringement of the Constitution of the Republic of Poland through the lack of mechanisms of independent external control while providing the telecommunications data of Polish citizens to the police and other services. The ruling said: "If accessing the data is of a disclosed nature, held without the knowledge and will of individuals, whose data are collected and at the same time with a restricted control from society, the lack of independent control from the authorities in the process creates the danger of abuses. It may not only contribute to the unsubstantiated intervention in freedom or human rights but also create a threat to democratic mechanisms of governance". (the Constitutional Tribunal of Poland, 2014, p.115).

The provisions that the Tribunal declared to be of unconstitutional nature were to be changed within 18 months from the publication in the Journal of Laws on 6 February 2016. The amendment of the Police Law, implemented in due time, brought no greater changes to the control of data access. New regulations theoretically provided the mechanism of verification of data access in the form of reports issued

to the regional count in every 6 months. Considering the amount of requests of the services on telecommunications data (2 177,916 in 2014) the court exercising such a control would not be able to assess the validity of most of them (Obem, Szymielewicz, 2015).

The lack of sufficient judicial control over the data gathered by services indicate potential lack of control over its safety. Łukasz Wojciechowski, an outstanding specialist on data protection, points out two main threads: unauthorised data access and their loss. In both cases the solution is to develop the procedures in order to provide the access and integrity control in both electronic and material way. The procedures shall include mechanisms of data access control, distribution of codes changed every 30 days, protection against viruses, sufficient control of devices and copies, as well as deletion of data from the devices that are to be disposed (Wojciechowski, 2016, p.14).

Joanna Świątkowska, a programme director of European Cybersecurity Forum – CYBERCES, reminds that the recent adoption of *the General Data Protection Regulation* imposes on the Inspector General for Personal Data Protection (GPDP) the procedures of personal data protection also in respect of the Internet (Świątkowska, 2016, p.63). That implements *i.a.* the obligation of obtaining the agreement from a person whose data is being processed as well as the control of all "processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes" (European Parliament, 2016, p.24).

Meanwhile, the new Polish law extends the range of collection to include the Internet data. Internet suppliers shall provide the agencies with personal data of the Internet users, as well as exploitation information, showing the activity of Internet users online. Since February 2016 the services (not only the Police, but also the Tax Office, the Military Police, Border Guards, Customs, the Internal Security Agency, the Military Counterintelligence Service, the Central Anti-Corruption Bureau) have had access to the information concerning all the websites and applications used by an Internet user, as well as time and duration of their visits. What is more, the access is possible without the awareness of an individual, as well as without presenting a vital explanation. In practice it

means the continuation of preventive surveillance, that is monitoring the citizens before any formal procedures are taken. However, the amendment confines that the access to the data should be restricted only to telecommunications, e-mail or Internet data and the secrecy of the correspondence shall be maintained.

ANALYSIS OF DATA RETENTION EFFICIENCY IN THE RESPECT OF CIVIL RIGTHS LIMITATIONS

National security is, according to the authors of publication of *National Security of Poland in the XXI century* : "(…) the greatest existential need, the national value and priority of Poland to ensure the maintenance, security and protection of the national heritage, values and national business and interest from the potential threats and creating the conditions of good life and personal development for future generations (...)" (Flis, Jakubczak, 2006, p.7). Therefore, it should come as no surprise that the country, as a guarantee of security, undertakes various means for its realization. Their effectiveness must be constantly verified not to allow any danger. In case of the surveillance described herein, the above-mentioned thread is the infringement of the privacy right, constituting the fundamental prerogative of the citizens. How is it possible to assess validity of breaching one law to protect another?

The optimal assessment of the action held can be estimated through valuating their efficiency, in this case the efficiency of retention data use may be measured by the number of terroristic attacks that it foiled. Due to the lack of access to the intelligence, the author based on published reports and opinions of specialists on security.

The review of opinions began with the position of the Privacy and Civil Liberties Oversight Board – PCLOB, the authority supporting the USA executive in the preparation and implementation of counter-terroristic regulations that respect citizens freedom. In a report issued on 23 January 2014 and prepared in order to assess section 702 of the Patriot Act, the authors disclosed: "We were unable to recognize any cases of threads to the USA, in which the program would significantly influence a counter-

terroristic investigation, and: there is no case to support the view that the program has directly contributed to disclosing any unknown conspiracy or a terroristic attack" (the USA Privacy, Civil Rights and Civil Liberties Compliance Office, 2014, p.150). The members of the Office decided the program of mass metadata gathering not to have legal grounds and as such shall be terminated and the gathered data – deleted.

Similar opinion on the programs of data storage was expressed by William Binney, a former agent of the USA National Security Agency, who pointed that effective processing of emails, texts, and internet connection of over 4 billion people is rather impossible. "For such an action to make sense, one employee would have to control 200,000 people every day. Agents burdened with information resigned from the targeted analysis – the only way to discover the real danger – in order to search in a simpler manner using the key words. It gives a lot of meaningless shots instead of meaningful connections between them". (Siedlecka, Szymielewicz, 2015).

