Adam Rogala-Lewicki

SECURITY SERVICES AFTER THE TERRORIST ATTACKS IN THE US AND EUROPE. PATRIOT ACT VERSUS THE RETENTION DIRECTIVE, OR THE LEGITIMISATION OF ABUSES IN THE SPHERE OF PRIVACY IN DEMOCRATIC STATES: A COMPARATIVE STUDY

Institutionally identified power using information products of its own services, in contrast to citizen, has historically had more available resources to obtain information from the surrounding. With the advancement of technology, individuals and consequently society have got emancipated enough to actively participate in the exchange of information and co-creation of information reality. Public and private sectors (with the dominance of the former or the latter depending on the period and the economic and state model of the country concerned[1]) have jointly generated a model of a global, digital, social regime, based on constant exchange of information.

Tools and institutions created on the basis of the order of state agencies or specialised private entities for the implementation of public tasks have been a driving force in the development of civilisation, every time inaugurating their application in the special use sphere and then, after the depreciation period, moving to the civilian everyday use space[2]. Modern technological, scientific or medical solutions can illustrate it. The Internet, which dates back

---

1 See more in Kołodko, G. 2013. *Wędrujący świat*. [*Wandering Word*.] Warszawa; Kołodko, G. 2013. *Dokąd zmierza świat. Ekonomia polityczna przyszłości*. [*Where the world is heading. The political economy of the future*.] Warszawa.

2 For example, advanced systems which are widely used in automotive serial production (e.g. ESP – Electronic Stability Program, or ABS – Anti-Lock Braking System) were initially introduced only in military and racing vehicles.

to the end of the 60s of the 20th century and is connected with the creation of the so-called ARPANET, was created as a result of the work of the American research organisation RAND Corporation looking for solutions to maintain leadership in the conditions of nuclear war[3].

In the public sphere technologically advanced systems for maintaining information advantage, and consequently also political superiority (in external terms – over international competition, in internal terms – over the private sector) remain under strict protection. The acceleration of technologisation processes and communication 'networking', and with it of social interaction, resulted in the change of the social, economic and political paradigm of the civilisational space. Professor Damir Črnčec classified this change by dividing the mentioned space in terms of time and subject. The specification is below (Chart 1).

Changing environmental conditions in broad terms, in the context of the competition for political influence, had to result in an even more refined form of reaction of the public sector. The need to anticipate threats necessitated the development and implementation of new technological solutions allowing state agencies to maintain and expand their information assets. For example, the US Echelon system designed with the participation of Great Britain, Canada, Australia and New Zealand is, *de facto*, a global eavesdropping tool tacitly accepted by the international community. The system was created under the so-called *AUSCANNZUKUS* agreement and is managed by the American National Security Agency, NSA. Elements of the Echelon system are installed in various parts of the world and equipped with technical devices to eavesdrop and intercept information transmitted through telecommunication channels. The architecture of the structure is programmed to collect and

[3] The first ideas to create an independent computer network crystallised in the 60s. Their culmination was the creation of ARPANET in the United States. A pioneering connection between computers in ARPANET took place exactly on 21 November 1969. From 1978 all devices equipped with modems could transmit and share data over telephone lines using the function *Bulletin Board Services* (BBS). On 1 January 1983 TCP/IP protocols were used in ARPANET. This moment is considered to be the beginning of the Internet. The first internationally joined network connected the United States, the United Kingdom and Norway. See more on this topic in Rothert, A. 2004. Technologia i demokracja. [Technology and Democracy.] In: Adamowski, J. ed. *Demokracja a nowe środki komunikacji społecznej*. [*Democracy and new means of social communication*.] Warszawa, pp. 37–53; Bendyk, E. 2011. Świat w pajęczynie. [The world in a spider's web.] *Niezbędnik Inteligenta, Cywilizacja 2.0 Świat po rewolucji informatycznej*. [*The Intelligent's essentials, Civilisation 2.0 the World after the information revolution.*] *Polityka*, Special edition, no. 8, pp. 15–17.

analyze data transfers. Any electromagnetic beam of information transferred anywhere in the world (as a fax, e-mail or phone call) can be intercepted. All intercepted data go to the headquarters in Fort Meade in the US, where they are then selected, categorised and compressed in algorithmic, linguistic and thematic terms. The platform processes and collects billions of electronic communications per day. It is estimated that at the beginning of the 20th century the system was able to intercept approximately 3 billion electronic information transfers per 24 hours[4].

Chart 1

The paradigm of the civilisational change

COLD WAR PERIOD			21st CENTURY
Technological change	Gradual	□	Very fast
Geopolitical environment	Familiar	□	Unpredictable/dynamic
Budget/people	Ample	□	Limited
Organisational structure	Hierarchical	□	Flattened, liquid, flexible
Non-core functions	Internal	□	Outsourcing
Work environment	dedicated	□	Virtual, network
Employee mobility	30 years	□	3–5 years
Risk taking	Avoidance	□	Management
Environmental awareness	Low	□	Growing
Personnel security	Narrow	□	Expanded
Cooperation	Incidental	□	Necessary

Source: Črnčec, D. 2009. A new intelligence paradigm and the European Union. *Journal of Criminal Justice and Security*, no. 1, p.152.

In 2013 the information that the same agency also uses other tools for electronic surveillance on a mass scale leaked to the public space. Edward Snowden, a former agent of the Central Intelligence Agency, CIA (cooperating with the company Booz Allen Hamilton – a subcontractor of NSA), having the access clause to top secret information, decided to become a so-called whistleblower, that is a denouncer. He grabbed international attention by revealing thousands of classified documents. The most interesting of them unmasked a spy program called PRISM[5], whose name does not appear to be

[4] European Parliament. 2001. *Temporary Committee on the ECHELON Interception System: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*, [2001/2098 (INI)], 11 July 2001.

[5] In May 2013 Edward Snowden met reporters Glenn Greenwald and Laura Poitras in Hong Kong and revealed some of the most top secret documents protected by the US

an acronym but a code name of its own. The disclosed materials reveal that PRISM is a telecommunications platform for data acquisition and handling launched in 2007 by the US NSA and the UK Government Communications Headquarters (GCHQ)[6]. The program handles information supplied by commercial entities cooperating with the agency, including, among other, such eminencies of the Internet industry as Microsoft, Yahoo Inc., Google, Facebook, AVM Software (the administrator of Paltalk), YouTube, Skype, AOL, and Apple Inc. These companies have committed themselves to sharing data stored on servers, disks, file transfers, those transmitted through the so-called Internet telephony (VoIP), video conferencing, chats, all the information collected on social networking sites and logins. PRISM operates on the basis of the so-called categorizing keywords. When the required phrase is found, the 'record' automatically goes 'to the desk' of the agent supervising the program.

For those interested in the functioning of special services this type of media reports are not surprising. The cell responsible for the information security of the USA, the above mentioned National Security Agency, the task of which is to intercept information relevant for the interests of the state by means of all possible channels (radio communications, telephone, computer), in fact, has been permanently spying on its own citizens for years. Already in the 60s it came to light that it had all recordings of telephone conversations in the USA. Even US President Harry S. Truman's regulation from 1952 bringing the NSA into life was top secret. Even today the statute of the Agency is secret, due to which an American citizen does not know to what extent it interferes in his private life[7]. Similarly, other agencies in democratic

---

intelligence services. The information provided by Snowden was published by American *the Washington Post* on 6 June 2013 and British *the Guardian* on 7 June 2013.

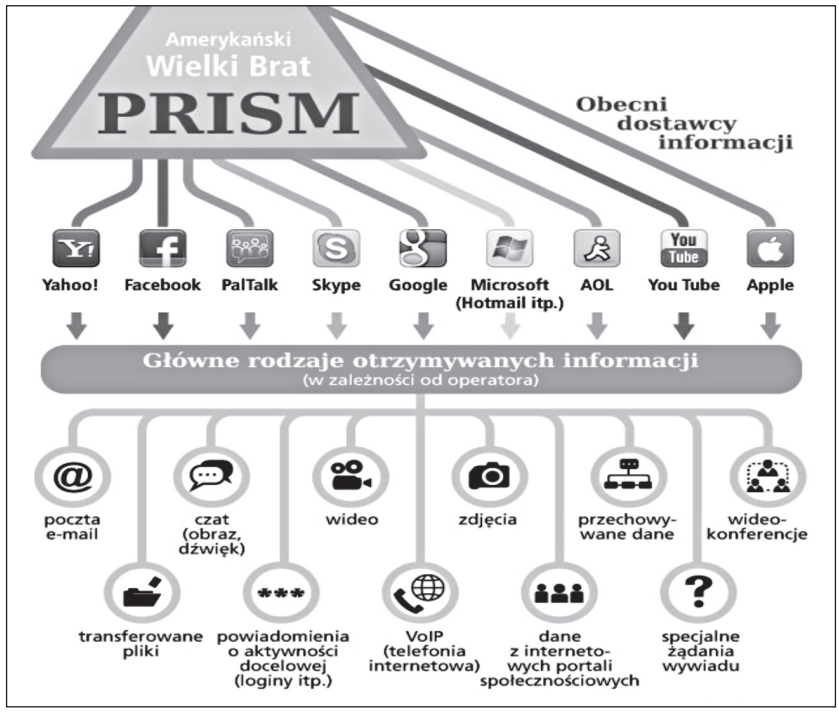
6 In the case of special services of the USA and the UK we can speak not only about the long-term, historically established close cooperation but even about the intelligence community. See Podolski, A. 2004. *Europejska współpraca wywiadowcza – brakujące ogniwo europejskiej polityki zagranicznej i bezpieczeństwa?* [*European intelligence cooperation – a missing link of European foreign and security policy*?] Warszawa: Centrum Stosunków Międzynarodowych, Raporty i Analizy no. 10, p. 1.

7 For many years, NSA employees and their family members when asked about the place of work were not authorised to use the name of the employer. The obligatory response was the employment in the US Department of Defence (DoD). Although today this ban is no longer applicable, the agency employees are bound by a number of restrictions. For instance, they are obliged to use help of only these dentists who are approved by the NSA protection bureau. Moreover, they have to inform about the people they enter into relations with or about every foreign trip. Such forms of security

legal states, which nominally strictly respect human rights, have taken care of their information work comfort. The motto – know everything, take care of the information advantage – guides all intelligence agencies[8].

Chart 2

Probable PRISM system architecture



Source: Koziej, S. Obywatele są bezbronni wobec zagrożeń takich jak PRISM. [Citizens are defenceless in the face of threats such as PRISM.] *Polska Agencja Prasowa* [Online]. Available at: http://wiadomosci.wp.pl/kat,1342,title,Stanislaw-Koziej-obywatele-sa-bezbronni-wobec-zagrozen-takich-jak-PRISM,wid,15741432,wiadomosc.html?ticaid=1127d3&_ticrsn=5; [Accessed: 7 July 2014].

and secrecy have led to the fact that over time the agency has acquired a grotesque acronyms – No Such Agency.

8 It is enough to mention, among others, Secret Service (former MI5), Government Communications Headquarters (GCHQ), Defence Intelligence Service (DIS) in the UK, *Bundesamt für Verfassungsschutz* (BfV) – (The Federal Office for the Protection of the Constitution), *Bundesnachrichtendienst* – BND (The Federal Intelligence Service) in Germany, *Direction Centrale du Renseignement Interieur* – DCRI (Central Directorate of Internal Intelligence), former *Direction de la Surveillance du Territoire* (Directorate of Territorial Surveillance) and *Direction Centrale des Renseignements Généraux* (Central Directorate of General Intelligence) in France.

In the US the legal basis for such a significant invasion of privacy is, among others, section 702 of the Foreign Intelligence Surveillance Act of 1978. The provisions were designed for obtaining intelligence information from abroad. According to the Act, intelligence activities cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States. In fact, the act legalises all 'eavesdropping' activities of the services. Although the activities carried out under Section 702 are subject to control by the United States Foreign Intelligence Surveillance Court, the executive and the Congress of the United States – there is common general acquiescence to abuse. The knowledge which the services have is, in fact, very dangerous also for these authorities, for which these services work and which nominally control their activities. The power that comes from this knowledge allows the services to actively participate in the so-called political games. Sabotaging decisions of the organs of power, curving vectors of political reality in order to achieve their own interests (often private ones) is not uncommon. The perspective of the amount of different, often competing services, completes the picture of the situation[9].

[9] In the presence of a number of special service institutions in the country, there is the problem of their rivalry and coordination of their activities. For instance, in the USA the service system consists of the following organisations: CIA (Central Intelligence Agency), DIA (Defence Intelligence Agency), NSA (National Security Agency), FBI (Federal Bureau of Investigation), AFOSI (Air Force Office of Special Investigations), NCIS (Naval Criminal Investigative Service), CGIS (Coast Guard Investigative Service), USACIC (United States Army Criminal Investigation Command), as well as offices dealing with intelligence in the Departments of Defense, State, State Security and various institutions at the state level (not counting private intelligence agencies). In Poland currently the following services operate: AW (the Foreign Intelligence Agency), ABW (the Internal Security Agency), SWW (Military Intelligence Service), CBA (the Central Anti-Corruption Bureau), CBŚ (the Central Investigation Bureau), as well as the information offices of the Police, State Border Service, Military Police, Customs Service and other. See Davis, P. H. J. 2010. Intelligence and the machinery of government: conceptualizing the intelligence community. *Public Policy and Administration*. no. 25 (29); Flanagan, S. J. 1985. Managing the Intelligence Community. *International Security*. vol. 10, no. 1, pp. 58–95; Omand, D. 2010. Creating intelligence communities. *Public Policy and Administration*. no. 25 (99); Rogala-Lewicki, A. *Czy polskie służby specjalne potrzebują formuły Intelligence Community*. [*Do Polish special services need formulas of Intelligence Community*?] Forum Studiów i Analiz Politycznych im. Maurycego Mochnackiego. [ISSN 2082-7997] Available at: http://www.fsap.pl/index.php?option=com_content&view=article&id=21%3Aczy-polskie-suby-specjalne-potrzebuj-formuy-intelligence-community&catid=7%3Acomments&Itemid=9&lang=pl [Accessed: 7 May 2014].

The realities outlined above do not interfere with the rules on access to public information and protection of personal data which are binding in these countries and which are the foundation of free democracies[10]. While the Foreign Intelligence Surveillance Act (signed by President Carter) opened the normative door to legalizing surveillance ajar, the US legislation adopted after the terrorist attacks on the World Trade Centre and the Pentagon on 11 September 2001, opened it wide. Already on 26 October 2001[11] the Congress enacted[12] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, that is the so-called Patriot Act, which increased the powers of all state

[10] Currently almost 100 countries around the world have laws guaranteeing access to public information (freedom of information legislation). The first act was adopted in Sweden in 1766 (Sweden's Freedom of the Press Act of 1766) and it is the oldest example of this type of legislatives. Scandinavian countries are considered to be the cradle of transparency of public space. In the USA the Freedom of Information Act (FOIA) was introduced by the administration of President Lyndon B. Johnson and entered into force w1967. Transparency in the US also is supported by other laws: The Privacy Act of 1974, Electronic Freedom of Information Act of 1996, The Intelligence Authorisation Act of 2002, OPEN Government Act of 2007, Wall Street Reform Act of 2010. On the territory of the European Union, issues of access to information at the disposal of bodies are regulated by: Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents (Official Journal L 145 of 31.05.2001) and Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (Official Journal L 345 of 31.12.2003).

[11] Critics of the Act point out that such a quick adoption of the Patriot Act was only possible if the document that counts 132 pages had been already prepared. Many commentators of political life in the United States pointed out that in the act in a draft version had been lying frozen on the legislative desk waiting for the right time justifying voting on it. Even worse shadow fell on the act after the release of the controversial film *Fahrenheit 9/11* by Michael Moore. It turned out that none of the senators had made an attempt to read the act before the vote. In one of the scenes in the film congressman John Conyers unscrupulously explains that parliamentarians do not read most of the adopted acts. He justifies it with the fact that otherwise the legislative path would extend dramatically over time. Director Michael Moore, to visualise the banality of the forms of law adoption in the United States, which may result in serious consequences, decided to inform citizens in a mocking form about the content of the Patriot Act. Namely, he hired an ice cream selling vehicle from which with the help of a megaphone he read the contents of the Patriot Act to the residents of Washington (including passing congressmen and senators).

[12] The act was passed by the lower house (Congress) by 357 votes to 66 and in the Senate by 98 to 1 and was supported by both the Republican Party and the Democrats. The only senator who voted against the entry into force of the act was Russ Feingold.

institutions caring for public order and safety. The attacks were not only a shock for the public, but turned out to be a surprise also for services. The humiliation of these formations forced the US legislature to verify the powers and tools at its disposal[13]. The events of 11 September and the necessity to combat terrorism became the clause justifying the expansion of the range of surveillance tools. The service felt political patronage liberating them from the constraints of democratic oversight and control.

Patriot Act

Since its entry into force the act has been the subject of criticism. It contains many extremely controversial provisions, dangerous from the point of view of preserving the right to privacy. John A.E. Vervaele, professor of penal-fiscal and economic law at the University of Utrecht and professor of European criminal law at the Europa College in Bruges, identified three areas of change that the patriotic act legalised. 'First of all, it has to be emphasised that the Patriot Act has considerably expanded the regular powers of investigation, especially in the field of electronic and digital surveillance, while at the same time it has weakened judicial control. Secondly, the Patriot Act has ensured that FISA security criminal law can be used on a much wider scale. Before the Patriot Act, a primary purpose standard had to be met. FISA was only allowed for primary foreign intelligence purposes. The Patriot Act has made it sufficient that the purpose is significant. It is allowed to pursue investigative purposes, as long as a significant purpose of the surveillance is to obtain foreign intelligence information. Thirdly, the Patriot Act has opened up the flow of information from the LEC to the IC and vice versa by breaking down the existing legal dividing wall'[14].

The author uses abbreviations: LEC, IC, FISA having in mind respectively – Law Enforcement Communities, Intelligence Communities and the aforementioned Foreign Intelligence Surveillance Act of 1978. In the Anglo-Saxon terminology the first term combines all the investigative authorities taking care of public order and security with the exception of special services

---

13 Cf. Desai, U., Crow, M.M. 1983. Failures of power and intelligence: use of scientific-technical information in government decision making. *Administration & Society* no. 15 (185).

14 Vervaele, J.A.E. 2005. Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law. *Utrecht Law Review* 2005, vol. 1, no 1, p. 8.

to which the second term applies. The third abbreviation is both the name of the legal act and in the operation language it is a synonym of electronic surveillance.

Before the entry into force of the Patriot Act, operational control in the area of communication was entrenched with restrictions[15], the investigation sector was separated from intelligence by an information barrier. The systemic difference between Law Enforcement Communities and Intelligence Communities, implicitly between law enforcement and intelligence and counterintelligence, lay in the realm of the matter of realised tasks. Intelligence in the first place is more interested in detecting threats to the regime and the essential interests of the state, while the police performs its criminal and preventive function. In short, in the world of law enforcement there is less politics and more everyday crime detection, while in the world of services there is just as much everyday threat detection, but mostly of the political colour. The historical dividing line ran along a changing path. In authoritarian systems, the police has been an armed wing of the political authority and a guarantor of its survival. John A.E. Vervaele presents a historical outline. 'Nevertheless, the historical distinction has to be viewed in perspective, as both the intelligence services and the police services are not ancient institutions and furthermore their relatively young existence has been politically marked. The turbulent political developments explain the differences in the relationship between intelligence and police services in the US and Europe. In Europe, the experience with the totalitarian regimes and their political police forces in Nazi Germany, in Russia, etc. has greatly influenced the organisation after WW II. The intelligence services went back to being separate organisations with their own statute'[16].

While the above-described structural distinction on the European continent is already fixed, in the United States the matter is not so clear-cut. The evolution of the security system in this country has led to a situation where

[15] Legal protection of citizens against surveillance in the American system was introduced by the High Court on the basis of the fourth amendment to the Constitution and the enforcement clause. In the case Katz v. Unites States the court decided that a warrant is required for eavesdropping, unless it is a matter of national security. In the case of Berger v. New York the court found that the warrant authorizing wiretapping must specify precisely the objective, method and duration. Conditions for obtaining a warrant are strictly defined in the regulations, and services in order to get one must show the so-called probable clause which proves that committing or an intention to commit a crime is probable.

[16] Vervaele, J.A.E. *op. cit.*, p. 4.

most of the institutions belonging either to the realm of Law Enforcement Communities, or Intelligence Communities in fact operate partly in one and the other. It was President Roosevelt who decided to extend the competence of the US Federal Bureau of Investigation (FBI) from the classic police to federal-police and federal-intelligence. Later the same formation was retrofitted with the possibility of action in the case of tasks, the effects of which go beyond the country's borders. This meant, in fact, the entry into the space previously reserved exclusively for the Central Intelligence Agency which has been established exactly for this purpose. Paradoxically, this task interchangeability does not mean perfect cooperation. In the framework of one state there are different procedures and methods of operation. It is obvious that the space of Intelligence Community is much more susceptible to the direct executive regulation coming from the president (including the less formal ones).