*T*he efficiency of American surveillance was also studied by the analytic center of New America Foundation. A report released on 13 January 2014 included a detailed analysis of 225 cases of individuals charged with terroristic activity in the USA and the methods used to open investigations. The experts decided that traditional means, such as criminal intelligence operations and cooperation with the informants, were sufficient to open the procedure in most of the cases. The input of surveillance programs in investigation openings had impact on 3.1% of the cases (of the USA citizens) and in 4.4% in cases of foreigners (Bergen, Sterman, Schneider, Cahall, 2016, p. 5).

On the Old Continent, the problem of validity of retention programs was brought up by the European Union. The evaluation report on the Retention Directive, prepared for the Council and the European Parliament, released on 18 April 2011, revealed a number of cases in which the data accessed from retention played a key role in the fight against organized crimes, including children's pornography, where data collected allowed to identify 178,000 users (out of 89 million controlled) who collected the paedophile content. (the European Commission, 2011, p. 29).

The day after the report of the European Commission was released, a coalition of 36 European non-governmental organizations called Euro-

pean Digital Rights created a shadow-report that resented quite different statistics. The research, commissioned by the German government (that did not implement the Retention Directive), underlined that among the sample of 1257 inquiries issued by the services to operators, only 4% could not have been realized due to the lack of data. This shows that in 96% of the cases collecting the data at the moment of capturing was sufficient. On the other hand, the Federal Criminal Police Office of Germany enclosed that the lack of retention data influenced 381 criminal charges in 2005 and 880 in 2010, which concerning 6 million of criminal investigations a year gives 0,001% of cases the data really influenced. Moreover, the data gathered by the authors of the report reflect that in 1/3 of the cases, despite the lack of telecommunications data, the legal proceedings were opened on the other grounds (European Digital Rights, 2016, p. 13).

CONCLUSION

The core of the problem concerning the fight against terrorism using the means of surveillance is of a multidimensional nature and its resolution cannot be found in any extreme standpoints. The protection of national interest cannot obscure the necessity of respecting citizens right to privacy and freedom of speech. On the other hand, the universal presumption of innocence in the contemporary geopolitical situation can lead to the escalation of terroristic actions. Quoting the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament: "Technical development is one of the factors influencing the crucial change in the model of action and operation of special services, that departed from the traditional concept of a targeted surveillance, being the necessary and proportionate counter-terrorism instrument and aimed at the systems of mass surveillance" (the European Parliament, the Committee on Civil Liberties, Justice and Home Affairs, 2014, p.2). Undoubtedly, controlling the communication of people accused of the state security harm is necessary, however, the mass data retention violates also the privacy of those citizens, who are not accused of any offences.

The question remains whether the control shall be preventive, that is to begin before any reasonable suspicion occur. The United States National Security Agency (NSA) answers that question: "Why do we gather your data? In the past the services started gathering information about a suspect after their identification, in order to collect evidence of their criminal activity. Nowadays, we gather all the available data on everybody to identify new targets" (The United States National Security Agency, 2016). The statement "new targets" seems to premise the suspicion of committing the offence, thus providing justification of monitoring citizens.

The analyses of the reports and data gathered by the author show that preventive data collection does not contribute to increase of police and other services efficiency in counter-terrorism struggle in an extend it infringes the grounds of open and democratic society functioning. The examples in which the information collected before had an important impact on the ongoing investigation do not allow to formulate a thesis that in case of their lack, the investigation would be impaired. Paraphrasing the shadow-report of the European Digital Rights – there is a great probability that plenty of cases in which telecommunications data was an important trigger for an investigation would be opened by the use of other measures. It is also supported by the overview of methods of investigation initiations created by the New America Foundation.

According to the author, the instrument of struggle with crime which reconciles the security and privacy issues is a quick freeze. In the given case the operators immediately, starting with the date of issuing the request by services, collect (freeze) the data of people suspect of criminal activity. The data is gathered without the anticipation for the court's decision, still, courts acceptance is necessary to be granted the data. The important feature of the quick freeze is the lack of preventive character of the means, it does not, however, relies to historic data.

Notwithstanding the model accepted, it is indispensable that Poland set new law regulations considering at the same time the right for privacy and the directives of the Court of Justice of the European Union and the Polish Constitutional Court. The most important issue, demanding an immediate intervention, is creating the mechanism of independent data control, governed by a public authority. The amendment to the Police Act

of 7 February 2016 resolves this issue only illusively. Instead of establishing an independent office to control data inquiries, 42 regional courts have been granted the authority. With over 2 million inquiries a year, we are provided with 50 000 cases a court. Thus, the profound control of the requests is impossible.