The difference between the European and American model settles on the way of transferring and using information. Different standards apply to the information to be used for national security purposes (e.g. in connection with counter-terrorism) and information used in the criminal procedure[17]. Before the entry into force of the Patriot Act, the transfer of information from the Intelligence Communities to the realm of Law Enforcement Communities took place on the basis of the so-called minimisation procedure which restricted the use of the information to the necessary degree. 'Minimisation aims to limit the acquisition, retention and dissemination of information concerning US citizens as much as possible. Only where such information is really crucial may it be stored. It is used only in the case of criminal offences which have been committed, are being committed or may be committed. are exempted from minimisation. (…) A classic component of minimisation is the information-screening wall. An official from the Department of Justice screens the FISA intelligence and only selects the parts that are relevant as evidence'[18]. Even when a piece of information leaked from one organisation to another, it was most often formatted in such a way that it was not possible to freely associate it with another plot, in another case. Additional restrictions were the result of a memorandum of 1995 of the then Attorney General

[17] The American nomenclature order distinguishes intelligence not only in the meaning of intelligence agencies, but also in the sense of activity that goes beyond the understanding of information. Intelligence is therefore something beyond, more sophisticated than information. See Freeman, O. 1999. Competitor intelligence: information or intelligence? *Business Information Review*, no. 16 (71).

[18] Vervaele, J.A.E. *op. cit.*, p. 6.

Janet Reno, which specified 'the procedures for contacts between the FBI and the Criminal Division concerning foreign intelligence and foreign counterintelligence investigations'[19]. Already the first paragraphs banned any direct exchange of information between Intelligence Communities and Law Enforcement Communities without the participation of the Assistant Attorney General for the Criminal Division. This person was a kind of interface connecting the two divisions, although sometimes they held offices in the same building.

Given how far the intelligence and investigation divisions were from each other from the communications point of view, and how long the coordination procedure was, the American model of information exchange went through a real revolution with the enactment of the Patriot Act. The Patriot Act enforced a reorganisation in the approach to the information management in the entire security system. The blame for ineffective prevention and consequently the occurrence of the terrorist attacks fell to the services. Intelligence had full details about the terrorists, but was unable to transfer them to the right place at the right time. The dysfunction resulting from the need to use every time the intermediation of another cell paralyzed the exchange of information between Law Enforcement Communities and Intelligence Communities. The aim of the Act was to cross this wall.[20] It turned out that the Act, extending general competences of American security organs, 'by the way' legalised uncontrolled surveillance. It also increased funding (a fund for financing the fight against terrorism was established) and substantially extended the scope of the operation of the National Electronic Crime Task Force Initiative[21].

The authors of the law began raising the operational powers by trying to define the boundaries of terrorist activity. Firstly, a whole list of new

---

19 *Memorandum of Attorney General (Janet Reno) to Assistant Attorney General, Criminal Division Director, FBI Counsel for Intelligence Policy United States Attorneys*. 19 June 1995. Available at: http://epic.org/privacy/terrorism/fisa/ag_1995_mem.html [Accessed: 21 January 2015].

20 The Patriot Act in addition to the standards explicitly assigned to the new law contained provisions which amended, among others, the Foreign Intelligence Surveillance Act of 1978 (FISA), the Electronic Communications Privacy Act of 1986 (ECPA), the Money Laundering Control Act of 1986, the Bank Secrecy Act (BSA), as well as the Immigration and Nationality Act (INA) of 1965.

21 See section 105 of the Patriot Act. The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

offences was added to the existing catalogue of terrorist acts[22]. Secondly, it introduced a very broad category of domestic terrorism crimes. In addition to the actions of 'mass destruction, killings and kidnappings' which then became domestic terrorism, activities dangerous to 'human life and the civilian population' were also considered a terrorist act. A state authority determines whether a given activity is actually dangerous. The final catalogue

[22] See the following sections of the Patriot Act: 32 destruction of aircraft facilities, 37 violence at international airports), 81 arson within special maritime and territorial jurisdiction, 175, 175b biological weapons, 229 chemical weapons, subsections (a), (b), (c), (d) and section 351 congressional, cabinet, and Supreme Court assassination and kidnapping, 831 nuclear materials, 842(m)(n) plastic explosives, 844(f)(2)(3) arson and bombing of Government property risking or causing death), 844(i) arson and bombing of property used in interstate commerce, 930(c) killing or attempted killing during an attack on a Federal facility with a dangerous weapon, 956(a)(1) conspiracy to murder, kidnap, or maim persons abroad, 1030(a)(1) protection of computers, 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through (v) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnapping), 1992 (relating to wrecking trains), 1993 (relating to terrorist attacks and other acts of violence against mass transportation systems), 2155 (relating to destruction of national defense materials, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organisations), or 2340A (relating to torture) of this title; (ii) section 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2284); or (iii) section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with a dangerous weapon), section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life by means of weapons, on aircraft), section 46506 if homicide or attempted homicide is involved (relating to application of certain criminal laws to acts on aircraft), or section 60123(b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49. See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism – USA Patriot Act, H. R. 3162*, (Public Law 107-56). Available at: http://epic.org/privacy/terrorism/hr3162.html [Accessed: 9 March 2015].

of forbidden acts, the commitment of which identifies the perpetrator as a terrorist is impressive. The intention is easy to understand. The broader the index of terrorist acts, the greater the freedom of services' work. They can immediately proceed in an extraordinary way, provided for terrorist threats[23]. The most controversial legal norms allowed the surveillance of persons connected with terrorist activities. Even a slightest suspicion of carrying out such an activity is sufficient to start the process of clandestine surveillance. The most dangerous turned out to be three operating methods: blank search and detention warrants (sneak and peek and library records), secret surveillance of persons not registered in the US and not affiliated to international organisations (a lone wolf), and the so-called roving wiretaps[24].

The first of the mentioned methods (sections 213 and 215 of the Act) allows to obtain any materials relevant to the investigation even if they are not 'connected' with the suspects. This provision is contrary to the established concepts of legal search and seizure which require the demonstration of a reasonable suspicion or probable cause of the relationship of one to the other. Presentation of the detention order of a specific thing (on the basis of the issued National Security Letter, NSL[25] to the person concerned was regulated in the so-called flexible standard, that is giving such an order within an unspecified period of time. This specific mode of postponing the formal disclosure of surveillance may last for years due to the possibility of extending the period of the order validity[26].

---

[23] New sanctions and penalties were also introduced. For example, for the crime of bringing the threat to mass transport means the penalty of 20 years imprisonment was provided if the mass transportation vehicle was empty, and life imprisonment if the mass transportation vehicle was carrying a passenger. See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism – USA Patriot Act, H. R. 3162* (Public Law 107-56). Available at: http://epic.org/privacy/terrorism/hr3162.html [Accessed: 9 March 2015].

[24] See *Reform the Patriot Act*. Available at: https://www.aclu.org/reform-patriot-act [Accessed: 1 March 2015].

[25] According to the Department of Justice on the average tens of thousands of National Security Letters (NSL), allowing for reading e-mails, eavesdropping conversations, viewing bank statements without a court order are issued each year for anti-terrorist investigations often in the case of people who have already been cleared of the charges.

[26] The formula of 'sneak and peek' was questioned by Judge Ann Aiken in the judgment of 26 September 2007 in the process of Brandon Mayfield unjustly arrested and imprisoned, whose incriminating evidence had been obtained by means of this method. The court ruled that this formula of gaining information about citizens is inconsistent with the Fourth Amendment to the US Constitution.

The second method (section 6001) also goes far beyond the framework of institutions legally recognised in democratic countries, because it unifies the possibility of clandestine surveillance of foreigners who are not accused of any charges, that is of persons over whom no US institutions have any legal sovereignty. Defenders of this approach assert that it is directed only to the so-called lone wolves, that is people engaged in one of the deadliest forms of terrorism.

The third type of covert acquisition of information (roving wiretaps), as described in Section 206 of the Act, results in the possibility of issuing permits for carrying out operational activities without specifying their scope (without indication of a person or object in the order) – which is a construction unprecedented in any state of law. Traditional warrants must always indicate the reason for conducting discreet surveillance and identify the object or the subject of surveillance. The roving wiretapping allows services to continue operations without the need to obtain new (updated) warrants, when 'the target' changes and uses a variety of tools of information transfer. The Department of Justice protects this solution, claiming that terrorists bypass traditional eavesdropping by constantly changing locations and devices by means of which they communicate.

All operating methods can be used in the absence of an individually defined target – which is a denial of legally conducted criminal proceedings. Services may be allowed to do so only on the basis of probable evidence of the occurrence of a specific threat (e.g. related to the specific environment of people) who, according to the body, are relevant for anti-terrorist proceedings. A service may see these traces (patterns) everywhere and in everyone. Opponents, not without a reason, see this as an insult to the Fourth Amendment to the US Constitution[27].

Moreover, section 203 of the Act introduced legislation amending the investigation procedure and removed barriers to the flow of information between intelligence Communities and Law Enforcement Communities. 'Any investigative or law enforcement officer, or attorney for the Government, who by any means authorised by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence

[27] The Fourth Amendment of the U.S. Constitution provides the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seised. See the U.S. Constitution Available at: http://libr.sejm.gov.pl/bibl/ [Accessed: 9 September 2014].

derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, or counterintelligence unit'[28]. A possibility of free transfer of information by investigating authorities to special services was introduced, including information obtained covertly. All of this without any authorisation or court supervision. Section 504 of the Act in the same way regulated the issues of information flow in the opposite direction, i.e. from special services to investigating authorities. The reigns of the new provisions completely disposed of the procedural information wall (screening wall). 'FISA surveillance means may be freely used for a law enforcement purpose. The former dichotomy between the IC and the LEC is history'[29]. The regulations allow for the almost wholesale collection of information on suspects – and that is regardless of their citizenship. The Patriot Act also provides for a necessity to disclose various types of information transmitted through electronic channels. Operators are obliged to provide data not only about the name of the recipient, his/her address, phone records, telephone number, duration of the service, but also the length of calls, the type of services used, IP address, method of payment, account and a bank card number. You can see the unlimited field for misuse.

The most far-reaching provisions of the Patriot Act, legalizing the most invasive operating methods, were supposed to be in force periodically until the extinguishment of the terrorist threat. The temporary period was introduced for sections 206, 215 and 6001 of the Act (sneak and peek, library records, roving John Doe wiretap, lone wolf). Meanwhile, in July 2005, the Senate passed a draft of the re-authorizing act USA PATRIOT and Terrorism Prevention Reauthorisation Act of 2005, which not only modified the most controversial provisions, maintaining other in force, but has also introduced new solutions. However, President George W. Bush signed a version of the law proposed by Congress of 2 March 2006 USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006. On 25 February 2010, in response to the re-expiring period of validity, the Congress passed the extension of the most controversial operational solutions, despite the ongoing discussion on

[28] Section 203 of the Patriot Act, H. R. 3162, (Public Law 107-56). Available at: http://epic.org/privacy/terrorism/hr3162.html [Accessed: 9 September 2014]. See also point (d) of section 203 Foreign Intelligence Information. (It shall be lawful for foreign intelligence or counterintelligence or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties).

[29] Vervaele, J.A.E. *op. cit.*, p. 11.

their amendments. President Barack Obama signed the prolongation twice, the last, four-year one on 26 May 2011 (the number of votes in the House of Representatives 250 to 153 and in the Senate 72 to 23). The Patriot Act was supposed to be a response to attacks by equipping security forces with the tools to conduct battles during the war. That is why, the Act provided the solutions which are unsuitable for peacetime. Meanwhile, two years after its adoption, a new draft, prepared by Attorney General John Ashcroft, was ready, which, *nomen omen,* provided even more far-reaching competencies. The solutions were so controversial that work on the project was classified. After their content was revealed to the public they were completely frozen[30].

Data retention

The problem of breaking the rules of privacy protection is a global problem plaguing countries with various political regimes. Poland is also not an exception in this group. A report prepared by the Commission on Human

[30] At the beginning of 2003 copy of a draft law prepared by the administration of President George W. Bush leaked to the US media. It was to go a step further in relation to the solutions binding under the Patriot Act. The draft, called the Domestic Security Enhancement Act of 2003, was quickly hailed as the 'second Patriot Act' or 'the son of the Patriot Act'. 10 divisions of the Department of Justice took part in the work on the draft. The draft itself provided solutions such as: (a) the removal of injunctions regarding spying on domestic entities by federal agencies, (b) obtaining authorisation by the Federal Bureau of Investigation to conduct external investigations based on intelligence information without obtaining court approval, (c) the creation of a DNA database of suspected terrorists, (d) the prohibition of any public disclosure of the names of tracked terrorists, including those who have been arrested, (e) exemption from civil liability for individuals and companies which voluntarily provide information to investigative agencies, (f) criminalisation of the civil use of encryption in communication, (g) the reversal of the burden of proof to refuse bail for persons accused of crimes related to terrorism, in such a way that persons accused of terrorism would be required to demonstrate reasons why they should be released on bail, (h) the expansion of the list of crimes subject to death penalty, (i) the exemption of the Environmental Protection Agency from the obligation to disclose the data on emergency situations related to chemical plants, (j) the introduction of the possibility of the granted citizenship revocation and deportation of US citizens providing support to terrorist groups. Available at: http://www-tc.pbs.org/now/politics/patriot2-hi.pdf; http://www.prisonplanet.com/analysis_newsom_021003_patriot.html,http://www.pbs.org/now/politics/lewis.html, http://www.sourcewatch.org/index.php/Patriot_Act_II [Accessed: 2 March 2015].

Rights at the Polish Bar Council, published in spring 2011, reveals that the police, security services and other government investigative cells reach for the private data of citizens often without any external supervision, including in particular judicial control. Statistical data expose the truth about officers who routinely take unfair advantage of the privileges. On the basis of the report it can be concluded that monitoring and recording of conversations 'for obvious reasons, in the vast majority of cases happens without the knowledge and consent of the intercepted persons. For this reason, in spite of the prior judicial supervision of the application of this measure, they have no opportunity to influence the decision on its application or present their arguments. The monitoring and recording of telephone conversations must be subject to particular restrictions in the course of criminal proceedings. (…) In the doctrine there are frequent voices acknowledging that the existing measures of supervision of law enforcement authorities are insufficient in this regard'[31]. Governmental acts containing operational competencies exclude the obligation to obtain a court approval for acquiring retention data, i.e. the data referred to in Art. 180c and 180d of the Act of 16 July 2004 – The Telecommunications Law[32], and identifying the beneficiary of postal services and pertaining to the circumstances of postal services or using these services.

The greatest controversy accompanies the regulations on access to phone records. The content of the legal standards applicable to the retention, storage and transmission of telecommunications data to services is particularly unfavourable from the point of view of privacy protection and remains the subject of the greatest concern. According to data from the European Commission, in 2010 Polish services applied more than a million times to telecom operators for the data of their customers (phone records), which places Poland at the top of the rankings[33]. In early 2011 the press announced these data in an alarming tone. 'Poland is the EU leader in obtaining our

[31] *Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli* – Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej. [The report of the Commission on Human Rights at the Polish Bar Council. *Data retention: concern for security or surveillance of citizens.*] Available at: http://archiwum.adwokatura.pl/?p=3566 [Accessed: 4 April 2014].

[32] Journal of Laws No. 171, item 1800, as amended.

[33] See Siedlecka, E. KE: Za dużo podglądacie. [The EC: you are spying too much.] *Gazeta Wyborcza* [Online] Available at: http://wyborcza.pl/1,75478,9453157,KE__Za_duzo_podgladacie.html [Accessed: 15 August 2014]. In the middle of 2012 the period of keeping the retention data was shortened to one year. See more in Bazański, Ł. Retencja danych oraz nowe obowiązki ISP w zakresie danych osobowych. [Data retention and new responsibilities of ISPs in the field of personal data.] [Online]

data from telephone operators by services, the police and the judiciary. (…) Annually, without any control they collected phone records, subscriber data and data on the movement of phone owners (BTS) 1 million 60 thousand times. That means 27.5 thousand checks per one thousand of adult Poles. The Czech Republic, second in the rating, had 10 checks. Great Britain and France – approximately 8.5, Germany – 0.2 per one thousand inhabitants (35 times fewer than in Poland)'[34].

In European law, in fact, we are dealing with a gap. Services take a shortcut and instead of submitting a reasoned application to the courts for permission to install wiretapping, turn to telecommunications providers asking for data. They concern such a long period and are so suggestive that they able to create a psychological and economic portrait of the given person.[35] 'Gaining information about with whom and at what time we talked

---

Available at: http://www.kike.pl/2013/02/28/retencja-danych-oraz-nowe-obowiazki-isp-w-zakresie-danych-osobowych/ [Accessed: 4 March 2015).

[34] Siedlecka, E. 2011. Służby zdradzają, jak często sięgały po bilingi. [Services reveal how often they reached for phone records.] *Gazeta Wyborcza* [Online] 10 February 2011, p. 6. Available at: http://wyborcza.pl/1,75478,9081579,Sluzby_zdradzaja__jak_czesto_siegaly_po_billingi.html#ixzz1TgKmikgS, [Accessed: 15 August 2014]. The then Secretary of the College for Special Services – Jacek Cichocki – gathered information on the amount of covertly collected data and their types. Although, among others, the police with the Central Investigation Bureau did not provide statistics, after analyzing the others, it turned out that the prosecutor's office, courts and police amount for 56% of total checks. The Border Guard (15% of all checks), the Internal Security Agency (13% of all checks), Military Counter-intelligence (11%), the Central Anticorruption Bureau (4%) and fiscal intelligence (1%). Cf. Siedlecka, E. 2011. Kogo można podsłuchać. [Who can be eavesdropped.] *Gazeta Wyborcza* 15 March 2011, p .7; Siedlecka, E. 2011. Służby zdradzają, jak często sięgały po bilingi. [Services reveal how often they reached for phone records.] *Gazeta Wyborcza* 10 February 2011, p. 6; Nisztor, P. Polacy pod kontrolą służb. [Poles under the control of the services.] *Rzeczpospolita*, no. 116 (8932), p. 1.

[35] The irregularities in this field have repeatedly been the subject of interest of the Ombudsman, whose interests concentrate on all violations of fundamental rights and freedoms. In this situation, the activities of police and special forces caused the danger of tearing the integrity of the right to privacy, and within it, the right to freedom and secrecy of communication. In his letter to the Prime Minister dated 1 April 2008 (Letter, RPO-578577-II / 08 / PS), the Ombudsman pointed out that the problem of operational activity of authorised bodies, including in particular special services, remains under his constant observation. The Ombudsman's interest in the question of operational control, understood as a covert activity of controlling the contents of correspondence, contents of parcels, obtaining and recording the content of telephone conversations and other information transmitted via telecommunications networks,

is the same invasion of privacy as wiretapping. Sometimes it is even more serious. Are we undergoing a psychiatric treatment? Do we have a lover? Do we visit certain places? Access to telecommunications data facilitates answers to such questions'. As Mikołaj Pietrzak, Chairman of the Commission on Human Rights at the Polish Bar Council, notes 'the problem is that while services have to obtain the consent of the court to use wiretapping, they have access to phone records at their sole discretion'[36]. It should be noted that the issue of data retention does not pertain only to phone records because it concerns also 'all the information necessary to determine who, where, when, with whom and how got connected or tried to connect by telephone. In this way no only the phone number is identified but also the time of the call, a relay station, within the range of which both the caller and the recipient were, which allows to determine the location of the person'[37].

The Act of Telecommunications Law provides that the operator and provider of telecommunications services are obliged at their own expense to: (1) retain and store data generated or processed in a communications network for 24 months, (2) make the data available to authorised entities, including the court and the public prosecutor and (3) protect the data from accidental or unlawful destruction, loss or alteration, unauthorised or unlawful storage, processing[38]. The above retention obligation covers data necessary to identify the network termination, the terminal device, the end user initiating the connection and the recipient of the call, as well as to identify the date, time of the call, its duration, type of connection, and the location of the telecommunications terminal[39].

---

results from the ease of crossing of boundaries of acceptability of state interference in the sphere of citizen's rights and freedoms by a public authority.

36 *Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli* – Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej. [The report of the Commission on Human Rights at the Polish Bar Council. *Data retention: concern for security or surveillance of citizens.*] Available at: http://archiwum.adwokatura.pl/?p=3566 [Accessed: 1 June 2014], p. 7.

37 *Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli* – Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej. [The report of the Commission on Human Rights at the Polish Bar Council. *Data retention: concern for security or surveillance of citizens.*] Available at: http://archiwum.adwokatura.pl/?p=3566 [Accessed: 1 June 2014], p. 4.

38 Art. 180a of the Act of 16 July 2004 – *Telecommunications Law*. (Journal of Laws of 2004, No. 171, item 1800).

39 Art. 180c of the Act of 16 July 2004 – *Telecommunications Law*. (Journal of Laws of 2004, No. 171, item 1800).

Authorised services, courts and the prosecutor's office were granted an exemption from telecommunications secrecy and protection of data of end users. The contents of Art. 180d of the Act implies easy access of these entities to the data: (1) concerning the user, (2) concerning transmission, which include data processed for the purpose of transmitting messages in telecommunication networks or charging fees for telecommunications services, including location data indicating the geographic position of the device of the end user, (3) going beyond the data necessary for the transmission of a communication or issuing of an invoice, (4) attempts to establish communication between the terminations of the network, including data on unsuccessful attempts which have been matched but not answered by the end user or the interrupted connections[40].