The Police Act does not regulate the matters of proportion in the usage of data and the duration of their storage. Concerning the first, it is vital to precisely determine the kind of crimes that validate the usage of retention information. For such, a catalogue of forbidden activities would be of a use, determining those actions that justify the breach of rights and freedoms of an individual. The present legislation does not provide any effective sensitive data protection, precluding them from the use for different purposes than those they had been disclosed for. Hence the necessary regulations shall be provided, obliging the services to store data only for the time of the investigation and demanding their immediate deletion after termination of the proceedings.

Thus prepared solutions would balance the issues of privacy and national security. Struggle with terrorism is an intricate process, entailing coordination of various elements: intelligence agencies, legislative solutions, social prevention as well as moral challenges. Renouncing the rules of freedom, that democratic societies are built upon, means in fact the triumph of terrorists.

BIBLIOGRAPHY:

Adamski, A. (2015). *Jawność i jej ograniczenia. Przeciwdziałanie przestępczości.* (vol. X.) Warszawa: C.H.Beck.

Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych (2016). *Your Data: If You Have Nothing to Hide, You Have Nothing to Fear.* Downloaded from: https://nsa.gov1.info/data/index.html#data.

Aleksandrowicz, T. (2015). *Terroryzm Międzynarodowy*. Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Bergen, P., Sterman, D., Schneider, E., Cahall, B. (2016*). Do NSA's Bulk Surveillance Programs Stop Terrorists?*. Downloaded from: https://static.newamerica.org/

attachments/4353-do-nsas-bulk-surveillance-programs-stop-terrorists-2/Bergen_NAF_NSA %20Surveillance_1_0_0.c7748e5bd84647fb8de43d3b664 961e9.pdf.

Boussios, E.G. (2016). *Termination or Accountability? The Controversy over the United States' Use of Cyberintelligence.* The Polish Quarterly of International Affairs, 2/2016. Downloaded from: https://www.pism.pl/publications/journals/The_Polish_Quarterly_of_International_Affais/2016/2.

Departament Skarbu USA (2016). *USA PATRIOT Act*. Downloaded from: https://www.fincen.gov/statutes_regs/patriot.

Flis, J., Jakubczak, R. (2006). *Bezpieczeństwo narodowe Polski w XXI wieku*. Warszawa: Wydawnictwo Bellona.

Fundacja Panoptykon (2016). *100 pytań o inwigilację do polskich władz*. Downloaded from: http://www.100pytan.org.pl/index.php.

Fundacja Panoptykon (2016). *Nadzór w telefonie.* Downloaded from: https://panoptykon.org/nadzor-w-telefonie.

Komisja Europejska (2011). *Sprawozdanie z oceny dyrektywy w sprawie zatrzymywania danych* (Dyrektywa 2006/24/WE). Downloaded from: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0225_/com_com(2011)0225_pl.pdf .

Obem, A., Szymielewicz, K. (2015). *Dane telekomunikacyjne: Karuzela liczb trwa, a problem nadal tkwi w złym prawie*. Downloaded from: https://panoptykon.org/wiadomosc/dane-telekomunikacyjne-karuzela-liczb-trwa-problem-nadal-tkwi-w-zlym-prawie.

Obem, A., Szymielewicz, K. (2014*). Snowden i Greenwald: Polskie władze współpracowały z NSA*. Downloaded from: https://panoptykon.org/wiadomosc/snowden-i-greenwald-polskie-wladze-wspolpracowaly-z-nsa.

Organizacja European Digital Rights (2011). *Shadow evaluation report on the Data Retention Directive (2006/24/EC).* Downloaded from: https://edri.org/files/shadow_drd_report_110417.pdf.

Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (2014). *Dokument roboczy Nr 1 w sprawie amerykańskich i unijnych programów nadzoru oraz ich wpływu na podstawowe prawa obywateli UE.* Downloaded from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7–2014–0139+0+DOC+XML+V0//PL .

Rada ds. Nadzoru nad Przestrzeganiem Prywatności i Praw Obywatelskich Stanów Zjednoczonych (2014). *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.* Downloaded from: https://www.pclob.gov/library/702-Report.pdf .

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection regulation).

Siedlecka, E., Szymielewicz, K. (2015). *Podsłuch rządzi strachem*. Downloaded from: http://wyborcza.pl/magazyn/1,145245,17924695,Podsluch_rzadzi_strachem.html.

Trybunał Konstytucyjny RP (2014). *Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. sygn. Akt K 23/11*. Downloaded from: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20140001055.

Świątkowska J. (2016). *Poland, the Czech Republic and NATO in Fragile Security Contexts. Lublin: IESW Reports*. Downloaded from: https://www.amo.cz/wp-content/uploads/2016/12/Poland-the-Czech-Republic-and-NATO-in-Fragile-Security-Contexts.pdf.

Wojciechowski, Ł. (2016). Information Security Policy as InfoSec instrument in the Polish local government system. Yearbook of the Institute of East-Central Europe. *Yearbook of the Institute of East-Central Europe 2016,* 14(2), pp. 75–94.