The scope of information which will eventually go to the desk of the officers – applicants include data such as: the surname and names, parents' names, the place and date of birth, the address of permanent residence, the national identification number – in the case of a Polish citizen, the name, series and number of identification documents, and in the case of a foreigner who is not a citizen of a Member State or the Swiss Confederation – the number of the passport or the residence permit. Officers also have information which is contained in the contract for the provision of telecommunication services and in other documents processed by the operator. It concerns, in particular, a list of subscriptions of the users or the network terminations[41], the tax identification number (NIP), the number of the bank account or the credit card, mailing address of the user if different from the address of permanent residence, and e-mail address and contact telephone numbers[42].

The public has repeatedly drawn attention to the abuses associated with the acquisition of information by services in Poland. A report prepared after the press news shows that no one is in control of 'checks' carried out by services. The lack of supervision and reporting in this area applies to all services, including the prosecutor's offices and courts. Currently, only the amended Act on the Police in Art. 19 paragraph 22 obliges the Attorney General to prepare annual reports for the Parliament on the amount of operational techniques applied by the police.

---

40 Art. 159 paragraph 1 point 1 and point 3–5 of the Act of 16 July 2004 – *Telecommunications Law*. (Journal of Laws of 2004, No. 171, item 1800).

41 Art. 179 paragraph 9 of the Act of 16 July 2004 – *Telecommunications Law*. (Journal of Laws of 2004, No. 171, item 1800).

42 Art. 161 of the Act of 16 July 2004 – *Telecommunications Law*. (Journal of Laws of 2004, No. 171, item 1800).

The right of access to retention information is a result and a derivative of the obligation which was imposed on the Polish legislator by the so-called Retention Directive[43], which was adopted under the pressure of international events. The wave of terrorism which swept, among others, through Europe (bombings in Madrid and London) and the USA (the attacks on the WTC and the Pentagon) became an excuse for strengthening the security department. The aim was to impose common standards in the Member States[44].

It should be noted that the standards contained in the retention directive did not enter into force in all European Union countries. In several countries the provisions of the Directive have been questioned as violating the universal right to privacy. The Constitutional Court of Romania (8 October 2009), the Federal Constitutional Court in Germany (March 2, 2010)[45], the Constitutional Court of the Czech Republic (31 March 2011)

[43] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* (OJ L 105, 13.4.2006.)

[44] The European legislator has acted on the assumption that there is a need to acquire at least the following information about citizens of the Union (requiring it from the Member States): (a) data necessary to identify the source of a communication, (b) data necessary to identify the destination of a communication, (c) data necessary to identify the date, time and duration of a communication, (d) data necessary to identify the type of communication, (e) data necessary to identify users' communication equipment or what purports to be their equipment, (f) data necessary to identify the location of mobile communication equipment. *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* (OJ L 105, 13.4.2006.)

[45] The main theses – which are the articulation of the charges against the directive – from the judgment of the Federal Constitutional Court in Germany: (a) unjustified, six-month storage of data on telecommunication connections by a private provider, (b) lack of careful, transparent and accurate standards of data protection, rules for using them and their legal protection, (c) absence of a precise indication of purposes the data can be used for, (d) the need for the creation of a regulation which would provide a clear and particularly high standard of their safety, (e) access to the data must be consistent with the principle of proportionality, (f) the use of the data should be permitted only in cases of particular importance. See *Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli* – Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej. [The report of the Commission on Human Rights at the Polish Bar Council. *Data retention: concern for security or surveillance of citizens.*] Available at: http://archiwum.adwokatura.pl/?p=3566 [Accessed: 4 April 2014], pp. 7–8.

unanimously ruled the inconsistency of laws implementing the Directive with the constitutions of these states.

Certain doubts were also reported by the European Court of Human Rights, which although recognises and recommends the distinction between information gained by wiretapping and this from phone records, also stresses that there are situations in which the latter can in a more considerable way interfere with the protection of privacy. 'On the basis of Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, the ECHR stated that by its very nature a phone record must be distinguished from wiretapping, which is undesirable and illegal in a democratic society unless there is a valid reason for it. But the use of data resulting from a phone record may, in certain circumstances, constitute a violation of Art. 8 of the Convention. Phone bill data contain information especially about dialled numbers, which are an integral component of telephone communications. As a result, the disclosure of this information to the police without the consent of the subscriber also constitutes intrusion in the rights guaranteed by Article 8. Meanwhile, in laws governing the powers of services the legislature provided a much lower standard of protection for data obtained from phone records in the course of operational activities than by means of wiretapping'[46]. The same European Court of Human Rights in its judgment of 30 July 1998 stated that 'control of a phone line is interference by public authorities in the right to respect for private life and correspondence. It does not matter that it involved only the use of a system registering calls from a particular telephone. Therefore, in this case, as in the case of wiretapping, legislation should include safeguards that will prevent abuses of power'[47].

The European Data Protection Supervisor (EDPS) also criticised the formula of data retention. On 31 May 2011 EDPS issued an opinion[48] in which he indicates that the Retention Directive does not meet the minimum standards on the right to privacy and protection of personal data. 'The EDPS repeatedly expressed doubts about the justification for retaining data

---

46 Constitutional Court's judgment of 20 June 2005, K 4/04 OTK-A 2005/6/64, Lex 155534. Cf. ECHR judgment of 2 August 1984 in the case Malone v. the United Kingdom, application no. 8691/79.

47 The case Valenzuela Contreras v. Spain, application no. 27671/95. See Constitutional Court's judgment of 20 June 2005, K 4/04 OTK-A 2005/6/64, Lex 155534.

48 European Data Protection Supervisor. *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, EDPS/11/6, Brussels, 31 May 2011.

on such a scale in light of the rights to privacy and data protection. The EDPS reminded about the need to justify whether the retention is necessary and proportionate. The EDPS concluded that the directive violates the guarantees of protection of personal data and privacy for the following reasons: (1) maintaining the obligation of data retention is not sufficiently justified by the Directive, (2) data retention could have been regulated in a way which is far less intrusive to the right to privacy, (3) the Directive leaves too big margin of freedom for Member States in the field of data processing, as well as does not determine who and to what extent is to be able to access the data'[49].

The provisions of the Directive were sharply criticised by the non-governmental sector publishing the so-called 'shadow report'. The authors from the Digital Civil Rights in Europe Foundation pointed out that 'European citizens have paid dearly both in terms of a reduction in the right to privacy and also in the chaos and lawless treatment of personal data. Europe's hard won credibility for defending fundamental rights has also suffered. The directive turned out to be a failure on every level: fundamental rights of the Europeans were threatened, it failed to harmonise data retention rules, in addition, these losses were not necessary in the fight against crime'[50].

In response to the avalanche of protests, the European Commission decided to publish its own evaluation report. Report from the Commission to the Council and the European Parliament – Evaluation report on the Data Retention Directive (Directive 2006/24/EC) was released on 18 April 2011. At the very beginning, it is stressed that data retention has become an extremely important tool to ensure security. The authors of the report recognise, however, risks arising from the possibility of abuse of the information. The directive was designed to make it easier for the authorities to investigate, detect and prosecute serious crimes. Meanwhile, some national

---

49 Europejski Inspektor Danych Osobowych o dyrektywie retencyjnej. [The European Data Protection Supervisor on the Data Retention Directive] Available at: http://www.europapraw.org/news/europejski-inspektor-danych-osobowych-o-dyrektywie-retencyjnej [Accessed: 7 May 2014].

50 „Nic nie zyskaliśmy, a straciliśmy prywatność" – Komisja Europejska ocenia dyrektywę o retencji danych, my oceniamy Komisję… i sytuację w Polsce. ['We have not gained anything, and lost privacy' – the European Commission evaluates the Directive on data retention, we assess the Commission ... and the situation in Poland.] [Online] Available at: http://panoptykon.org/wiadomosc/nic-nie-zyskalismy-stracilismy-prywatnosc-komisja-europejska-ocenia-dyrektywe-o-retencji-d [Accessed: 21 August 2014].

legislators, as highlighted in the report, used the circumstances related to the implementation of the EU act to increase the detection of all types of wrong-doing and forbidden acts. Differences between countries are evident. 'Ten Member States (Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, Netherlands, Finland) have defined the possibility of using data retention in the case of serious, enumerated crimes while eight Member States (Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, Slovenia) of all crimes. The legislation of four Member States (Cyprus, Malta, Portugal, United Kingdom) refers to "serious crime" or "serious offence" without defining it'[51].

The report draws attention to the fact that the majority of EU countries have introduced into their legal order provisions going far beyond the goals which the Directive obliged them to achieve. National bodies which do not provide adequate protection have obtained access to the data. All Member States have provided access for police services and prosecutors. Six countries have included the tax authorities and three border police. Regarding the aspect of prior authorisation for access to the data, national laws vary considerably. 'One Member State allows other public authorities to access the data if they are authorised for specific purposes under secondary legislation. Eleven Member States require judicial authorisation for each request for access to retained data. In only three Member States prior judicial authorisation is required. Four other Member States require authorisation from a senior authority but not a judge. In two Member States, the only condition appears to be that the request is made writing'[52]. This means that in the case of some national authorities the only safeguard is the requirement of the written form of the request. Needless to say, in such a situation it is difficult to achieve the appropriate proportionality and restraint.

Capturing the actual amount of information collected by security and public order services (law enforcement authorities) is impossible. Some light can shed by data on the number of inquiries/requests for information retention. It is worth noting that only nineteen states (out of twenty-seven) provided their statistics. Based on the data from the years 2008–2009, it is estimated that on average telecom operators receive 2 million requests per year. Differences in individual countries should be noted. The scope ranges

---

51 *Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, 3 COM(2011) 225 final, Brussels 18.4.2011, p. 6.

52 *Ibidem*, p. 9.

from approximately 100 requests on Cyprus to more than 1 million in Poland. There is no precise data on initiated criminal proceedings, allegations, indictments, final judgments – the actual effects of this instrument of obtaining evidence. In the report of the Commission one can only find a general remark that the mechanism has become a valuable weapon to prevent, detect and combat crime. 'Member States generally reported data retention to be at least valuable, and in some cases indispensable for preventing and combating crime, including the protection of victims. Retained traffic data have proven necessary in contacting witnesses to an incident who would not otherwise have been identified'[53]. However, the authors of the document are not able to answer the question to what extent the collected data actually contribute to improving security in Europe[54]. The wording related to general usefulness cannot be satisfactory in the face of such a substantial interference in the space of legally protected privacy.

To sum up, only in 2010 data on the connections and location of an average European were recorded every six minutes. Various services generated approximately 2.5 million requests on the basis of which they received information allowing them to create a psychological portrait of each person. It can therefore be assumed that in 2008–2011 approximately 10 million requests were submitted. Each was probably related to a case that covered at least a few people. There are requests thanks to which officers receive detailed information about dozens of people. Assuming conservatively that on the basis of one request it is possible to create an economic and psychological image of three people it gives a total of approximately 30 million citizens. The scale for potential abuse is enormous.

---

53 *Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, 3 COM(2011) 225 final, Brussels 18.4.2011, p. 23.

54 In the conclusions the authors of the report formulate recommendations for the future. In order to make data retention more transparent and less controversial, legislation at the national level should be standardised, in particular as regards the application of the principle of proportionality. See *Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, 3 COM (2011) 225 final, Brussels 18.4.2011, pp. 30–33.

EPILOGUE

Caring for safety and order is the primary responsibility of the state sector[55]. Some point that it is primary in relation to all the others. Abraham Maslow places safety just after physiological needs but before the need for belonging, respect and self-realisation in his hierarchy of needs. Without having a sense of security it is difficult to realise others, e.g. social or economic needs. States are responsible for identifying, anticipating and eliminating threats. However, the modern world is characterised by the occurrence of increasingly sophisticated forms. At the same time social relations are less and less straightforward. Particularly in information and network societies. Various activities overlap, creating tension. The scope of protection of the right to privacy intersects with the scope of the right to enjoy the sense of security. The question of establishing a hierarchy of values arises. While in an authoritarian state a political superior can set and can move freely the line between the privileges, in free societies the process of demarcation of the border with the participation of actors of the public scene lasts incessantly. Violence and suddenness of terrorist attacks not only exposed general carelessness of public authorities, but above all became a pretext for granting unprecedented privileges to the security sphere. However, while the deprivation of terrorists of the right to privacy is justified and socially acceptable, this general attack on privacy creates dissonance which is difficult to accept. There is a reasonable suspicion that maintaining a healthy balance between democratic values has got out of control. Certainly, efforts should be made to ensure that the state adheres to the principle of restraint in the "collection" of data and does not relativise the general 'ultimate need' clause. Moderation seems to be here an attribute which imposes discipline. However, the fight against terrorism has become an excuse for extending competences. States, regardless of whether they are a cradle of democracy and human rights

[55] Security is often expressed using the following criteria: subjective (individual, local, national, international and global), objective (military, political, economic, ecological, cultural and social), spatial (domestic, local, sub-regional, regional), importance (state, sense, process, purpose, value, need, structure, organisation), ingredients (negative – focused on survival, positive – focused on freedom of development), and the area of the organisation (internal and external). See more in Brzeziński, M. 2009. Rodzaje bezpieczeństwa państwa. [Types of state security.] In: Sulowski, S., Brzeziński, M. eds. *Bezpieczeństwo wewnętrzne państwa*. [*The internal security of the state*.] Warszawa, p. 34. Cf. Korzeniowski, L.F. 2012. *Podstawy nauk o bezpieczeństwie. Zarządzanie bezpieczeństwem*. [*Fundamentals of sciences about security. Security management*.] Warszawa, p. 99–143.

or an oasis of authoritarian lawlessness, when it comes to information, always show a natural tendency to expand the methods of obtaining it – often using clandestine methods. Christopher Andrew identified three main reasons for maintaining the cult of secrecy: (1) historical events of assigning too much weight to all public actions, (2) secrecy obsession, (3) finally, international law prohibiting the interception of diplomatic correspondence[56].

Services of democratic states must not be treated as institutions acting to the detriment of citizens. The case, however, concerns a method of using information[57]. An explicit obligation of providing public authorities with relevant information by the citizens, or vice versa, an order imposing an obligation on state authorities to search for data, contain legalistic instructions in them. The state can require from its citizens only such kinds of information (and in any case no other) which are described in a normative act of general application. In this regard, the acquisition method and the subjective nature of the data themselves cannot be inconsistent with (at least) the regulations about personal data protection. The model of law-making *ex definitione* eliminates cases of overt acquisition of information about citizens which would violate the relevant standards. While the boundaries of overt methods are, firstly, inscribed in the natural everyday life, secondly – are clearly prescribed by law, thirdly – do not raise serious controversy, confidential methods leave a free space for abuse, misinterpretation and instrumental use. And secret ways should be somewhat on the carpet and provided with a greater degree of care and supervision[58].

---

[56] See more in Andrew, Ch. 1977. Whitehall, Washington and the intelligence services. *International Affairs*, vol. 53, no. 3, pp. 390–404. Secrecy translates into an operational model of the entity, including the characteristics of the conditions of confidential activity in the organisation. Cf. Dufresne, R.L., Offstein, E.H. 2008. On the virtues of secrecy in organisations. *Journal of Management Inquiry*, no. 17 (102); Little, L. 2008. Privacy, trust, and identity issues for ubiquitous computing. *Social Science Computer Review*, no. 26.

[57] Cf. Siemiątkowski, Z. 2009. *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*. [*Intelligence and power. Civilian intelligence in the system of exercising political power of the PRP*.] Warszawa; Smith, M. J. 2000. Intelligence and the core executive. *Public Policy and Administration*, no 25.

[58] William E. Colby, a long-time chief of the CIA, presented an excellent analysis of the compatibility of the covert space in a free society. Colby believes that hidden and overt spheres cannot be treated as a dichotomy in a democratic country because both of them (exposure, secrecy) are necessary for a truly free society. Without secrecy democracy would not be able to function (e.g. secret votes cast in elections, the relationship doctor-patient, lawyer-client). Colby, W.E. 1976. Intelligence secrecy and security in a free society. *International Security*, vol. 1, no. 2, pp. 3–14; Cf. Thompson, E.P. 1979.

The future looks interesting in this context. While in the US we should expect the prolongation of the validity of relevant provisions of the Patriot Act (especially in the context of the fight against the Islamic State), in Europe things are not so clear-cut. There are visible differences between the American and European models. It is true that solutions infringing the previously solidly protected privacy were implemented on the old continent. However, this interference is not so blatant. The disproportions most probably result from the position, interests and socio-political traditions. The United States profess the concept of a strong state – the guardian of the world order. It is in the US where access to weapons is universal and patriotism is often identified with the military aspect. Europe seems to be a place with a more restrained socio-political culture. The EU is committed to represent the interests of many states-economies with various traditions and values. A more pragmatic legal system dominates here, with a highly extended regime of protection of human rights (with a strong influence of the Scandinavian countries with a long tradition of privacy), with supranational judiciary in the form of the European Court of Human Rights and the European Court of Justice. It was in Europe where three national constitutional courts (Germany, the Czech Republic and Romania) adjudicated the contradiction of the provisions of the Retention Directive with the internal legal order (creating an interesting constitutional case – breaking so far widely accepted principle of the primacy of European law established by ECJ[59] judicature). On 8 April 2014 the European Union Court of Justice, in joined cases C-293/12 and C-594/12

The secret state. *Race Class*, no. 20 (219). Cf. Garson, G. D. 2006. Securing the virtual state: recent developments in privacy and security. *Social Science Computer Review*, no. 24 (489). Cf. Gadzheva, M. 2007. Privacy in the age of transparency. *Social Science Computer Review*, no. 26 (60).

[59] The rules of: (a) the autonomous legal order, (b) the primacy of Community law, (c) the direct application of Community law were precisely defined by the jurisprudence of the European Court of Justice, which expressed them, among others, in the following cases Van Gend & Loos, Flaminio Costa v. ENEL, ERTA, Defrenne Cassis de Dijon, Von Colson and Kamann, Marleasing, Foster, or Francovich. In the case of the Federal Constitutional Court of the Federal Republic of Germany it was not the first time that the precedence of Community law over national one was questioned. In the case of Kloppenburg the Court admitted the precedence, but at the same time stipulated that it is not automatic and cannot go too far in German constitutional law. See more on this topic in Jeneralczyk-Sobierajska, A. ed. 1998. *Wzajemne relacje prawa międzynarodowego, wspólnotowego oraz prawa krajowego. Hierarchia norm oraz stosowanie prawa przez sądy.* [*Mutual relations of international, Community and domestic law. The hierarchy of standards and application of law by courts*.] Łódź: Instytut Europejski.

Digital Rights Ireland Ltd. and C-594/12 Kärntner Landesregierung and others, ruled that the Retention Directive was invalid.[60] Preventive collection of data on all telecommunications connections without judicial review was considered disproportionate infringement of civil rights and liberties[61]. The Court confirmed reservations reported not only the NGO community but also by national courts finding that the provisions of the Directive exceed the principle of proportionality guaranteed in Art. 7, 8 and 52, paragraph. 1 of the Charter of Fundamental Rights of the European Union.[62] The judgment was issued pursuant to Art. 267 of the TFEU, which means that it was binding only for the national court which had asked for the preliminary ruling. However, it should provide a sufficient basis to take action unifying judicature for any other national court (such a position was expressed, for example, in the judgment of the ECJ of 13 May 1981 in case C-66/80 International Chemical Corporation). If the court declares that an act adopted by the organisational unit operating within the European Union is invalid, it is required to take the

[60] The Retention Directive was also previously subject to control by the Court of Justice of the European Union. In Case C-301/06 Ireland v. Parliament and Council (CJEU judgment of 10 February 2009) the Court examined the correctness of the legal basis, not referring, however, to the issue of the compatibility of the directive with fundamental rights. See *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, Brussels 18 April 2011. COM (2011) 225 final, p. 20 ff.

[61] According to the Court, the directive did not provide sufficient guarantees for limiting the invasion of privacy. **A**mong other things, the scope of the directive covered all individuals without restrictions or exceptions (e.g. depending on the purpose). There was no guarantee that national bodies could use the obtained data solely for purposes justifying the regulation. Moreover, it did not provide procedures for access to the data covered by retention, including prior judicial or administrative review. See Co oznacza dla nas wyrok ETS w sprawie retencji danych. [What the ECJ judgment on data retention means for us.] [Online] Available at: https://wprawoautorskie.wordpress.com/2014/04/09/retencja-danych-wyrok-ets/ [Accessed: 5 March 2015]; Cios dla Wielkiego Brata w UE. Dyrektywa retencyjna jest nieważna – wyrok ETS. [A blow for Big Brother in the EU. Retention Directive is invalid – ECJ judgment.] [Online] Available at: http://di.com.pl/news/49732,0,Cios_dla_Wielkiego_Brata_w_UE_Dyrektywa_retencyjna_jest_niewazna_-_wyrok_ETS.html [Accessed: 5 March 2015]; Dyrektywa retencyjna jest nieważna – wyrok TSUE. [The Retention Directive is invalid – the judgment of the ECJ.] [Online] Available at: http://www.europapraw.org/news/dyrektywa-retencyjna-jest-niewazna-wyrok-trybunalu-sprawiedliwosci-unii-europejskiej [Accessed: 5 March 2015].

[62] *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Protocols, Annexes, Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon*. Official Journal of the European Union, C 83, 30 March 2010.

necessary measures to comply with the judgment of the Court of Justice of the European Union (art. 266 of the TFEU). In connection with the fact that the Court did not limit the temporal effects of the judgment, the judgment in the case of Digital Rights takes *ex tunc* effect, i.e. with retroactive effect from the date of entry into force of the relevant legal act.

Although this decision is of fundamental importance, and Peter Hustinx, the European Data Protection Supervisor, found that this is the end of the validity 'of most privacy infringing law ever adopted in the European Union', the annulment of the directive, as a rule, did not affect directly the nullity of national legislation implementing it. Its annulment can result only from the activity of the national legislature – on its own initiative or as a result of the judgment of the national constitutional courts. This was the basis of the Polish Constitutional Court judgment. In the case no. K 23/11, of 30 July 2014, the Constitutional Court examined the constitutionality of regulations implementing the Retention Directive in Poland. The Constitutional Tribunal (full bench) adjudicated, among others, that provisions empowering the Police, the Border Guard, Tax Audit, the Military Police, the Internal Security Agency, the Foreign Intelligence Agency and the Central Anti-Corruption Bureau to obtain data covered by the telecommunications secret were inconsistent with Articles 47 and 49 in conjunction with Article 31(3) of the Constitution as they do not provide for independent supervision over granting access to communications data referred to in Article 180c and 180d of the Act of 16 July 2004 – Telecommunications Law[63]. In the oral explanation of

[63] In its judgment of 30 July 2014, the Constitutional Tribunal adjudicated that: (1) Article 19(1)(8) of the Act of 6 April 1990 on the Police, Article 9e(1)(7) of the Act of 12 October 1990 on the Border Guard, Article 36c(1)(5) of the Act of 28 September 1991 on Tax Audit, Article 31(1)(17) of the Act of 24 August 2001 on the Military Police and military authorities responsible for maintaining order and discipline – construed as concerning offences specified in the Polish penal law which were prosecuted on the basis of ratified international agreements upon consent expressed by statute, were consistent with Article 2, Article 47 and Article 49 in conjunction with Article 31(3) of the Constitution of the Republic of Poland as well as Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, done at Rome on 4 November 1950, as amended by Protocols No. 3, 5 and 8 as well as supplemented by Protocol No. 2, (2) Article 27(1), in conjunction with Article 5(1)(2)(b), of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency was inconsistent with Article 2, Article 47 and Article 49 in conjunction with Article 31(3) of the Constitution, (3) Article 20c(1) of the Act on the Police, Article 10b(1) of the Act on the Border Guard, Article 36b(1)(1) of the Act on Tax Audit, Article 30(1) of the Act on the Military Police and military authorities responsible for maintaining order and discipline, Article 28(1)(1) of the Act on the Internal Security Agency and

the verdict it was emphasised that 'every person has the right to protection against external monitoring of his personal activity, in every dimension – both in the real and in the virtual world'[64]. The judge pointed to the need to provide guarantees for the freedom and anonymity of individuals, especially in the era of the development of new technologies. The court adjudicated

the Foreign Intelligence Agency, Article 32(1)(1) of the Act on the Military Counter-Intelligence Service and the Military Intelligence Service, Article 18(1)(1) of the Act on the Central Anti-Corruption Bureau, Article 75d(1) of the Act of 27 August 2009 on the Customs Service – insofar as they did not provide for independent supervision over disclosing communications data referred to in Article 180c and Article 180d of the Act of 16 July 2004 – the *Telecommunications Law*, were inconsistent with Article 47 and Article 49 in conjunction with Article 31(3) of the Constitution, (4) Article 19 of the Act on the Police, Article 9e of the Act on the Border Guard, Article 36c of the Act on Tax Audit, Article 31 of the Act on the Military Police and military authorities responsible for maintaining order and discipline, Article 27 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, Article 31 of the Act on the Military Counter-Intelligence Service and the Military Intelligence Service, Article 17 of the Act on the Central Anti-Corruption Bureau – insofar as they did not provide for a guarantee that materials which contained information that was prohibited from being evidence should be subject to immediate, witnessed and recorded destruction, in the case where the court had not lifted professional confidentiality requirement, were inconsistent with Article 42(2), Article 47, Article 49, Article 51(2) and Article 54(1) in conjunction with Article 31(3) of the Constitution, (5) Article 28 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, Article 32 of the Act on the Military Counter-Intelligence Service and the Military Intelligence Service, Article 18 of the Act on the Central Anti-Corruption Bureau – insofar as they did not provide for the deletion of data that were irrelevant for the conduct of investigative proceedings, were inconsistent with Article 51(2) in conjunction with Article 31(3) of the Constitution, (6) Article 75d(5) of the Act on Customs Service, insofar as it allowed for retaining other materials than those that contained information which was relevant for proceedings in cases on tax misdemeanours or offences specified in chapter 9 of the Act of 10 September 1999 – the Penal Fiscal Code, was inconsistent with Article 51(4) of the Constitution. See Constitutional Court's judgment of 30 July 2014, no. K 23/11. [Online] Available at: http://trybunal.gov.pl/rozprawy/wyroki/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/ [Accessed: 3 March 2014].

64 Retencja danych – wyrok Trybunału Konstytucyjnego z 30 lipca 2014, sygn. K 23/11. [Data retention – Constitutional Court's judgment of 30 July 2014, no. K 23/11.] [Online] Available at: http://akrasuski.com/news/11/18/Retencja-danych-wyrok-Trybunalu-Konstytucyjnego-z-30-lipca-2014-r-sygn-K-23-11.html; Trybunał Konstytucyjny podważył część przepisów o retencji danych telekomunikacyjnych (sygn. K 23/11). [The Constitutional Court questioned some of the provisions on retention of telecommunications data (file no. K 23/11).] [Online] Available at: http://prawo.vagla.pl/node/10103 [Accessed: 4 March 2015].

that the provisions within the scope indicated therein would cease to have effect after the lapse of eighteen months from the date of the publication of the judgment in the Journal of Laws.

The nearest future will show whether the above-described reaction characteristic of democratic legal states, as a naturally occurring force balancing unhealthy disproportions which were implemented after the terrorist attacks at the same time in the area of security and privacy, will become a the rule.

References

Andrew, Ch. 1977. Whitehall, Washington and the intelligence services. *International Affairs*, vol. 53, no. 3, pp. 390–404.

Bazański, Ł. Retencja danych oraz nowe obowiązki ISP w zakresie danych osobowych. [Data retention and new responsibilities of ISPs in the field of personal data.] [Online] Available at: http://www.kike.pl/2013/02/28/retencja-danych-oraz-nowe-obowiazki-isp-w-zakresie-danych-osobowych/ [Accessed: 4 March 2015].

Brzeziński, M. 2009. Rodzaje bezpieczeństwa państwa. [Types of state security.] In: Sulowski, S., Brzeziński, M. eds. *Bezpieczeństwo wewnętrzne państwa*. [*The internal security of the state*.] Warszawa, p. 34.

Cios dla Wielkiego Brata w UE. Dyrektywa retencyjna jest nieważna – wyrok ETS. [A blow for Big Brother in the EU. Retention Directive is invalid – ECJ judgment.] [Online] Available at: http://di.com.pl/news/49732,0,Cios_dla_Wielkiego_Brata_w_UE_Dyrektywa_retencyjna_jest_niewazna_-_wyrok_ETS.html [Accessed: 5 March 2015].

Colby, W.E. 1976. Intelligence secrecy and security in a free society. *International Security*, vol. 1, no. 2, pp. 3–14.

Co oznacza dla nas wyrok ETS w sprawie retencji danych. [What the ECJ judgment on data retention means for us.] [Online] Available at: https://wprawoautorskie.wordpress.com/2014/04/09/retencja-danych-wyrok-ets/ [Accessed: 5 March 2015].

Črnčec, D. 2009. A new intelligence paradigm and the European Union. *Journal of Criminal Justice and Security*, no. 1.

Davis, P.H.J. 2010. Intelligence and the machinery of government: conceptualizing the intelligence community. *Public Policy and Administration*. no. 25 (29).

Desai, U., Crow, M.M. 1983. Failures of power and intelligence: use of scientific-technical information in government decision making. *Administration & Society* no. 15 (185).

Dufresne, R.L., Offstein, E.H. 2008. On the virtues of secrecy in organisations. *Journal of Management Inquiry*, no. 17 (102).

Dyrektywa retencyjna jest nieważna – wyrok TSUE. [The Retention Directive is invalid – the judgment of the ECJ.] [Online] Available at: http://www.europapraw.org/news/dyrektywa-retencyjna-jest-niewazna-wyrok-trybunalu-sprawiedliwosci-unii-europejskiej [Accessed: 5 March 2015].

European Parliament. 2001. Temporary Committee on the ECHELON Interception System: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), [2001/2098 (INI)], 11 July 2001.

Europejski Inspektor Danych Osobowych o dyrektywie retencyjnej. [The European Data Protection Supervisor on the Data Retention Directive] Available at: http://www.europapraw.org/news/europejski-inspektor-danych-osobowych-o-dyrektywie-retencyjnej [Accessed: 7 May 2014].

Flanagan, S.J. 1985. Managing the Intelligence Community. *International Security*, vol. 10, no. 1.

Freeman, O. 1999. Competitor intelligence: information or intelligence? *Business Information Review*, no. 16 (71).

Gadzheva, M. 2007. Privacy in the age of transparency. *Social Science Computer Review*, no. 26 (60).

Garson, G.D. 2006. Securing the virtual state: recent developments in privacy and security. *Social Science Computer Review*, no. 24 (489).

Kołodko, G. 2013. *Dokąd zmierza świat. Ekonomia polityczna przyszłości*. [*Where the world is heading. The political economy of the future*.] Warszawa.

Kołodko, G. 2013. *Wędrujący świat*. [*Wandering Word*.] Warszawa.

The USA Constitution. Available at: http://libr.sejm.gov.pl/bibl/ [Accessed: 9 September 2014].

Korzeniowski, L. F. 2012. *Podstawy nauk o bezpieczeństwie. Zarządzanie bezpieczeństwem*. [*Fundamentals of sciences about security. Security management*.] Warszawa, p. 99–143.

Koziej, S. Obywatele są bezbronni wobec zagrożeń takich jak PRISM. [Citizens are defenceless in the face of threats such as PRISM.] *Polska Agencja Prasowa* [Online]. Available at: http://wiadomosci.wp.pl/kat,13-42,title,Stanislaw-Koziej-obywatele-sa-bezbronni-wobec-zagrozen-takich-jak-PRISM,wid,15741432,wiadomosc.html?ticaid=1127d3&_ticrsn=5; [Accessed: 7 July 2014].

Little, L. 2008. Privacy, trust, and identity issues for ubiquitous computing. *Social Science Computer Review*, no. 26.

Memorandum of Attorney General (Janet Reno) to Assistant Attorney General, Criminal Division Director, FBI Counsel for Intelligence Policy United States Attorneys. 19 June 1995 Available at: http://epic.org/privacy/terrorism/fisa/ag_1995_mem.html [Accessed: 21 January 2015].

„Nic nie zyskaliśmy, a straciliśmy prywatność" – Komisja Europejska ocenia dyrektywę o retencji danych, my oceniamy Komisję… i sytuację w Polsce. ['We have not gained anything, and lost privacy' – the European Commission evaluates the Directive on data retention, we assess the Commission ... and the situation in Poland.] [Online] Available at: http://panoptykon.org/wiadomosc/nic-nie-zyskalismy-stracilismy-prywatnosc-komisja-europejska-ocenia-dyrektywe-o-retencji-d [Accessed: 21 August 2014].

Nisztor, P. Polacy pod kontrolą służb. [Poles under the control of the services.] *Rzeczpospolita,* no. 116 (8932), p. 1.

Omand, D. 2010. Creating intelligence communities. *Public Policy and Administration*. no. 25 (99).

European Data Protection Supervisor. 2011. *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, EDPS/11/6, Brussels, 31 May 2011.

Podolski, A. 2004. *Europejska współpraca wywiadowcza – brakujące ogniwo europejskiej polityki zagranicznej i bezpieczeństwa?* [*European intelligence cooperation – a missing link of European foreign and security policy*?] Warszawa: Centrum Stosunków Międzynarodowych, Raporty i Analizy no. 10, p. 1.

Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), 3 COM(2011) 225 final, Brussels 18.4.2011, p. 23.

Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli – Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej. [The report of the Commission on Human Rights at the Polish Bar Council. *Data retention: concern for security or surveillance of citizens.*] Available at: http://archiwum.adwokatura.pl/?p=3566 [Accessed: 4 April 2014].

Retencja danych – wyrok Trybunału Konstytucyjnego z 30 lipca 2014, sygn. K 23/11. [Data retention – Constitutional Court's judgment of 30 July 2014, no. K 23/11.] [Online] Available at: http://akrasuski.com/news/11/18/Retencja-danych-wyrok-Trybunalu-Konstytucyjnego-z-30-lipca-2014-r-sygn-K-23-11.html

Rogala-Lewicki, A. *Czy polskie służby specjalne potrzebują formuły Intelligence Community*. [*Do Polish special services need formulas of Intelligence Community*?] Forum Studiów i Analiz Politycznych im. Maurycego Mochnackiego. [ISSN 2082-7997] Available at: http://www.fsap.pl/index.php?option=com_content&view=article&id=21%3Aczy-polskie-suby-specjalne-potrzebuj-formuy-intelligence-community&catid=7%3Acomments&Itemid=9&lang=pl, [Accessed: 7 May 2014].

Siedlecka, E. 2011. Służby zdradzają, jak często sięgały po bilingi. [Services reveal how often they reached for phone records.] *Gazeta Wyborcza* [Online] 10 February 2011, p. 6; Available at: http://wyborcza.pl/1,75478,9081579,Sluzby_zdradzaja__jak_czesto_siegaly_po_billingi.html#ixzz1TgKmikgS, [Accessed: 15 August 2014].

Służby zdradzają, jak często sięgały po bilingi. [Services reveal how often they reached for phone records.] *Gazeta Wyborcza* 10 February 2011, p. 6.

Siedlecka, E. 2011. Kogo można podsłuchać. [Who can be eavesdropped.] *Gazeta Wyborcza* 15 March 2011, p .7.

Siedlecka, E. KE: Za dużo podglądacie. [The EC: you are spying too much.] *Gazeta Wyborcza* [Online] Available at: http://wyborcza.pl/1,75478,9453157,KE__Za_duzo_podgladacie.html [Accessed: 15 August 2014].

Siemiątkowski, Z. 2009. *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*. [*Intelligence and power. Civilian intelligence in the system of exercising political power of the PRP*.] Warszawa.

Smith, M. J. 2000. Intelligence and the core executive. *Public Policy and Administration*, no 25.

Staniszkis, J. 2006. *O władzy i bezsilności*. [*About power and powerlessness*.] Kraków.

Staniszkis, J. 2003/4. *Władza globalizacji*. [*The power of globalization*.] Warszawa.

Stawecki, T. 2005. *Rejestry publiczne. Funkcje instytucji*. [*Public registers. Functions of institutions*.] Warszawa.

Stiglitz, J. 2007. *Globalizacja*. [*Globalisation*.] Translated by H. Simbierowicz, Warszawa.

Thompson, E. P. 1979. The secret state. *Race Class*, no. 20 (219).

Trybunał Konstytucyjny podważył część przepisów o retencji danych telekomunikacyjnych (sygn. K 23/11). [The Constitutional Court questioned some of the provisions on retention of telecommunications data (file no. K 23/11).] [Online] Available at: http://prawo.vagla.pl/node/10103 [Accessed: 4 March 2015].

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism – USA Patriot Act, H. R. 3162, (Public Law 107-56). Available at: http://epic.org/privacy/terrorism/hr3162.html [Accessed: 9 March 2015].

Wzajemne relacje prawa międzynarodowego, wspólnotowego oraz prawa krajowego. Hierarchia norm oraz stosowanie prawa przez sądy. [*Mutual relations of international, Community and domestic law. The hierarchy of standards and application of law by courts*.] Łódź: Instytut Europejski.

Vervaele, J.A.E. 2005. Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law. *Utrecht Law Review*, vol. 1, no 1.

Security services after the terrorist attacks in the US and Europe. Patriot Act versus the Retention Directive, or the legitimisation of abuses in the sphere of privacy in democratic states: a comparative study

Summary

Acceleration of technologisation processes, networking of communication, and in consequences it social interactions, resulted in a shift of social, economic and political paradigm in the civilisation sphere. For the purpose of anticipation of an increasing of more and more sophisticated threats, state law enforcement and intelligence agencies developed and implemented new technologies to allow secret services not only maintain *raison d'être* but also to preserve and expand assets. And so the existence of American system *Echelon* or the revealed by Edward Snowden *PRISM* platform opened public eyes to the fact that the intelligence agencies (in particular, the US National Security Agency) are not only able to capture any tele-information signal but actually takes advantage of this privilege. Despite these attributes, due to administrative and logistical shortcomings, secret services did not avoid the embarrassment associated with effectively carried out terrorist attacks. Paradoxically, instead of diagnosing the errors within the structures, public sector responded in, previously unknown in democratic countries, increasing the competences of the security forces, *de facto* legalizing almost total surveillance. Symbolic examples are extremely controversial provisions

of the Patriot Act in the US and the EU Retention Directive. As a consequence, the fight against terrorism has become an excuse for blunt violation of standards related to privacy.

Służby bezpieczeństwa po zamachach terrorystycznych w USA i Europie – Patriot Act *versus* dyrektywa retencyjna, czyli legitymizowanie nadużyć w sferze prywatności w demokratycznych państwach prawa – studium porównawcze

Streszczenie

Akceleracja procesów technologizacji usieciowienia komunikacji, a wraz z nią interakcji społecznych, skutkowała zmianą paradygmatu społecznego, ekonomicznego i politycznego w przestrzeni cywilizacyjnej. Na potrzeby antycypowania coraz bardziej wyrafinowanych form zagrożeń opracowano i wdrożono nowe rozwiązania pozwalające państwowym agencjom bezpieczeństwa nie tylko utrzymywać *raison d'être* ale także zachować i poszerzać swoje aktywa. I tak amerykański system *Echelon*, czy ujawniona przez Edwarda Snowdena platforma *PRISM*m uświadomiły opinii publicznej, że agencje wywiadowcze (w tym w szczególności amerykański *National Security Agency*), nie tylko są w stanie przechwycić każdy sygnał teleinformacyjny, ale faktycznie z tego przywileju korzystają. Mimo takich atrybutów, z uwagi na braki administracyjno-logistyczne, nie ustrzegły się kompromitacji związanej ze skutecznie przeprowadzonymi atakami terrorystycznymi. Paradoksalnie zamiast szukać błędów wewnątrz struktur, sektor publiczny odpowiedział, nieznanym wcześniej w państwach demokratycznych, zwiększeniem kompetencji służb bezpieczeństwa, *de facto* legalizując niemal pełną inwigilację. Symbolicznymi przykładami są niezwykle kontrowersyjne przepisy zawarte w amerykańskiej ustawie *Patriot Act* oraz unijnej dyrektywie retencyjnej. W konsekwencji walka z terroryzmem stała się usprawiedliwieniem dla bezceremonialnego pogwałcenia norm związanych z ochroną prywatności.

Службы безопасности после террористических атак в США и Европе – Patriot Act *versus* ретенционная директива, или узаконивание злоупотреблений в сфере частной жизни в демократических правовых государствах – сравнительное исследование

Резюме

Ускорение процессов технологизации сетевой связи, и, в связи с этим, интеракция социальных процессов, привела к изменению общественной, экономической и политической парадигмы в цивилизационном пространстве. С целью прогнозирования возникновения всё более изощрённых форм угроз были разработаны и внедрены новые решения, позволяющие управлениям национальной безопасности не только поддерживать *raison d'être* (смысл), но также сохранять и расширять свои активы. Таким образом, американская система *Echelon*, или раскрытая Эдвардом Сноуденом платформа *PRISM*М оповестили общественное мнение о том, что спецслужбы (в том числе и в особенности американская *National Security Agency*), не только в состоянии уловить каждый телеинформационный сигнал, но и фактически пользуются этой возможностью на практике. Несмотря на перечисленные атрибуты, по причине недоработок административно-логистического характера, службы не застраховали себя перед компрометацией, связанной с результативно проведёнными террористическими атаками. Что парадоксально, – вместо того, чтобы искать ошибки во внутренних структурах, государственный сектор отреагировал ранее несвойственным для демократических государств расширением полномочий спецслужб, *de facto* (фактически), узаконивая почти тотальный контроль. Символическими примерами являются чрезвычайно противоречивые положения, содержащиеся в американском законе *Patriot Act* (Акт патриотизма), а также в европейской ретенционной директиве. В результате борьба против терроризма стала оправданием для бесцеремонного нарушения норм, связанных с неприкосновенностью частной жизни.